IT Nation SECURE MSP+ Playbook

Book 1: Fundamentals

v.2020.F1.1.2

WISE TOGETHER RISE TOGETHER

IT NATION SECURE cybersecurity by ConnectWise

Legal Disclaimer

Please note that these playbooks are provided only as examples and are for reference purposes only. In many instances, your existing procedures may suffice. Prior to implementing or adopting these sample playbooks, ConnectWise strongly encourages any organization to consult with its legal counsel, accounting, financial and/or human resource professionals. By doing so, this will assist your organization in developing policies and procedures that reflect its organizational philosophy and that are appropriate to their specific circumstances and consistent with applicable federal, state, and local laws.

These are provided as a free resource and "as is" without warranty of any kind. ConnectWise makes no legal representation concerning the adequacy of these playbooks or its compliance with federal, state, or local laws.

Never use sample policies and procedures that you find online as-is, as any policy you adopt needs to reflect the actual practices in your company. They must also be in compliance with all applicable laws and regulations, and there can be significant differences in state and local compliance requirements. You should always consult with a licensed attorney with experience specific to employment law prior to finalizing policies and procedures, whether they are individual documents or combined to form an employee handbook or procedures manual.

©2020 ConnectWise, LLC. All rights reserved.

Table of Contents

Introduction

Welcome to the IT Nation SECURE MSP+ Book 1: Fundamentals.

The MSP Community spoke, and we listened! IT Nation Secure has developed this book to help organizations standardize on a baseline set of security controls and practices. The book is a how-to for implementing these controls and practices, with each section building upon the last to culminate a solid foundational security program with measurements. Please note that this is a set of generic guidelines. Your organization may already have some, part, or all of these guidelines already implemented throughout your organization. Additionally, some of these programs may already be enhanced, either through your own hard work or compliance-related activities due to client requirements. We encourage you to read through the book to ensure you meet the baseline standard in all areas of Yellow before moving toward the Green or Blue. Use your best judgement and when in doubt or if you need assistance, please reach out to the team. Our goal with this Yellow book is to allow organizations to enhance and add the additional controls and practices needed to achieve MSP+ Certification, and then move toward SECURE MSP+ Accreditation.

Each section in this book contains a high-level program or set of security features. The sections contain elements on specific topics, practices, and controls with general guidance and information needed to help establish the fundamentals and framework to grow and mature a culture of security across your MSP organization. The IT Nation Secure team has developed the MSP+ Framework with influence from many popular standards of controls such as NIST, CIS, Cyber Essentials, and Essential Eight.

What is the IT Nation SECURE MSP+ Cybersecurity Framework?

The IT Nation SECURE MSP+ Cybersecurity Framework is a cybersecurity certification program for the MSP community. Based upon best practices and providing a journey of growth from baseline security elements to that of a repeatable and adaptive program, the MSP+ Cybersecurity Framework is designed as a resource to assess and enhance the cybersecurity posture and services provided by MSPs to their clients. The SECURE MSP+ Accreditation serves as a verification and validation process for MSPs to ensure suitable levels of cybersecurity procedures are in place, as well as the relevant cyber hygiene to protect their own systems, services, and data in addition to that of their clients.

How does this fit with our Security Journey?

The IT Nation MSP+ Cybersecurity Framework provides a roadmap for the security journey an organization needs to undertake in order to build an active, long-term, sustainable culture around cybersecurity. The SECURE MSP+ phased approach outlines and provides guidance for the growth and maturation of a cybersecurity program across the business and services of an MSP organization.

How do I apply this framework?

The IT Nation SECURE MSP+ Cybersecurity Framework outlines the progress for cybersecurity maturity and growth. Many MSP organizations know they need to improve their security posture and program, but do not necessarily know how to make those improvements or where to even begin. The MSP+ Cybersecurity Framework grew out of the demand for easy-to-follow assistance in identifying and managing cyber risk for the MSP to mature its business and services.

Why the different colors?

The color-coded guides from IT Nation SECURE MSP+ are inspired by the publication of the U.S. Government's "Rainbow Series" of color-coded books for evaluating "Trusted Computer Systems." If stacked together, the Rainbow Series of books would be six feet tall. Much like the creators of the Rainbow Series, IT Nation felt that having a color code would aid the MSP community with the adoption of the MSP+ Cybersecurity Framework. Fortunately, with digital technology, the MSP+ Cybersecurity Framework will not harm too many trees with its publication. Following is a breakdown of the colorized playbooks for the MSP+ Cybersecurity Framework:

Yellow Book provides the baseline or Fundamentals of SECURE MSP+ cybersecurity concepts for the foundation upon which to construct a mature and adaptive program across an MSP business, and services offered to clients. The Yellow Book presents the essential cybersecurity guidance to MSPs on how to implement a secure IT infrastructure to help reduce risk and vulnerabilities within the services provided to their clients.

Green Book offers informed guidance for expanding into the next elements of the MSP+ Cybersecurity Framework. The Green Book focuses upon the security journey for overall improvement and how to get better at monitoring and managing risk across the MSP operations and services. By taking this next step in the MSP+ Cybersecurity Framework, an MSP can better understand the effectiveness of their existing cybersecurity risk management efforts and work to identify any improvement opportunities within the context of their whole organization. Certification may be accomplished through a cybersecurity self-assessment against the MSP+ Cybersecurity Framework.

Blue Book outlines the plan for SECURE MSP+ Certification in addition to providing the guidance to attain the next maturity level of the security journey of the MSP organization. The Blue Book also offers relevant guidance to develop a formal system of metrics and measurement when defining a risk and security program across the MSP organization. Additionally, the Blue Book defines the requirements for SECURE MSP+ Certification that involves an assessment by an independent third-party (IT Nation) as a due diligence activity to validate a level of assurance with the overall security of the MSP operations and services.

What does it mean to be "SECURE MSP+ Certified" by IT Nation?

There are two types of certifications MSPs can achieve through the SECURE MSP+ program. The first is to self-attest all the requirements and objectives have been completed and receive an MSP+ Certification. This means the MSP can simply take an assessment and sign off that the organization has attained all the requirements and objectives set forth by the SECURE MSP+ governing body, IT Nation Secure. This is covered within the **MSP+ Green Book certification**. After completing all these objectives, your organization will have implemented all the necessary security controls, policies, and processes to best protect your organization and your SMB clients from a cybersecurity incident.

The second certification is the **SECURE MSP+ Certified Partner** based on the MSP+ Blue Book. This certification builds upon the Green Book by adding a few additional controls and producing evidence to support your self-attestation. The self-assessment and evidence will be reviewed by the governing body, IT Nation Secure staff, to ensure all items meet the standard set forth in the Blue Book. Once accepted, you will be granted access to the elite membership logo to use and promote your business.

Mirrored after the Cyber Essentials certification, the following outlines the path to certification for both MSP+ and SECURE MSP:

1. Decide which SECURE MSP+ Certification level you wish to certify towards.
2. Review the requirements for the certification and if for SECURE MSP, collect the evidence.
3. Ensure all the security controls outlined in the requirements for the certification have been implemented.
4. Submit your self-assessment questionnaire or update it if for SECURE MSP+.
5. If achieving a SECURE MSP+ Certification, upload all the required evidence for review.
6. Review and resolve any discrepancies outlined.
7. Resubmit the evidence for the discrepancies noted, if any.
8. Final review and certification issuance, assuming a positive outcome of the review.

Governance Program

Governance may be one of the drier subjects in Security, but it is also one of the most important. New technologies, data growth, and increasing cyber threats create challenges for organizations looking to set frameworks, strategies, and policies for keeping all that information secure. Governance aims to set strategic measures to protect an organization's information, which can be comprised of highly sensitive data and information.

The IT Governance Institute defines Information Security Governance as "a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risk appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security program."

Basically, Information Security Governance requires the assigning of roles and responsibilities, creating organizational structure, and defined measurements, all developed strategically with guidance from the board of directors and/or executive leadership.

Information Security Governance is often confused with IT Management. IT Management is primarily concerned with making tactical decisions to mitigate and prevent security risks. Governance focuses on the strategic, not the tactical. It is not the implementation of the policy; it is the oversight and creation of the program.

While security should be a concern for all employees, ultimately, leadership is responsible for establishing and maintaining a framework for Information Security Governance. Whether it is the board of directors, executive management, or an advisory committee — or all of these — Information Security Governance requires strategic planning and decision making.

Start with Policies

As part of your Governance Program, Information Security Policies will help establish the program and security within your organization.

Creating effective information security policies (ISPs) and ensuring compliance are critical in preventing security incidents. Policies are important for new and established organizations because they provide clear guidance and direction on how businesses, employees, contractors, and third parties conduct themselves while using information systems.

Information security policies aim to enact protections and limit the distribution of data to only those with authorized access. Organizations create ISPs to:

- Establish a general approach to information security.
- Detect and minimize the impact of compromised information assets such as misuse of data, networks, mobile devices, computers, and applications.
- Protect the reputation of the organization.
- Comply with legal and regulatory requirements like NIST, GDPR, HIPAA, and FERPA.
- Protect their customer's data.

- Provide effective mechanisms to respond to complaints and queries related to real or perceived cybersecurity risks such as phishing, malware, and ransomware.
- Limit access to key information technology assets to those who have an acceptable use.

An information security policy can be as broad as you want it to be. It can cover IT security and/or physical security, as well as social media usage, life cycle management, and security training.

The following nine Information Security Policies should form the foundation of your program. As you mature your program and move through the certification process, other policies will be added to your program.

Acceptable Use Policy
The Acceptable Use of Information Technology Resources Policy establishes the minimum standards for the acceptable use of your Information Technology resources.

Anti-Virus and Malware Policy
All applicable systems must be configured with Information Security Committee approved anti-virus software. The software must be configured to scan for viruses in real-time and end-users must not be able to configure or disable the software.

Data Access and Password Policy
This policy establishes security and business requirements for controlling and authorizing access to Company information assets. Access to these assets should maintain adherence to the principle of "Least-Privilege," ensuring that appropriate access is provided to accomplish the tasks of the business and excessive privileges should be avoided and deemed a risk to the organization.

Data Back-up Policy
Your Company must define and implement a comprehensive strategy for cyclical backup of data and programs. The strategy and implementation approach must be documented as part of the Back-up and Restoration Standard and comply with the Data Retention Policy.

Facility Security Policy
Access to your facilities must be controlled and approved by the appropriate level of management.

Perimeter Security and Administration Policy
This policy establishes the standards for administrative controls and baseline configuration for perimeter security controls including, but not limited to, firewalls, routers, and endpoint protection, whether managed by employees or by third parties.

System Configuration Policy
System infrastructure, including servers and other related devices, must be properly configured to prevent unauthorized access.

Telecommuting / Remote Work Policy
Telecommuting or remote working is an arrangement in which the participant performs their Company work at the participant's home or approved location for a specified period. The policy is intended to create flexible work conditions for the participant that will also help the organization accomplish its services more effectively. Successful work-at-home arrangements serve the needs of both participants and your company.

Vulnerability Identification and System Updates Policy
From a security perspective, software updates and security patches are released by the vendor to mitigate known flaws and vulnerabilities within their software. A Vulnerability Identification and System Updates Policy should contain standards for the identification, remediation, and prevention of system vulnerabilities to be established to protect the network, systems, and data of the MSP organization. This policy may include the timelines for patching applications, operating systems, and firmware.

How to Implement a Governance Program

Best Practices for implementing an Information Security Governance Program include:

Take a Holistic Approach

Before implementing any part of the program, it is important to understand how your organization views the impact of security on your organization. In other words, does your organization understand what data needs to be protected, where the risks to that data reside, what policies are in place, and which teams are responsible for carrying out these policies?

As you start to build out your program, you will need to get buy-in and input from all stakeholders including sales, marketing, IT, operations, and legal departments. They will each have different concerns and challenges, as well as skills and expertise.

This holistic approach ensures that leadership, the creators of the program, achieve more levels of control and visibility in the program.

Develop Awareness and Training throughout the Organization

Continuous adherence to security governance requires education, awareness, and training for everyone involved. Setting up an Information Security Governance Program and then not following through can bring negative results to the program. These negative results can lead to a misunderstanding of the policies, roles and responsibilities, and even security vulnerabilities.

Security is not just a concern for IT. It is everyone's responsibility.

Frequent company-wide communications including newsletters, lunch and learns, and education on best practices keep security in the minds of all employees. Although developed by the Board of Directors and/or Executives, Information Security Governance is the responsibility of everyone. Governance creates the policies and assigns responsibility, but each member of the organization is responsible for following the security standards.

Awareness Training and Education around security best practices must become a continuous process in your organization.

Monitor and Measure

Metrics are tools designed to improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data. Information security metrics monitor the accomplishment of goals by quantifying the implementation level of security controls. The efficiency of the controls is quantified by analyzing the adequacy of security activities and identifying possible improvement actions.

Constant assessing and measuring are needed to have a successful Information Security Governance Program.

What you need to know:

- What teams or individuals are not following the security policies?
- What policies are working?
- What policies are not working?
- Are the number of security incidents increasing or decreasing?

Measuring the performance on your efforts makes sure your objectives are being achieved and resources are managed appropriately.

This topic is so important we have a whole chapter on Security Metrics and their measurements.

Establish Open Communication Among All Stakeholders

It is crucial that all stakeholders communicate directly with their leadership. Working in silos risks obfuscating important communication as it relates to security governance. Make certain everyone knows how to communicate directly with leadership if needed.

If a security incident occurs, do employees at every level of the organization feel comfortable letting leadership know? Or will they attempt to cover up and shield top executives from any negative news?

Open communication that starts at the top and reaches all the way down into the organization promotes trust while improving visibility. To enhance engagement and participation, consider creating a steering committee with key executives and representatives from your different teams. Regular meetings of this committee will help ensure ongoing adherence to security policies. It also helps in the education and training of the organization as new policies are created and implemented.

Be Agile and Adaptable

As we discussed at the beginning of this section, technologies, data growth, and increasing cyber threats are rapidly evolving and can impact your business. Your Information Security Governance Program must be agile and adaptable to these changes. Monitor and measure your

program to see what is and is not working to help you understand what may need to change. If something is not working, do not be afraid to communicate and make changes.

The continuous assessment process monitors the initial security posture of your Information Security Governance Program to track the changes to the information system, analyzes the security impact of those changes, makes appropriate adjustments to the security controls and to the system's security plan, and reports the security status of the system to the Board of Directors and Executives.

To put it briefly, building a successful Information Security Governance Program does not happen overnight. Governance, just like Security, is a journey of learning, revising, and adapting to your environment. Emerging technologies and cyber threats will continue to be a part of our business. Strategic Information Security Governance must be at the forefront of our operations to prevent scrambling after a breach occurs. Your goal should be to deliver information security to reduce adverse impacts and risks to acceptable levels. Incidents and threats will occur, but with a measurable and adaptable Information Security Governance plan in place, your organization's security posture will be much stronger and able to protect your valuable information.

Privacy Program

Privacy is becoming a crucial area of focus for organizations of all sizes, and privacy topics are constantly in the news. It is critical to know your organization's business, people, and data before you can build your privacy program. You must lay the foundation, merge any existing and new pieces into one program, and then lead the way on all things privacy. Where do you start? What are the priorities? How do you introduce privacy concepts? You need a plan.

Privacy Program: Business, People & Data

Before building the privacy program, take time to get to know the business by becoming familiar with the products or services you offer. Understand who your customers are. Then, looking to privacy, what do the senior leaders see as most important? Additionally, are there any current policies or practices in place? If so, you have something to build on, but if not, now is the time to start building your Privacy Program.

Pulling existing privacy concepts together or building the privacy foundation anew not only establishes your program, but also helps your colleagues get a cohesive picture of privacy and its importance to the organization.

We are going to start building our Privacy Program by focusing on what we can do internally to the organization. The first key initiatives we are going to focus on are creating an Internal Privacy Policy, establishing a protocol for Data Retention, and educating your employees on the Privacy Program.

Internal Privacy Policy

Often, an internal policy can function like an introduction to privacy for employees. The policy can address a variety of topics specific to the way you want privacy to function in your organization. You may want to lay out what types of data the organization controls, the proper procedures for handling the various types of data, any security protocols relevant to privacy, or other privacy procedures that make sense for your company.

The difference between an Internal Privacy Policy and a Privacy Statement is that the Internal Privacy Policy is intended for internal use (policy formation and informing employees). The Privacy Statement is used for external purposes, like informing customers and suppliers.

We need to take care of privacy issues, as we have personal information about our employees and customers, not to mention confidential information about our company.

Your company's Internal Privacy Policy should cover areas such as:

- Employee records: personal information, medical history, etc.
- Email and Internet usage guidelines
- Handling client/customer information
- Internal systems and access: permission, responsibilities, access to files, etc.

- Mobile devices: company phones, laptops, and other devices and their disposal
- Established laws and regulations
- Consequences for violating the policy

It seems like a lot to cover, and it is, but these are all important topics that require significant consideration to get started.

When creating your Internal Privacy Policy, be specific, and do not leave room for your employees to interpret your intent. If you think you must spell it out for them, do so. There are a lot of great resources out there to provide examples of privacy policies, including the ConnectWise University: https://docs.connectwise.com/ConnectWise_Business_Knowledge/Information_Security_Policies.

Here are a few questions you should ask when developing your policy:

- Do all employees follow strict password and virus protection procedures?
- Are employees required to change passwords often, using foolproof methods?
- Is encryption used to protect sensitive information (a particularly important measure when transmitting personally identifiable information over the Internet)?
- Do you have staff specifically assigned to data security?
- Do staff members participate in regular training programs to keep abreast of technical and legal issues?
- Have you developed security guidelines for laptops and other portable computing devices when transported off-site?
- Do you have procedures to prevent former employees from gaining access to computers and paper files?
- Are sensitive files segregated in secure areas/computer systems and available only to qualified persons?

When creating this policy, it is also important that it states how to report a suspected or known security incident. Whether it is an accidental sending of an email to the wrong contact or clicking on a suspicious link in an email, every incident needs to be reported. The policy should include a list of email addresses, phone numbers, or other contact information so employees know how to report a security incident.

Protocol for Data Retention

If your company does not have a policy on data retention, it is time to design a plan which addresses the types of data you control and how long your company will retain that data. Not only can this reduce the risk and impact of a data breach, but it will also cut data storage costs.

This project can take some time but talking to the data storage team/administrator and other stakeholders about how much data you have and how far back it dates is a good place to start. Digging into the details on how long you need the various types of data will likely require decisions from senior leaders. This project can encompass various company-specific decisions but designing a data deletion policy is a worthwhile effort.

Local, state, federal and international policies, rules, statutes, and laws, as well as industry-imposed regulations specify the types of data that businesses must retain, and these bodies set the length of time that specific types of data must be retained and maintained.

Two good reasons to develop a Data Retention Policy, for both electronic and hard copy files, are to remove outdated and duplicate data and to create and save more storage space.

Following are some steps to consider when developing a Data Retention Policy:

- **Create a Team**
  It should include accounting, legal, finance, and department managers. Data deletion needs to be looked at from different angles. While the term for a financial document may be met, there may be a legal hold on the document which would require an exception to the deletion of that document. All parties must think through exceptions when creating this policy.
- **Review Contracts and Agreements**
  Contracts and agreements with your customers and vendors should be reviewed for consistent Terms and Conditions regarding the storage of data.
- **Determine all applicable regulations**
  Several regulatory bodies which have specific data retention and deletion periods include the IRS, HIPAA, and GDPR. Knowing which regulations, the organization must adhere to will shape your Data Retention Policy.
- **Define the data to be included**
  Documents, emails, contracts, employee and customer records, invoices, and financial reports are just a few.
- **Write your Data Retention Policy**
  Once you understand what happens to old data that you can remove or archive, it is time to formally write the policy. There are a lot of great resources out there to provide examples of data retention policies, including the ConnectWise University: https://docs.connectwise.com/ConnectWise_Business_Knowledge/Information_Security_Policies.
- **Ensure Awareness of the Policy**
  You never want to leave your vital organizational data to chance at any level, so provide employees with a copy of your data retention policy, once completed.

Data Retention Policies are key in managing and protecting your company's data to avoid any civil, criminal, or financial penalties which sometimes result from poor data management.

Employee Training on Privacy Policies

The purpose of policy is to create repeatable, reliable processes which do not require senior management oversight to keep your company secure. Now that you have an Internal Privacy Policy and a Data Retention Policy, you still need to train the staff to make sure they understand the content and can implement and track the procedures.

If the policies are designed using a step-by-step explanation that anyone can follow, it is easy to train your staff. With good documentation, any employee should be able to pick up a policy and understand its intent.

Provide hands-on training for the staff and walk them through the policies the first time. Do not just hand them out to your staff to read. The training process itself will highlight any weak areas in the written documentation. The staff also can contribute to the documentation by identifying gaps or areas that need clarification.

An important aspect of policy training is version control. Policies evolve with the needs of the company. The challenge is consolidating the changes in one place where they can be kept current and accessible. Too often, policies are amended to accommodate changes such as a new vendor or new regulation. Those policy changes may be noted by an individual within the department, but they seldom make their way back up the chain of command to be assessed and included in the master copies of the policy. If the keeper of that policy should be out sick or leave the company, the policies which were in their charge no longer work because they were not properly documented.

To help manage policies and provide the high-level oversight that the executive team needs to ensure compliance, use simple tools to keep the staff on task and provide a means to track their progress in reviewing and implementing policies. Simple checklists and reporting protocols will verify the staff is up to date on the latest policies.

Effective policy training is largely a matter of explain, refine, and repeat. As part of your training, be sure to create the feedback mechanisms necessary to capture any refinements or necessary changes. Be sure to amend your master documentation with the feedback so the policies are always current.

Other great ways to accomplish awareness of your privacy program include:

- Post information security and privacy messages within logon banners such as timecard logins, expense reporting, or other applications. These should be changed weekly or monthly.
- Hold a privacy poster contest.
- Host demonstrations of security and privacy applications used by your company.
- Pick a privacy or security policy and publicize it each month, highlighting why the policy is needed.
- Publicize recent security incidents and how they could have been avoided.
- Recognize an employee each month as being outstanding for their privacy practices.
- Post privacy posters in the break room or common areas. There are great sites out there that provide these materials.

You get the idea. Get everyone involved so they are always thinking about privacy and security. Starting and maturing your Privacy Program is a crucial step in keeping your company and your customer's data safe and secure.

Security Program

This Yellow Book provides the baseline of IT Nation SECURE MSP+ cybersecurity concepts for the foundation upon which to construct a mature and adaptive security program across an MSP business and client services. The Yellow Book is designed to present the essential cybersecurity guidance to an MSP on how to invest and implement a secure IT infrastructure with essential cybersecurity to help reduce risk and vulnerabilities within the MSP business operations and within the services provided to their clients.

The content of the IT Nation SECURE MSP+ Fundamentals Playbook (Yellow Book) should serve as a guide for an MSP organization to implement essential MSP security fundamentals as part of an overall security program. With the number of small to medium businesses that outsource their IT operations and services to the partner MSP community, it is important to establish a baseline of cybersecurity and compliance practices that address the unique risks, threats, and attacks accompanying the shared services model provided by MSPs. With the one-to-many model of an MSP serving its clients, a single cybersecurity compromise within the MSP environment could easily flow downstream into the connected systems of their clients. An MSP that secures their own IT systems, business operations, and workforce personnel practices will be in a much better position to protect their own clients from additionally falling victim to the same cybersecurity incident.

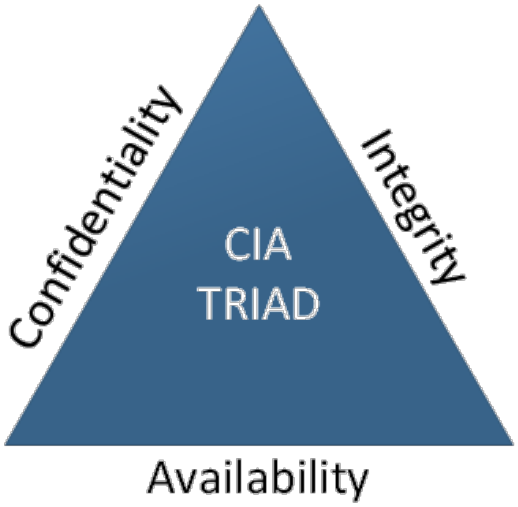
The overall Security Program consists of several interrelated programs, some of which may overlap within this guide. The main topic for the Yellow Book is to help outline and define how an MSP security program interacts and intersects with these initiatives while also providing a stronger cybersecurity stance for the MSP clients. With the framework of standards, protectives technologies, business practice, and user education adopted as part of an initial program, the foundation to grow and mature the cybersecurity culture of the MSP organization will naturally develop – with a small bit of work.

Organizational Controls

The problematic initiative with establishing a security program within an MSP is that the organization must consider a multitude of factors, and as such, the individual elements of the security plan may be different for each MSP. However, the goal of the IT Nation SECURE MSP+ program is to help an MSP organization determine a baseline of controls appropriate for specific circumstances surrounding the business and customer needs.

Most MSP organizations could be classified as a small or medium business employing less than 500 people that make up their workforce personnel. As a small and mid-size businesses (SMB), many MSPs have not fully invested themselves in the practical application of an overarching security program. This could be due to the problem that plagues many organizations – lack of resources, lack of IT knowledge, and lack of budget.

An MSP organization must assess and decide what elements of their IT systems and digital assets fall within the scope to apply baseline security controls. By identifying and documenting the computers, servers, network devices, mobile devices, information systems, applications, services, cloud applications, and third-party service providers that are required to conduct business and support customers, an MSP can then determine its value to the organization and work to secure it accordingly.



As part of determining the value of the IT system or digital asset, an MSP organization should assess the level of damage related to a compromise within the aspects of confidentiality, integrity, and availability of the IT systems and the data assets. Often cited as the CIA Triad, the concepts of confidentiality, integrity, and availability are the guiding principles that many organizations use in order to tailor their compliance programs.

- Confidentiality is achieved by preventing or limiting the disclosure of information to unauthorized individuals or entities. Confidentiality of data may be addressed through physical or logical access controls, user identity and access management, and the use of encryption.
- Integrity can be achieved by ensuring the accuracy and completeness of the data or systems that provide services. At a minimum, integrity checking monitors for the modification or deletion of files. Additionally, there are a variety of software tools and utilities available for integrity checking that compare hashed values and/or generate log entries upon the modification or deletion of files.
- Availability is the concept that ensures the reliable access to data and services is there when it is needed. Implementing high availability systems throughout your security architecture is one way to safeguard availability of data and services. High availability systems are intended to be fault tolerant and designed to prevent disruptions from power outages, hardware failures and denial-of-service attacks.

The IT Nation strongly recommends that MSP partner organizations consider ALL their IT systems and assets – whether company owned, outsourced, contracted, or otherwise used as part of the business operations – within the scope for recommended security baseline controls.

After documenting its collection of IT systems and digital assets, the MSP organization should look to identify and document its business and information security risks. A systematic risk assessment should be conducted to recognize any potential threats and vulnerabilities your

organization may have, in order to develop a security plan with prioritized efforts and investments.

Plan of Action and Milestones (POAM)

In developing the fundamentals and maturing a security program for the MSP organization, one must consider that at any given moment there will be a good number of actionable plans on file within individual workloads. The driving idea is for the MSP organization to maintain (develop and implement) plans of action for vulnerabilities and deficiencies across the systems within their organization. To integrate plans surrounding patches, upgrades, deficiencies, vulnerabilities, or any unmet requirements into an all-inclusive view, initiative should be taken from the top of the organization and must be adopted by all workforce personnel.

A Plan of Action and Milestones is often referred to as a POAM or POA&M. A POAM is a documented plan that indicates the specific measures the MSP organization will take to correct deficiencies found during a security assessment. For the MSP, the POAM should clearly identify tasks to be accomplished, who owns the actions, and any resources required for the plan to be implemented. In short, POAM will need to be developed for any of the following scenarios:

- When new requirements to software, systems, or processes are introduced
- When vulnerabilities are discovered and require remediation
- When deficiencies are identified and need to be addressed

Much like the steps needed when managing a project, each POAM has a life cycle that starts with the identification of a need, documents the steps to address that need, and then goes away as that need is met. A POAM can be a very simple document that states the issue, contains bulleted action items assigned to owners, and sets a milestone marker as a date the action is to be completed. Once all requirements are addressed, the POAM will naturally depart from workflows to be archived for reference if needed.

The plan of action and milestones (POAM) serves as a tool the MSP organization can use as part of Risk Analysis and Risk Management.

- **Risk Analysis:** The MSP organization conducts an honest and thorough assessment of potential risks and vulnerabilities that may impact the confidentiality, integrity, and availability of critical systems and important data.
- **Risk Management:** The MSP organization implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level of acceptance and/or compliance.

Investment into Cybersecurity Program

The secret to the success of any security program effort involves the active participation of workforce personnel and upper management in developing a security mindset to protect their physical workplace and to secure access to important data. Upper management must embrace the security program and lead the organization by example throughout the adoption and

implementation of security training and policies. When the MSP employees and workforce personnel witness upper management taking an active role, they will comprehend and appreciate the importance of the security program and follow through on assigned training and take ownership of their role in ensuring safety and security across the organization.

An MSP organization should consider aspects of the following IT components, scenarios, and associated projects as part of a maturity roadmap to be implemented:

- Mobile and Desktop Devices
- Cloud application and Directory Services
- Mobile-Device Manager (MDM/Cloud Service)
- On-Premise Applications
- On-Premise IT Infrastructure
- Security Incident and Event Management (SIEM)
- Identity and Access Management Capabilities
    - Identity Store
    - Access Rights Management (Role-Based)
    - Authentication and Authorization
- Network Segmentation Capabilities
- Encryption Capabilities (Disk Level)
- Network Monitoring Capabilities
- Asset Management Capabilities
    - Vulnerability Scanning
    - Automated Update
    - Asset Identification
- Remote Monitoring and Management (RMM) Capabilities
- Professional Services Automation (PSA) Capabilities

A purpose of a POAM is to facilitate a disciplined and structured approach to tracking the risk mitigation activities in accordance with any of the above projects and initiatives. The POAM should include the MSP's intended corrective actions and the current threat level for any findings identified as part of the project. As such, the POAM includes the:

- Security categorization of the information system (Critical/High/Medium/Low)
- Specific issues or defects with deployed security controls
- Importance of the identified security control issues or defects
- Scope of the issue or defect with the components that make up the environment
- Proposed risk mitigation action to address the identified issue or within the implementations (e.g., prioritization actions for time and talent – workforce, time, funding, etc.)

Physical Security Measures

Frankly, the most important asset an MSP organization has is the people that comprise their workforce personnel. The initial security policies and practices adopted by any MSP organization must ensure the physical safety and security of visitors, contractors, employees, and workforce personnel at the business offices and work facilities. By implementing a few common security practices, an MSP organization will be in a better position to protect its people and minimize many of the underlying risks surrounding IT assets and important data.

Gaining access to your property, offices, and workspaces can provide an individual with the potential opportunity to not only to steal physical items from the facilities, but also to potentially access and infect computers (desktops, laptops, and servers) with malware or gain access to important information via the IT infrastructure (networks, Wi-Fi, switches and routers). A practical risk assessment of all MSP offices and workspaces to identify physical security vulnerabilities should include an initial review of:

- Where any unauthorized access may be occurring or could possibly occur.
- Where entrances and exits to business-critical spaces may not be covered by a high-definition security video camera.
- Where any undetected and/or unmonitored intrusions could occur on the property, throughout the buildings and into critical areas within the buildings.
- How existing access control processes work in order to make certain that access credentials are adequate and current, and that any access control database is up-to-date with the proper list of individuals who may access certain controlled areas such as server rooms or IT equipment areas.
- How physical security policies and procedures, including hiring background checking as it relates to security vetting, are being utilized across the organization and if they currently meet the needs of the business.
- How the existing security staffing levels fit the current needs of the organization.

Though they may differ based upon the specific needs of the organization, there are several baseline physical security measures that an MSP can adopt in order to help protect and secure IT and digital assets.

Secure IT Servers & Equipment

Obviously, the business needs to have some method of securing and controlling access to the premises. A small office with single door for entry can most likely be secured with a simple door lock and key. However, a much larger business worksite with multiple entry points may require a more advanced way to secure the facility by using a system employing keycards and ID badge access. The access controls should be in-line with the business needs of the MSP. Additional security access control systems could include high-tech options, such as biometric finger-print scanning or a lock with a PIN-entry system.

Physical security vulnerabilities and cyber risks:

- Digital switches that have open, unused ports
- No VLAN separation between guest and business networks
- Unencrypted communications being passed across the network
- Switches that do not have the MAC address of their attached devices "locked"
- Switches that are not configured to lock out any unknown devices when connected
- IT cabinets and closets that are unlocked or open to more than just authorized workforce personnel
- Areas that contain sensitive equipment or data are not fitted with security cameras
- Security servers are not kept in locked racks and access to the "server room" is not controlled
- Cameras viewing sensitive areas of the workplace are kept in view of the public
- USB and DVD drives are not disconnected or disabled from video monitoring systems

Clean Desk Policy

It is crucial to protect sensitive information from disclosure where the workplace is open to employees, visitors, vendors, and cleaning crews. The adoption of a clean desk policy is designed to allow for the protection of any information and data that may be found at a user's workstation. With the removal or secure storage of sensitive information when employees or workforce personnel are away from their desk, the MSP organization can ensure that data confidentiality, integrity, and availability may be guaranteed. A clean desk policy should also include areas away from a desk and carry over into common areas and meeting rooms by erasing whiteboards and gathering materials that may be left behind after a meeting.

During the day it is good practice for workforce personnel to:

- Use lockable drawers or filing cabinets to store sensitive documents and any computer media.
- Use security cables to lock laptops to a workstation or desk.
- Lock desktop/laptop screens when walking away from a workstation with Ctrl+Alt+Delete (Windows) or Command+Ctrl+Q (Mac OS).

One good practice is to not leave any sensitive documents or information laying around. Such items that could be potentially be disruptive to the security of your organization include:

- User IDs & Passwords
- IP addresses
- Contracts
- Account numbers
- Client lists
- Intellectual property
- Employee records
- Anything you would not want disclosed

At the end of the workday, each person should be aware of their workspace and take a few moments to prepare the area:

- Organize and secure any sensitive material
- Lock any drawers, file cabinets, and offices
- Secure expensive company equipment (laptops, tablets, mobile devices, etc.)
- Secure any personal items (headphones, earbuds, tablets, etc.)

Visitor Program

Having a clearly understood visitor policy and escort program is vital to the security of employees, workforce personnel, clients, physical assets, and important data. The type of visitor policy needed fully depends upon the type, size, and location of your MSP office and workspace. For example, how you manage the visit of a guest at a small MSP in a shared office complex with ten employees will likely be much different than the procedures in place at a larger MSP that may be hosting a data center within their own building. However, no matter the size of the MSP office or facilities, certain common issues will need to be addressed by the organization. If you currently do not have a visitor policy or escort program, then now is the time to create one by way of establishing clear policy and procedures. If the MSP organization currently has a visitor policy, then periodically revisit, review, and update it to meet any new challenges or address any issues. Following are some guidelines to help with the creation or review of a visitor policy and visitor escort program.

Define Authorization Procedures

Clearly define and document who has the authority to approve visitors to your facilities. In some cases, an MSP may allow anyone on staff the ability to authorize and admit guests. In other organizations, only managers or receptionists may check in visitors. It is a best practice to have clear procedures as to who will hold authority to allow visitors within the workplace environment.

Establish Office Access RestrictionsA visitor policy should include details surrounding which areas of the workplace are open to which types of guests. For example, you may open the conference rooms to all visitors and not allow visitors into the server rooms or certain floors of the building. Pay special attention to any rooms used for IT equipment or for storing confidential information; such sites should be off-limits to all non-employees. It is a common workplace practice to restrict visitor access at some level beyond the lobby.

Maintain A Visitor Log

At all times, it is a good practice to know who is always in your workplace or office. Depending upon the size of the MSP organization and the type of business, visitor sign-in procedures should include the use of a valid, government issued photo ID as proof of identification. Additionally, in case of an emergency, it is critical to know who is onsite and that they have been accounted for. To help with the process of logging visitors and keeping records, there are many

software applications available that can ensure a level of confidentiality and offer records for reports and future reference.

Highlight Identification for Guests while in the Office

A good security measure that most any MSP organization can implement is to issue ID cards for both staff and visitors. Many organizations choose to identify workplace visitors while onsite with a printed ID badge to promote the clear recognition of guests. Not only can the use of ID cards work as a way for security staff to check people entering the building, the ID cards also make anyone without one stand out among other workforce personnel.

Establish Guidelines for Escorting Visitors

For both security and visitor-safety reasons, make certain that guests are not allowed to freely wander around the workplace on their own. Consider establishing specific responsibilities and guidance for employees to be responsible for escorting a visitor to the workplace. For instance, an employee acting as a visitor escort may be responsible for safely evacuating the guest in case of an emergency. Additionally, the employee escort may also be responsible for making sure their visitor complies with existing company policies and practices good security measures while a guest of the MSP organization.

Define Visitor Types

Different kinds of visitors may require different treatment when visiting a workplace at the MSP organization. When visiting a site, will the treatment of friends and family of employees require a different protocol from other guests, such as vendors or contractors? Depending upon the type of business conducted by the MSP, there may be legal restrictions or regulations in place as to who may access a facility where government or payment card information is processed. Are there any requirements necessary for foreign nationals or visitors requiring a background check to be cleared to access a facility? Additionally, the MSP must consider the whole of their visitors and workforce personnel as being made up from different types of employees as well, such as temporary workers, former staffers, and even employees who access the workplace during off hours.

Implement Visitor Policies for Recording, Wi-Fi, and Non-Disclosure

The protection of individual privacy, intellectual property, and other confidential information should be a major concern for every MSP organization. Such protection may require placing certain restrictions upon the authorized guests within the workplace. As a best practice, a visitor policy should contain details surrounding the appropriate use of your guest wi-fi network and any related technology. Address any concerns over the use of recording equipment (cameras, phones, and audio devices) to capture photographs, video, or audio recording while the visitor is a guest of the organization. Depending upon the guest and the intention of certain meetings, non-disclosure agreements should be addressed – especially if dealing with any intellectual property.

Educate Staff

A visitor policy is only as good as it is understood and implemented. Make certain that the employees of the organization are familiar with the defined policy and procedures for handling visitors. Investing the time in spreading awareness and educating workforce personnel may allow the MSP organization to stave off a security breach. Through implementing training and education, the workforce personnel of the MSP organization will know the correct procedures to help visitor interactions run smoothly and minimize any unnecessary risk.

Boundary / Perimeter Security Solutions

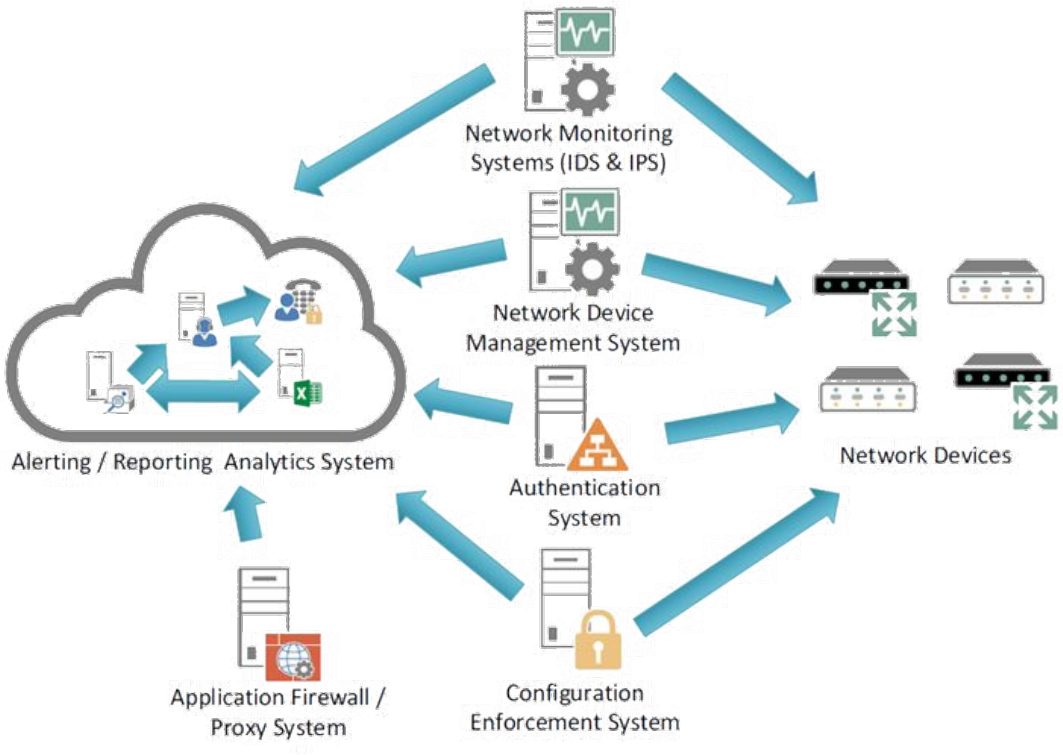
Imagine the boundary/perimeter security design as one of layered defenses similar the fortifications of a medieval castle surrounded by a moat and high walls. To access the castle, one must cross a lowered drawbridge and be inspected by guards prior to passing through an open, raised portcullis in order to enter the courtyard. Once inside, one may have free access to roam throughout the courtyard but are restricted from entering the interior of castle keep. As the daily onslaught of complex and frequent cybersecurity threats carry the most serious challenges for many organizations, the need exists for an MSP to assign operational workforce personnel and financial resources to defend and protect their IT infrastructure and business operations.

To ensure a comprehensive boundary/perimeter security architecture, an MSP should identify and document what critical systems, services, and data must ultimately be protected and then design their boundary/perimeter security to scale in order to meet the immediate business and operational demands. An MSP must be flexible enough to meet any future needs as the organization grows and changes. Adopting best practices surrounding boundary/perimeter protection, which is the first layer of defense within the network, serves to prevent many of the malicious attacks that can directly disrupt internal MSP operations. Best practices help to avoid a potential downstream impact to client IT systems and their data environments.

Boundary/perimeter security protection makes use of numerous tools and solutions (i.e., firewalls, routers, VPNs, Intrusion Detection Systems (IDS), etc.). More precisely, boundary/perimeter security protection solutions serve to secure and monitor the connections of a trusted network with an untrusted or public network. Additionally, Boundary/Perimeter Security protection includes the monitoring and control of network communications within an internet-facing, external boundary, or logical perimeter of connected business IT systems and services. The intent of such boundary/perimeter defense posture is to prevent and detect any malicious or unauthorized access to IT systems and important data.

Boundary protections are commonly the first line of defense against an outside attacker. It is common practice for an attacker to poke at an organization's network boundaries in order to probe and build an attack profile with the information gathered from the perimeter network. Today, a stand-alone firewall is no longer enough to protect against the more complex threats. Boundary defenses now require additional perimeter solutions such as IDS/IPS, SIEM, SSL

Decryption, Outbound Proxy, and network monitoring, as highlighted within the following diagram.



A Layered Boundary Defense

When properly implemented and layered together, many tools could likely detect and potentially prevent such malicious activity from taking place. These tools include:

- Perimeter IDS/IPS: Filters unwanted, malicious communications (inbound).
- Outbound Web Proxy: Filters employees from visiting unwanted sites (outbound).
- SSL Decryption: Analyzes encrypted data for examination and content control.
- SIEM: Correlates and consolidates logs and data from multiple sources.
- Application Aware Firewalls: Analyzes outbound traffic for irregularities.

Along with layered security (Defense-in-Depth) and other similar concepts, boundary / perimeter protection is an example of the information security principle of confidentiality, integrity, and availability (CIA) for the critical IT system resources of the MSP business operations and client services.

At a minimum, the administration of boundary / perimeter security devices should follow and maintain a configuration management standard that includes the following documentation:

- A current network topography diagram (representing both the logical and physical design) that includes all connections to and from all service networks.

- A list of all ports, protocols, and services used for business connections to and from network segments carrying confidential or regulated data.
- An exception ledger that documents the business justification for all insecure ports in use between private networks and public/untrusted networks (e.g., FTP, Telnet).
- An identified and defined roles and responsibilities assignment for device management.
- The formal process for assessing, conducting, and approving changes to firewall policy rules, router configurations, etc.

Firewalls

NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy, defines firewalls as "devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures." Firewalls provide boundary / perimeter security by restricting inbound and outbound traffic to the essential minimum necessary to properly conduct business. The most common deployment of firewalls is to create a buffer between an IT network and other, external networks such as the internet, which is essentially an open, public network.

The adoption of firewall security configuration standards and operational practices establishes one of the core essentials necessary to defend MSP organizations against known and unknown cyber threats. The evaluation, adoption, and implementation of a firewall solution should combine the knowledge and understanding of information risks and best-practice guidance with security and policy configurations aligned with business interests. Firewalls are a necessary solution for every MSP to help protect against:

- Criminal hackers trying to breach the internal network or services.
- Viruses that spread from computer host to computer host by way of the internet.
- Outbound malicious network traffic originating from a virus or other malware.

While firewalls are often discussed within the context of Internet connectivity, they may also be deployed within other network environments to restrict connectivity to and from internal networks reserved for sensitive functions (e.g., accounting or human resources) or to meet industry requirements or regulations (e.g., PCI or HIPAA). By employing firewalls to control connectivity to these areas, an organization can prevent unauthorized access to its systems and resources.

Several types of firewall technologies may be implemented as a stand-alone device or as part of an integrated device platform known as a next-generation firewall (NGFW). Traditionally, a firewall provides stateful inspection of network traffic. It either allows or blocks traffic based on state, port, and protocol, and then filters the traffic based on administrator-defined rules. A next-generation firewall not only provides the stateful inspection of incoming and outgoing network traffic, but also blocks modern threats such as advanced malware and application-layer attacks. A next-generation firewall may include the following capabilities:

- Stateful inspection
- Integrated intrusion prevention
- Application awareness and control
- Threat intelligence source integration
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

When installing a new firewall solution or making a change to an existing firewall configuration, one must consider any potential security risks to avoid potential security issues. By its nature, security is a complex topic and often varies from use case to use case. Following industry best practices for configuring firewalls can help capitalize upon the efficiency and effectiveness of the solution.

A firewall policy is the collection of individual rules that manage what is and what is not permitted through a firewall. For example, a transport layer (OSI layer 4) firewall enforces the following elements within an individual rule that makes up its overall policy:

- Source IP Address (or range of IP addresses)
- Destination IP Address (or range of IP addresses)
- Destination Port (or range of ports)
- Protocol of the Traffic (TCP, ICMP, or UDP)

Each element may be configured to either block or allow.

As described within the UK government's Cyber Essentials program, administrators should regularly perform the following actions as a minimum best practice for all network firewalls (or equivalent devices):

- Change any default administrative passwords on the firewall.
- Prevent remote access to the firewall's administrative interface from the Internet, unless there is a documented business need and the risks are fully accepted and understood.
- If remote administrative access to the firewall is allowed and utilized, one of the following control mechanisms must be used:
    - Another, or secondary, authentication factor, such as a one-time token.
    - An IP whitelist that limits remote access to a small range of trusted IP addresses.
- Block and drop any unauthenticated inbound connections by default.
- Ensure inbound firewall rules are approved and documented by an authorized individual; the need for the rule must be included in the documentation (see below).
- Remove or disable permissive firewall rules as soon as they are not needed.

Document Firewall Rule Changes

It is recommended to identify and document each firewall rule so you know what action a firewall rule was intended to perform or enforce. It is good practice to track the following:

- The operational purpose or business need of the firewall rule.

- The affected service(s) and application(s).
- The affected users and devices.
- The date when the rule was added.
- The date when the rule should expire or is no longer required, if applicable.
- The name of the person who added or changed the rule.
- The name of the person who approved the rule or the rule changes.

Establish a Formal Firewall Change Procedure

As the MSP organization grows and expands, firewall rules will need to be modified to accommodate new services and new devices. Documenting each firewall rule and the person who approved the rule helps to lay the groundwork for establishing formal change procedures for modifying the boundary / perimeter elements.

The following are recommendations that and MSP organization should adopt as part of a firewall change procedure process:

- Define and adopt a change request process for users to request firewall changes.
- Establish a group or committee to process and analyze incoming change requests, determine their impact, and approve the best, most secure course of action.
- Create a standardized process for testing new change requests on production firewall rules. For example, in a test environment or by piloting a limited program.
- Document procedures and guides for deployment of tested change requests into production firewall rules.
- Ensure there is a process to test and validate that new firewall changes and settings are operating as intended.
- Track changes and maintain a documentation repository for all firewall changes that have been implemented.

Block Traffic by Default

Block all network traffic by default and only allow specific traffic to known and identified services. This approach to firewall management provides a respectable amount of quality control over the allowed traffic and reduces the likelihood of a perimeter breach due to a policy misconfiguration. As most firewall policies are enforced by reading a control list of rules from the top down, blocking by default can easily be established by simply configuring the “last rule” in a firewall policy to deny all traffic.

The “last rule” serves as a safety measure to prevent unwanted network traffic from passing through the firewall. Also known as an “any-any-any drop” rule or a “clean-up” rule, this rule is normally defined as:

- Source IP Address = ANY
- Destination IP Address = ANY
- Service / Application = ANY
- Action = DROP

- Logging = Enabled

The firewall solution vendor should have step-by-step documentation describing how to specifically configure rules to block traffic by default.

Only Allow Specific Traffic to Known Services

Blocking all network traffic by default and creating firewall rules that only allow specific traffic to identified services enforces the principle of least privilege over the boundary / perimeter network traffic. It is recommended to specify as many parameters as possible within a firewall rule and to limit the use of "ANY" in a rule.

The most explicit rule in the list performs its action prior to the next rule in the list. Working from the top down ensures that network traffic permitted by the first rule is not blocked by the other rules as the firewall works down the list of rules within the policy.

The SANS Institute provides a non-vendor specific Firewall Checklist that provides a generalized listing of best practices and security considerations to be used when implementing or auditing the security, rules, and policies of a firewall. The following is the recommended order for the application of firewall rules from SANS:

- Anti-Spoofing Filters (block internal / private IP addresses as appearing from the outside – see RFC 1918 https://tools.ietf.org/html/rfc1918)
- User / Application rules (e.g. allow HTTP HTTPS to public-facing web server)
- Management Rules (e.g. SNMP traps to network management server)
- Drop Noise Filters (e.g. discard any OSPF and any HSRP chatter)
- Deny and Alert (alert monitoring systems or firewall administrator of suspicious traffic)
- Deny and Log (log any remaining traffic for analysis and identification)

The SANS Institute Firewall Checklist and other useful step-by-step security guides are located at the following URL: https://www.sans.org/score/checklists/firewall

Logs and Auditing

On the firewall solution, ensure that logging is enabled and that the logs are periodically reviewed by assigned staff to identify potential patterns that may indicate a compromise or ongoing attack. Many vendors provide or include a built-in reporting utility for the detailed analysis of information related to the network traffic with their firewall solutions. The reporting utility should help staff with auditing logs to identify any anomalies or events that may imply the need to modify the firewall settings to address an ongoing issue, such as a false positive or false negative alert.

False Positive alerts are mislabeled security alerts and indicate that there is a threat when there is not. False or non-malicious alerts can include misconfigured software, poorly coded software, or unidentified network traffic.

False Negative alerts are the opposite of false positives and indicate that there is no vulnerability when there actually is a vulnerability. A false negative alert may be an unknown cyber threat that requires further investigation from the staff analyst assigned to the role.

The decision to modify firewall rules may be based off compiled reporting information and analysis of alerts. Modify rules to reduce noise from false positives and to improve the firewall's overall security and service throughput.

Additionally, firewall logs can be forwarded to a security information and event management (SIEM) platform that collects and aggregates log data generated throughout the technology infrastructure of an organization. The SIEM may provide more robust reporting and analytics.

Review Rules and Patch Devices

The networks will continue to change as the organization grows and matures and new devices and users are added. Because those users and devices will need to access new services and new applications, new rules and policies will need to be added to production firewalls. It is a best practice to establish a regular maintenance schedule for implementing changes to production firewall rules. The organization may want to make firewall changes during off-peak hours, such as a Thursday night or a time over the weekend. The change window depends entirely upon the organization and the nature of the change.

Additionally, it is a good practice to perform a regular audit of all existing firewall rules. At a minimum, the organization should audit the firewall on an annual basis. However, depending upon the rate of growth and change, the organization may decide to perform firewall audits quarterly or semi-annually. The schedule should be based upon the fluid nature of the organization and the rate of changes to firewall policy. Old firewall rules will need to be reviewed against the current business needs and removed as needed. These audits will also help catch any weakness or oversight in the configuration of the boundary / perimeter security controls. In addition to the firewalls audits, it is also recommended to review the security and policy controls to address any changes in technology or within the business operations of the organization.

Finally, the firewall (software or device) should always be running with the most recent vendor patches and firmware. If the firewall is operating in an unpatched state, then it may be vulnerable to certain cyberattacks that could potentially bypass the firewall and existing protection rules. Use a scheduled maintenance window to install and certify that the latest patches and updates for your firewall solution are installed. The firewall vendor should have helpful guides and documentation that step through the specific patching process for their product. If vendor patches and updates are automatically downloaded from the internet, confirm that the updates are received from a trusted vendor site.

VLANs and Segmentation

Virtualization has become universal across many aspects of information technology and its adoption in networking is no exception. Virtual Local Access Networks (VLANs) are widely used

on most every network. Many managed services providers (MSP) configure (OSI layer 2) VLANs to segment, isolate, and better manage their clients and client host systems. Isolating clients in this manner is a good security practice. Whereas a flat network allows an attack surface to all hosts with an IP addresses, a properly segmented VLAN helps to bolster security by isolating and hindering an attacker's ability to extend their access to hosts across the VLAN segments.

A Local Area Network (LAN) connects computers, laptops, servers, printers, and other network capable devices using Ethernet cables or Wi-Fi. LANs are designed to provide networking and internet services within a single, physical location and on the same network or subnet. In contrast, a VLAN is a custom network created from devices that reside on one or more existing LANs. A VLAN enables groups of devices from multiple networks to combine as if they were on a single logical network. The result is a virtual LAN that can be administered in the same manner as a physical LAN. Computers in a VLAN may be separated by bridges, routers, or switches and may physically reside in different locations. Compared to LANs, VLANs help to reduce network traffic and collisions and are often more cost effective.

A VLAN acts like a physical LAN but allows hosts to be organized together in the same broadcast domain even if they are not connected to the same switch. According to Cisco Systems, the top switch manufacturer and vendor, VLANs are commonly used for the following:

- To increase the number of broadcast domains while decreasing their size.
- To reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood.
- To separate hosts that contain sensitive data and improve security.
- To create more flexible network designs that group users by department instead of by physical location.
- To easily make administrative and network changes by simply configuring a port into the appropriate VLAN.

Additionally, VLANs are configured using the standard layer two (L2) technology built into most modern switches. VLANs also benefit from the security capabilities built into the switch by the vendor and from standards based on IEEE Standard 802.1Q created by the Institute of Electrical and Electronics Engineers (IEEE). The vendor supplying network peripherals and switches to the organization should be able to provide documentation and procedures for the proper deployment and configuration of VLANs to meet any of the solutions described above.

However, when using switches and VLANs, it is essential to keep in mind a few security considerations and to address potential vulnerabilities of layer two across the organization.

Physical Security

Because a switch can be managed via a console port that is physically located on the switch itself, it is recommended to house all switches and network infrastructure devices in a secure, locked room or cabinet. Personnel access to the IT equipment should be limited and controlled.

Telnet Access

Administration of a switch can be conducted over Telnet, an unsecure, unencrypted protocol. If an attacker intercepts the Telnet packets, they may be able to obtain the login credentials and gain administrative access to the switch. To protect against this, it is recommended to use Secure Shell (SSH) as an alternative to Telnet when performing switch administration.

SNMP Access

The Simple Network Management Protocol (SNMP) is used by network management for the collection of information about network devices. Older versions, prior to SNMP version 3, lack many of the security enhancements and may allow both READ and WRITE capabilities. It is recommended to use SMTP version 3 or to only allow READ for the older versions.

Reduce Exposure

Switch administrators can decrease a switch's attack surface and potential exploit by disabling unnecessary services and by turning off unused Ethernet ports. Additionally, switch administrators can limit the number of MAC addresses that each switch port can learn.

Logging

As with firewalls and other boundary / perimeter network devices, an organization should log any attempts to access the switch. It is recommended to regularly review access logs to help switch administrators identify potential threats.

Change Control

As an organization grows and more network administrators are employed, multiple switch administrators may have to share the roles and responsibilities for configuring network devices and switches. Having a formalized change control policy and accompanying procedures will help administrators to properly document, approve, and coordinate changes to the IT environment.

VLAN Configuration

For best results, consult with the switch vendor for the organization and consider the following recommendations for configuring VLANs on a network switch:

- Many switches include a trunk port feature. Unless needed, it is recommended to set the trunk settings to "OFF" instead of "AUTO".
- Do not send user data over an IEEE 802.1Q trunk's native VLAN.
- A private VLAN partitions the layer 2 broadcast domain of a VLAN into subdomains, allowing ports on the switch to be isolated from each other. It is recommended to use private VLANs to prevent an attacker from compromising one host in a VLAN and then using that compromised host as a pivot point to attack other hosts within the VLAN.

VLAN Hopping Exploits

The VLAN hopping exploit allows an attacker to bypass layer 2 restrictions configured to isolate and divide network hosts. Many networks either are misconfigured or have an unsecure VLAN implementation. Improper VLAN configuration allows an attacker to perform VLAN hopping by way of switched spoofing, double tagging, or a combination of both.

Switch Spoofing Attack

A switch spoofing attack works by manipulating an incorrectly configured trunk port. The default trunk port on a switch is normally used for logging or packet capture. This trunk port is configured to have access to all VLANs and will pass all traffic for multiple VLANs across the same physical port (or link between two switches). After an attacker establishes a trunk link, they gain access to the traffic from any VLAN. The switch spoofing exploit is only successful when the switch is configured to automatically negotiate a trunk. Following are recommendations to avoid switch spoofing attacks:

- Never leave an access port on a switch open and configured with dynamic desirable, dynamic auto, or trunk mode.
- Hardcode all access ports on the switch and disable Dynamic Trunking Protocol (DTP).
- Hardcode all trunk ports and never enable Dynamic Trunking Protocol (DTP).
- Shut down all unused interfaces on the switch.

Double Tagging Attack

Double tagging attacks occur when an attacker adds and modifies VLAN tags on an Ethernet frame to allow packets to be sent through any VLAN and connected switch. This attack bypasses the network controls that logically isolate VLANs from one another as most switches will only remove the outer tag and forward the frame to all native VLAN ports. However, the double tagging exploit is only successful if the attacker belongs to the native VLAN of the trunk link on a switch. Additionally, this attack is only performed in one direction as it is impossible to encapsulate the return packet. Following are recommendations for preventing a double tagging attack:

- Do not put any host on the default VLAN of the switch.
- Change the native VLAN ID to an unknown VLAN name created by the switch administrator (document this setting).
- Perform explicit tagging of all native VLANs on all trunk ports of the switch.

Please refer to the vendor of your switch for additional documentation and procedures that may be required to protect the organization against VLAN hopping exploits.

Internet Gateways / Proxy Servers

Proxy servers and internet gateways can both route traffic from inside a network to the outside, public internet. However, an internet gateway acts more like an open door that provides a gateway for the organization to access the internet. By contrast, a proxy server acts more like a like a bank teller window that blocks the inside network from being fully exposed to the public internet. A proxy server can actively filter which connection is allowed, but a gateway does not necessarily perform any filtering. Elements of both internet gateways and proxy servers can be combined into a hybrid network device. Vendors often offer these hybrid network devices as a solution under next-generation firewalls.

Internet Gateway

For two networks to communicate, a default (or network) gateway must be provided from each network. Within a boundary / perimeter security context, a gateway defines what is internal to the network and what is external. If a computer needs to communicate with a host outside the network, then an internet gateway must be configured to gain access to the outside internet or third-party network. Without a gateway, the computer will not be able to communicate with other hosts beyond its own internal network.

Proxy Server

A proxy server acts on behalf of the internal network and regulates access and connections from the outside. Any outside user or service attempting to connect to a host inside a network with a proxy will only connect and see the IP address of the proxy server. The proxy acts as a regulated barrier that hides the internal network from the outside. Additionally, configuring the Internet options of internal hosts to first point to the proxy server prior to surfing the internet allows the internal hosts to remain anonymous.

Proxy servers can also report capabilities and provide caching of frequently accessed websites. Most vendor proxy solutions can track website hits and use the collected data to store and report upon the information of websites visited by the users. Additionally, proxies allow for caching, which reduces internet bandwidth utilization because the most popular websites are saved by the proxy server. User connection requests are returned to the cached information rather than pulled from the Internet. The cache settings of a proxy server can be configured to refresh after several requests or a set time in order to pull new content and updates from the Internet.

Blocking or Filtering User Access to Websites

A proxy server without filtering is like a gateway that simply passes requests from the internal host computer to the Internet. However, a proxy server can be a very powerful boundary / perimeter security solution that acts like an internet gateway but also protects the internal network from outside threats. A gateway merely routes information from within the network to the outside, and without any enhanced next-gen firewall features, a gateway may expose the inside network to potential risks.

Unless it is part of a next-gen firewall solution with enhanced features, a gateway normally cannot block access to websites. A proxy server can block websites by redirecting user web requests to a website internal to the network. Also, with most vendor proxy solutions, administrators can block access to certain categories of websites. It is recommended to block certain categories of known websites that offer up extreme, sensitive, malicious, or sexually related content that would normally be considered unsuitable for sharing within the workplace. The proxy server can be configured so that when a user attempts to access a blocked website, they will be redirected to a customized page stating that that they are attempting to access a blocked website. The customized page can also provide additional information as to whom to

contact for further information if the user believes the site being blocked serves a legitimate business need.

Prior to blocking content from the internet, it is recommended to review and update any human resource policies or internet use policies currently in use across the organization. Creating a policy and implementing a proxy solution that prevents users from visiting inappropriate websites is the easiest solution. It is recommended to block internal network access to the following not sufficient for work (NSFW) website categories:

- Adult Content / Pornography
- Aggressive Behavior
- Controlled Substances
- Dating Sites
- Gambling
- Gaming
- Guns
- Intolerance & Hate Speech
- Malicious / Malware Sites
- Sexual
- Social Media
- Violence

Virtual Private Network (VPN)

A VPN is an encryption-based communication method that connects a remote office or worker to an organization's private network over a shared or public network. The encryption effectively makes a tunnel within the public network that data can pass through without being read by eavesdroppers. The end user's device and the server it is connecting to are the only devices able to decrypt the data. VPNs are commonly used by organizations that need to connect a remote worker or location to a more central private network.

An SSL VPN encrypts data using the SSL protocol, or its successor, transport layer security (TLS) protocol. Nearly all modern web browsers have begun to use SSL/TLS protocols when connecting users to websites. This means there is no need for specialized client software that users must download or run to establish a VPN connection. Therefore, an SSL VPN is also known as a clientless VPN. Several types of VPNs are available:

SSL Portal VPN

An SSL Portal VPN uses a single SSL connection to a gateway website that gives the user access to private network services. A user must only provide login credentials to use the SSL Portal VPN.

SSL Tunnel VPN

An SSL Tunnel VPN can access network services that are not necessarily web-based. A browser

that can interact with and display active content is required for an SSL Tunnel VPN. Active content includes JavaScript applications or interactive features.

IPSec VPN

IPSec is a suite of protocols for securing communications cryptographically. An IPsec VPN creates a tunnel where the client and server must negotiate the methods and parameters to secure the tunnel. Security associations are the one-way communication through which negotiations happen.

Virtual private network (VPN) best practices include researching which vendor matches an organization's needs, preparing for surges in use, keeping the VPN updated and patched, using multi-factor authentication for VPN connections, and avoiding free VPNs.

During March 2020, in response to the coronavirus pandemic, the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released alert AA20-073A for enterprise VPN security. The pandemic caused a significant spike in the number of employees working remotely and working from home. The CISA alert listed security threats associated with a large remote workforce. The threats connected to VPNs include:

- More vulnerabilities are found by malicious actors when organizations use VPNs.
- Organizations are less likely to keep VPNs updated with the latest security patches.
- Organizations may have a limited number of VPN connections, leaving some employees without one.

To mitigate these risks, CISA recommends implementing these VPN best practices:

- Update VPNs, network infrastructure devices, and remote employees' devices with the latest patches and configurations.
- Implement multi-factor authentication on all VPN connections or otherwise use strong passwords.
- IT security personnel should test VPN limitations in preparation for mass usage.
- If possible, security personnel should use tools like rate limiting to prioritize users requiring higher bandwidths.

Wi-Fi / Wireless Networks

Securing the Wi-Fi in use at the MSP organization is one vital component that helps to protect data and to ensure the security of critical business systems.

- **Change the Default Admin Password on the Wi-Fi Router**
  The default password for most every Wi-Fi router is easily found with a quick internet search. A Wi-Fi router with a default password is easy prey for a malicious hacker. Such access would allow an attacker to hijack the network and possibly launch additional attacks aimed at other companies through the compromised router. Additionally, a malicious hacker could easily change DNS settings to redirect those using the Wi-Fi to

fraudulent sites in an attempt to steal sensitive user information.

- **Update the Wi-Fi Router Firmware**
  Every piece of hardware or software requires updates and patches to fix known issues and expand additional features. Make it a plan to regularly update the Wi-Fi router's firmware to address any known bugs or security vulnerabilities. As an added benefit, many firmware fixes are often released to address performance issues. Some Wi-Fi routers can be configured to automatically download updates and the most recent firmware update may be found within the administrative console.

- **Create a Guest Wi-Fi Network**
  Do not allow your guests to join the same Wi-Fi network your employees use for production and daily operations. Establish a separate wireless network to minimize the risk of exposing internal systems to potential snooping or malware that may reside on the guest device.

Secure Email Gateway (SEG)

Email is the primary target hackers use to gain access to private company data. Email is often the least protected means of passing data into and within an organization. Modern methods of attacking email systems and users have grown in sophistication and the targeting of individuals. Organizations from all industries are facing an increasing number of targeted threats such as phishing attacks, ransomware, and malicious attachments.

Whether residing on-premises or within the cloud (Office 365, G-Suite), email and messaging gateways provide initial filtering and protect business operations from spam, viruses, malware, and potential denial of service attacks. Gateways scan incoming, outbound, and internal email communications for any sign of malicious attachments or URLs.

The following are core features to look for in a secure email gateway:

Spam Filtering

Spam filtering is the primary feature and function of a secure email gateway (SEG). All SEGs use some sort of SPAM filtering technology that blocks or quarantines items from known spam email domains. Advanced SPAM protection features may include algorithms to detect patterns that commonly appear in spam emails, such as keywords and malicious links, and help block new spam emails from entering email inboxes. It is recommended to receive as little SPAM as possible.

Virus and Malware Protection

Virus and malware scanning features are also common in many SEGs to help block items from infecting the organization's hosts and networks. By scanning attachments and embedded URLs, the malware protection engine within the SEG can identify and then quarantine messages containing malicious content.

Phishing Protection

In a phishing attack, an attacker uses email messages to trick a user into falling for a scam that may potentially reveal private or sensitive information (financials, passwords, credentials, etc.). SEGs may provide an organization with a certain level of protection against phishing attacks by catching and classifying suspicious emails. Using anti-fraud technologies in conjunction with reputation analysis, SEGs with phishing protection can spot and prevent several different spoofing techniques and attacks.

Admin Controls and Reporting

The administrative console of a SEG should allow for the configuration of policies and rules for the quarantine of suspect email items. Additionally, the console should allow for robust reporting and drill-down dashboards that provide insight into the use and protection of messaging across the entire organization.

No matter the size of an MSP organization, email is a prime target for attackers. A Secure Email Gateway is a security necessity to help protect business operations and critical data. Secure Email Gateways offer the most vital level of protection against compromise from malicious messages and attachments. Using a Secure Email Gateway is an easy way for organizations to enhance their security posture.

Intrusion Detection & Protection Systems

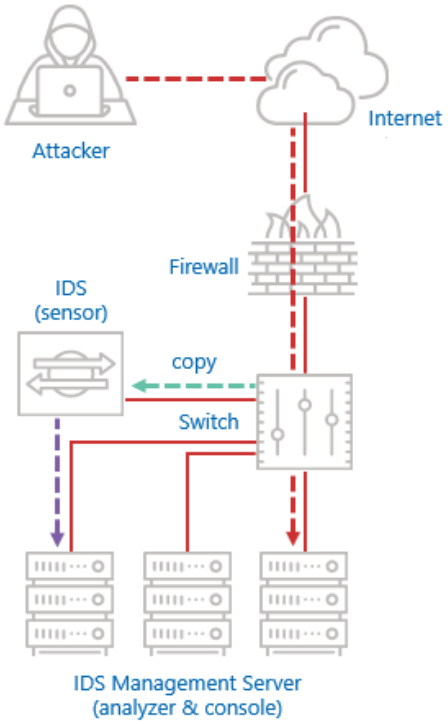
Intrusion Detection Systems (IDS) work in conjunction with routers and firewalls to monitor network usage abnormalities. A solution can be put in place to protect an organization's IT resources from both external and internal issues and misuse. An IDS continuously monitors the network or a host and notifies administrators when a perceived threat is detected. The two broad categories of IDS include:

Network-Based IDS

Network-based IDS systems are configured to identify potential attacks within a monitored network and can issue a warning to an administrator. A network-based IDS placed between the Internet and the firewall will detect all attack attempts prior to entering the firewall. If the IDS is placed between a firewall and the internal business network, it will detect attacks that pass through the firewall and send warning of a potential intruder. An IDS is not designed to replace a firewall but rather to provide a complementary function by way of validation checking a firewall policy.

Host-Based IDS

A host-based IDS system is a software application designed to work in a specific environment (Android, Linux, Windows, etc.) and monitor internal resources of the operating system to warn an operator of an attack. These host-based sensors are configured for a specific environment and monitor various host resources and processes of the operating system to warn administrators of a possible attack. Host-based IDS sensors can detect modification or execution of files and then issue a warning when an attempt is made to run a privileged command.



Components of an IDS Solution

The main components of a network-based IDS are:

- Sensors for collecting data in the form of network packets, log files, system call traces, etc.
- Analyzers to examine input from the sensors and determine intrusive activity.
- Administrative console to view dashboards, analyze alerts, produce reports, and configure detection rules.

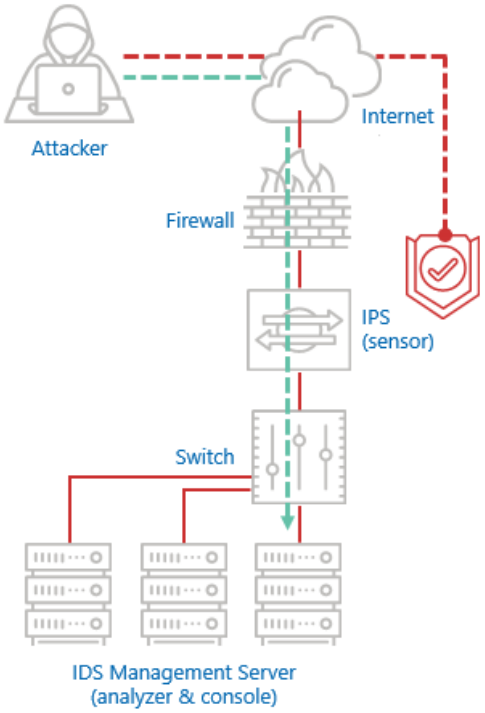
IDS can perform intrusion detection and gathering of evidence of intrusions, but it is not useful if policy definitions are weak or if existing back doors in applications are being used in the attack.

Intrusion Prevention Systems (IPS)

Like an IDS, an IPS is designed to not only detect attacks, but also to prevent the intended hosts from being affected by the attacks. An IPS solution complements most firewall, antivirus, and antispyware tools by providing additional protection from new and emerging threats.

When placed at the perimeter of the network boundary (egress and ingress points), an IPS solution works by examining network traffic flows and preventing attacks, such as worms or network aware malware. By adopting and properly managing an IPS solution, an MSP organization can ensure that network-based attacks are blocked at the perimeter.

The major advantage of an IPS over an IDP is that an IPS can help block an attack when it occurs. Rather than simply sending an alert, an IPS actively attempts to block malicious and unwanted traffic.



IPS in Action

As depicted in the preceding diagram, legitimate traffic is allowed but malicious packets can be blocked inline before the attack reaches the target.

Host / System Protection

Every organization faces security threats. Often, the weakest link in security is the human element. When humans operate computers, anything can happen. To protect end users and host computers, an MSP organization must address many types of security threats.

Secure Configuration / System Hardening

Hardening limits the attack vectors that can be used as a point of compromise. System hardening is the process of implementing security controls on a computer system to prevent the controls set to open by default from being a significant vulnerability. A hardened system limits storage of sensitive data and has unnecessary functions disabled. Such functions may include ports, services, and protocols that are not required for the intended use of the system within the enterprise environment.

Most systems come with a known guest account or default password. Such known elements should be changed or disabled prior to production use. It is common for most computer vendors to set the default controls to open to allow ease of use over security. This introduces

significant vulnerabilities unless the system is hardened. The process of determining what is hardened and to what level varies based on the operating system, installed applications, system/platform use, and exposure. The exact controls available for hardening may vary.

Controls commonly used to harden a system include:

- File system permissions
- Access privileges
- System services
- Configuration restrictions
- Authentication and authorization
- Logging and system monitoring

Regardless of the specific operating system, system hardening should implement the principle of least privilege or access control. Prior to making changes, administrators should fully understand the types and roles of accounts on each platform they are configuring for protection.

Additionally, server hardening is an important practice designed to protect an organization's servers from attack. Microsoft Windows servers will require a different method and script compared to UNIX/Linux server operating systems.

In Windows systems, the Registry is a database that stores configuration options and settings as keys and values, with most of this data stored in the %SystemRoot%\System32\Config directory. Major keys and values are:

- HKEY_CURRENT_CONFIG: Contains volatile information generated at boot.
- HKEY_CURRENT_USER: Contains settings specific to the current user.
- HKEY_LOCAL_MACHINE\SAM: Contains local and domain account information.

UNIX/Linux has special directories that store critical information and should be given extra consideration when hardening the server. Note that this is a non-exhaustive list:

- /etc/passwd: Maintains user and password information.
- /etc/shadow: Stores an encrypted copy of the user accounts in /etc/passwd.
- /etc/group: Contains group information for every account.
- /kernel: Contains the core kernel files.

For an administrator, identifying the location of critical information is imperative to security and is key for incident response.

The following sources offer additional guidance on the secure hardening of systems to help mitigate potential risk to systems and services provided by the organization. Prior to

implementing any such changes within a production environment, it is a highly recommended to test any changes and assess their impact.

NSA CSS Cybersecurity Advisories & Technical Guidance

The NSA develops and distributes configuration guidance for variety of software, both open source and proprietary. The NSA does not favor or promote a specific software product or business model. Rather, they promote enhanced security. Fortunately, the NSA has leveraged its elite technical capability to develop advisories and mitigations on evolving cybersecurity threats and has shared their guidance with the public.
Link: https://www.nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance/

Program Clean Up

Remove unnecessary programs. Every program installed on a host endpoint or server operating system is another avenue of potential entrance for a hacker. Removing unnecessary or unneeded programs helps to limit the number of ways into a system. If the program has not been vetted by the organization and has not been "locked down," then it should not be allowed for install on the server or host computer. Attackers look for backdoors and security holes when attempting to compromise networks. Removing extra software helps to minimize their chances of breaching an organization's systems.

Use Service Packs

Hardening systems and software includes keeping them up-to-date and installing the latest versions. This is a very simple task and should be considered a best practice. Providing security across all systems cannot be accomplished by simply turning on a single tool, especially when dealing with new and emerging zero-day attacks. However, patching and applying service packs to servers and host operating systems is an easy policy and practice to put in place.

Patching and Patch Management

A regular part of the security routine should involve the planning, testing, implementing, and auditing of patches through an automated patch management software. At a minimum, an MSP organization should ensure that the server and host operating systems, as well as the individual software programs on the client's computer, are patched on a regular schedule. Patching and vulnerability awareness are covered in more detail with this document.

Use Group Policies within Microsoft Active Directory

It is recommended to clearly define what groups can access and maintain Microsoft Active Directory groups and rules. Occasionally, issues may arise due to simple user error that can open the gateway for a successful cyber-attack. At a minimum, define and enforce a policy to make all users implement strong passwords, secure their credentials, and change them on a regular basis. Additionally, IT administrators can establish or update user group policy objects (GPOs) to ensure all users are aware and comply with these procedures.

Security Templates & Baselines

Templates and baselines are commonly used in corporate environments. Use templates to load groups of policies in one procedure. Microsoft has a Group Policy Settings Reference Guide for Windows and Widows Server (Link: https://www.microsoft.com/en-us/download/details.aspx?id=25250) and a great reference for managing and deploying Microsoft Windows 10 (Link: https://docs.microsoft.com/en-us/windows/deployment/deploy-whats-new). Additionally, adopt a Microsoft security baseline. A baseline is a group of Microsoft-recommended configuration settings that explains their security impact based upon feedback from Microsoft security engineering teams, product groups, partners, and customers (Link: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines).

Microsoft Office Macros

Configure the Microsoft Office Macro settings to prevent uncontrolled macros from running. This will significantly reduce the organization's attack surface and improve the security of all end-user workstations, regardless of operating system. Microsoft Office files can contain macros built upon the Visual Basic for Applications (VBA) programming language. Normally, such macros are designed to aid with automated tasks. However, malicious attackers can use social engineering and phishing techniques to trick a user into opening a file that contains a scripted attack within its embedded macros. As part of their Essential Eight elements to protect against cyber-attacks, the Australian Cyber Security Centre (ACSC) recommends establishing policy and procedures to protect against malicious macros.
Link: https://www.cyber.gov.au/publications/microsoft-office-macro-security

Access Control

The fundamental use of accounts and passwords is the primary way that many organizations allow access to the mobile devices, workstations, laptops, servers, applications, websites, and cloud-based services. Because the simple combination of a user ID and a password often allows a user access to systems and critical information throughout the organization, it is imperative that policies and processes are in place to ensure that only authorized individuals have active user accounts.

User accounts should only be granted the minimum amount of access (least privileged) that is required for the individual to perform their required job function. By adopting a stance of least privileged access, organizations can greatly reduce the risk of information being stolen, exposed, or damaged. Defining the roles and responsibilities of each job function is a recommended practice that can help to limit user rights and access to services and critical data.

In addition to the regular credentials assigned to individuals for everyday use, organizations will also have administrative, or privileged, accounts that carry elevated access and enhanced privileges to systems, applications, services, and information. These privileged accounts are often assigned to systems administrators to use for managing and maintaining services provided to both internal users and customers. In a Microsoft Windows Active Directory

environment, these privileged users will likely be part of the Domain Administrators and Local Administrators groups.

An MSP organization should take care with the provisioning and use of privileged accounts. Privileged accounts with elevated access should not be used to perform daily activities that require the use of email and internet browsing. Because hackers have demonstrated a consistent and ongoing ability to obtain access to host systems inside the network boundary through phishing, web browsing, and other email attacks, privileged accounts remain high-value targets of compromise.

When securing user accounts, service accounts, and privileged accounts, it is critical for the MSP organization to actively manage the lifecycle of user accounts from creation and daily use to deletion. To minimize opportunities for attackers to leverage account credentials, consider the following recommendations:

- Do not share accounts. Ensure that all accounts are associated with an identity or owner with an active user, a privileged user, or a service account.
- Separate privileged accounts and limit their use for normal office productivity tasks.
- Do not share administrative or privileged accounts.
- Immediately disable employee or contractor account access upon termination.
- Monitor daily user activity for oddities, patterns, and trends.
- Audit logs for successful and failed login attempts for systems or services.
- Implement multi-factor authentication wherever possible.
- Enforce strong and complex password policies.
- Review privileged access assignments (at least annually) and document all changes.

Patch Operating Systems (OS)

Legacy systems running on operating systems that are no longer supported by the vender may place the MSP organization at risk of compromise. At a minimum, the system administrators and network personnel should ensure that all software is up-to-date, properly licensed, and fully supported. Legacy systems should be carefully analyzed, and IT teams should commit to the following:

- Create a comprehensive inventory of host systems.
- Invest in upgrades.
- Patch vulnerabilities regularly.

Vulnerabilities are frequently discovered in software programs, including the host operating system. Once discovered, malicious individuals or groups quickly organize to take advantage of the opportunity to exploit newly published vulnerabilities and attack computers and networks with these weaknesses.

It is recommended to only run current, vendor-supported operating systems for which security patches are made available in a regular and timely fashion. Upon their release by the vendor,

available security patches should be tested and then applied to production systems on a schedule appropriate to the severity of the risk they mitigate.

Many patches are assigned a risk score from by the National Vulnerability Database (NVD) utilizing the Common Vulnerability Scoring System (CVSS). The CVSS is an open framework for communicating the characteristics and severity of software vulnerabilities and providing a recommend schedule for organizations to address patches deemed high or critical. It is recommended to remediate or patch critical vulnerabilities within 48 hours of the initial publication of the vulnerability alert and to address high vulnerabilities within 7 days. For critical vulnerabilities that have a direct impact on the organization, be sure to prioritize the patching of Internet-facing systems where public services are vulnerable.

Consider the following questions when assessing the risks that a newly published vulnerability may pose to business operations and creating a patch schedule:

Likelihood of the Vulnerability Leading to Compromise

- Has a working exploit code been published and publicly known?
- Has an exploitation been publicly or privately observed?

Exposure of Existing Systems or Services

- Are the vulnerable systems or services Internet-accessible?
- Are the vulnerable systems or services open to all hosts on the internal network or open to only specific, authorized hosts?

Context of the Vulnerability in the Form of an Attack against the Organization

- How severe does the vendor or the CERTs rate the vulnerability?
- Is the attack complexity considered to be high or low?
- What kind of impact will result? (confidentiality, integrity, or availability)
- How difficult would it be for existing security solutions to detect an ongoing attack exploiting the vulnerability?
- Is there protected, sensitive, or restricted data on the system?

Mitigation of the Vulnerability without an Available Patch from the Vendor

- Are there any verified workarounds or temporary solutions that can quickly be implemented until a full patch release from the vendor can occur?

Understand that patching is an ongoing, recurring activity that will always need to be addressed. Throughout the organization, IT systems and application owners should maintain a patch management plan and coordinate activities with both business operations, technical stakeholders, and possibly customers.

Patch Applications

A robust security program that implements security processes into each phase of the software development lifecycle can reduce the overall risk to the organization. Aspects of security should be a concern at any of the development, testing, and implementation phases. By incorporating security from the start of a software development lifecycle, major flaws in design, development, and implementation can be identified and remediated early in the process, reducing risk and cost to an organization in the future.

Vulnerabilities are frequently discovered in software programs, including the host operating system. Once discovered, malicious individuals or groups quickly organize to take advantage of the opportunity to exploit newly published vulnerabilities and attack computers and networks with these weaknesses. Additionally, malicious actors can take advantage of vulnerabilities in web-based applications by performing injection exploits—including buffer overflows, SQL injection attacks, cross-site scripting, and click-jacking of code—to gain control over vulnerable machines.

It is a core security best practice to only run current, vendor supported software applications for which security patches are made available in a regular and timely fashion. Upon their release by the vendor, available security patches should be properly tested and then applied to production systems on a schedule appropriate to the severity of the risk they mitigate. Never test on production systems.

Security Software & Malware Protection

Malware is short for malicious software and is an encompassing, catch-all term that describes any malicious program or code that is harmful to systems.

Malware is the hostile, intrusive, and intentionally nasty software code that seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations. Malware is designed to infiltrate, damage, or obtain information from a computer system without the owner's consent.

Terms associated with malware include the following:

- **Computer Virus:** A malicious piece of code that infects an existing file on a system and gets propagated when the infected file is used or accessed.
- **Worm:** A malicious piece of code that, when executed, propagates itself and infects multiple systems in a short space of time. Unlike a virus, a worm is an independent program that does not rely on an existing file on a system.
- **Trojan Horse:** Malicious code that is hidden on a single system and does not replicate, but can be as destructive as a virus or worm on a system.
- **Spyware:** Software designed to monitor a user's actions and report this information to a third party without consent of the user of the system. For example, a keylogger that

reads keystrokes and sends this information to a third party with the intent to obtain passwords and other sensitive information.

- **Adware:** Software that plays, displays, or downloads advertising material to a system after software has been installed or while software is being used. This is not malicious but is done without the user's consent.
- **Ransomware:** A form of malware that locks users out of their device and/or encrypts their files, then forces the user to pay a ransom to get them back.

Other types of cyberattacks include:

- **Advanced Persistent Threats (APTs):** Complex and coordinated attacks directed at a specific entity.
- **Backdoor:** Regaining access to a compromised system by installing software.
- **Brute Force Attack:** Trying all possible combinations of passwords or encryption keys.
- **Buffer Overflow:** Forcing a program or process to store more data in a buffer (temporary data storage area) than it was intended to hold.
- **Cross-Site Scripting (XSS):** Malicious code is injected into a website without being validated or encoded and sent to a different user.
- **Denial of Service (DoS) Attack:** A single source floods a system with so many requests that it becomes overwhelmed.
- **Distributed Denial of Service (DDoS) Attack:** Multiple sources flood a system with so many requests that it becomes overwhelmed.
- **Man-in-the-Middle Attack:** An attack strategy in which the attacker intercepts the communication stream between two parts of the victim system.
- **Social Engineering:** Any attempt to exploit social vulnerabilities to gain access to information.
- **Phishing:** Email attack that attempts to convince a user that the originator is genuine.
- **Spear Phishing:** Social engineering techniques are used to masquerade as a trusted party to obtain important information.
- **Spoofing:** Faking the sending address of a transmission.
- **Structure Query Language (SQL) Injection:** insertion or 'injection' of a SQL query via the input data from the client to the application.
- **Zero-Day Exploit:** A vulnerability that is exploited before the software vendor is aware of it.

If a system is infected with malware, the organization is likely to suffer from problems like slow system response, malfunctioning systems, data loss, or hidden infection that goes unseen until it causes harm elsewhere. Malware problems can largely be avoided by using any of the various

means of protection available. It is recommended to look toward a vendor with an endpoint protection platform that offers the following protection capabilities.

Anti-Malware Software

Detecting and disabling malware before it causes harm.

- Anti-Malware software must be kept up-to-date, with signature or data files updated daily at a minimum. Updates may be achieved through automated updates or with a centrally managed deployment.
- The software is configured to automatically scan files upon access. File scanning should include when files are downloaded and opened and when they are accessed from a network folder.
- The software can automatically scan web pages for malicious content and downloads when sites are accessed through a web browser.
- The software can blacklist and prevent connections to malicious websites on the Internet unless there is a clear, documented business need and the associated risk is understood and accepted by the organization.

Application Whitelisting

Executing only software that is known to be worthy of trust.

- Only approved applications, restricted by code signing, can execute on host systems.
- Applications are approved prior to deploying them to host systems.
- IT and business operations should maintain a current list of approved applications.
- Restrict users from installing any unauthorized applications.

Application Sandboxing

Executing untrusted software in an environment that controls access to other data. All code of unknown origin should be run in a sandbox environment to prevent and limit access to other host resources unless explicit permission is granted by the user. This includes:

- Other sandboxed applications
- Data stores (documents, photos, files)
- Sensitive peripherals (mic, camera, USB attached items)
- Local network access

Host-based Firewall / IPS

Use a host-based firewall on devices that are used on untrusted networks, such as public Wi-Fi hotspots. Host firewalls operate like boundary firewalls but only protect the single device on which it is configured. Host firewalls offer a more tailored approach to policy rules and provide the means to apply different policy rules to the device when it connects from different locations (in the office, at a hotel or at coffee shop, etc.).

Event Log Collection

A lack of security logging and analysis within an organization enables attackers to hide their location and activities in the network. Organizations must collect, manage, and analyze event logs to detect unusual, anomalous activities and to investigate security incidents. Without security logs, it is difficult to understand what an attacker may have compromised and to effectively respond to the security incident, even if the victim organization knows which systems have been compromised.

Within many organizations, most breaches are not initially detected and may not be discovered until several months after the initial attack. Often, breaches are only detected after it is discovered that compromised sensitive information has been released or is for sale on the dark web. Normally, when data is being exfiltrated from the system during an attack, the security staff responsible for monitoring system logs would be alerted by some obvious indicators.

Event data is best collected and correlated from multiple sources and sensors, including:

- Syslog (no correlation)
- SIEM or MDR Solutions (correlation)
- Procedure or Policy on Log Settings for Different Sources

It is recommended to store the event log history in a secure location and to ensure that the logs are stored for long enough to aid in forensics.

What to Log

When it comes to logging, no one size fits all solutions. Turning on too much can result in "alarm fog" and legitimate attack notifications may get lost in the noise and go undetected. However, OWASP and NIST offer guidance for security log management. They provide recommendations for collecting, managing, and analyzing audit logs to tune the analysis and better identify events that could help detect, understand, or recover from an ongoing cyber-attack. OWASP recommends generating and collecting the following logs for analysis:

- Embedded instrumentation code
- Network firewalls
- Network and host intrusion detection systems (NIDS and HIDS)
- Closely related applications (e.g., filters built into web server software, web server URL redirects/rewrites to scripted custom error pages and handlers)
- Application firewalls (e.g., filters, guards, XML gateways, database firewalls, web application firewalls)
- Database applications (e.g., automatic audit trails, trigger-based actions)
- Reputation monitoring services (e.g., uptime or malware monitoring)
- Other applications (e.g., fraud monitoring, CRM)

- Operating system (e.g., mobile platform)

Additionally, it is recommended to always log the following events:

- Input validation failures (e.g., protocol violations, unacceptable encodings, invalid parameter names and values)
- Output validation failures (e.g., database record set mismatch, invalid data encoding)
- Authentication successes and failures
- Authorization (access control) failures
- Session management failures (e.g., cookie session identification value modification)
- Application errors and system events (e.g., syntax and runtime errors, connectivity problems, performance issues, third party service error messages, file system errors, file upload virus detection, configuration changes)
- Application and related systems startups, shutdowns, and logging initialization (starting, stopping, or pausing)

It is recommended to regularly perform testing and validation activities to confirm that logging policies, processes, and procedures are being followed at both the infrastructure and system levels throughout the organization. Organizations should also periodically review the design of the log management infrastructure and implement changes as needed. Periodic reviews of log management processes and procedures should also be conducted so that log management continues to be effective at detecting the latest threats in changing environments.

SEIM - Where to Log

For some organizations, log management can be hard to master. Obtaining logs from various IT servers and systems can be taxing on the assigned workforce personnel. Additionally, having processes in place to ensure that collected log data is accurate, holds the information required to make informed decisions, or contains the data to alert on any suspicious activity can prove to be even more difficult without the use of automation and specialized software.

The adoption of SIEM technology is the foundation to implementing an effective log management program. While it may be possible to detect malicious behavior by analyzing raw log data, a SIEM greatly reduces the amount of time and effort involved in analysis and can increase the effectiveness of logs. A SIEM can easily perform a variety of actions that reduce the amount of manual effort and can increase both the effectiveness of the logs and the overall productivity of the workforce personnel assigned to the log analysis task.

SIEM software or appliances collect and aggregate log data generated throughout an organization's technology infrastructure. This can include log data from host systems and applications, network and security devices such as firewalls, and security tools. A SIEM can normally perform many of the following tasks:

- Normalization of log data fields

- Normalization of log time
- Event and Incident categorization
- Event notifications
- Alarm notifications when an event has occurred
- Automatic log collection

After a SIEM has been deployed, IT systems and security platforms capable of logging should be configured to forward their logs to the SIEM. These logs include:

- Firewalls logs
- IDS/IPS systems logs
- Proxy logs
- System logs

Monitoring

With logs being collated and analysed by the SIEM, it is possible to start defining specific events and alarms to alert staff of potential malicious activities. Automated alerts can be extremely helpful. Additionally, having a knowledgeable, well-trained staff who can periodically review logs and alerts to hunt for potential attacks may prove valuable to the organization. Assigned workforce personnel should have a documented process for following up on any identified incidents and workflows for configuring new event rules and alerts within the SIEM platform to detect similar incidents in the future.

Implementing analysis techniques and workflows designed to customize alerts based upon what normal network activity looks like can greatly assist with identifying a successful or an unsuccessful attack. With a combination of the SIEM and talented personnel providing monitoring, the organization may be able to proactively react to an in-progress cyber-attack and stop it. This would place the organization in a much better position as opposed to that of a case where data had been exfiltrated and exposed. The natural evolution for an organization with enhanced monitoring capabilities is to mature and develop a proper incident response program. The program should include documented plans, clearly defined roles, staff training, executive management oversight, and other security measures designed to aid in the discovery and effective containment of cyber-attacks.

Unfortunately, in most cases, the chance of a successful cyberattack is not “if” but “when.” Responding to security incidents has become a normal part of the daily operations of many organizations. This holds especially true for MSPs and their SMB customers. Even large, well-funded enterprises barely keep up with the ever-evolving cyber threat landscape of new and emerging threats. An organization operating without documented incident response plans or processes may go weeks, if not months, before realizing that an attack has compromised their systems and caused serious harm to their environment. In such cases, a compromised

organization may not be able to block or eradicate the attacker's presence and find themselves hard pressed to restore the integrity of their network and systems.

Following are recommended best practices to consider when beginning to develop an incident response program:

- Deploy monitoring agents, endpoint security products, and log correlation and collection technologies to enable detective and forensic capabilities.
- Perform 24x7 monitoring and analysis of event data through local or managed security services providers.
- Explicitly define procedures and roles and communicate to relevant workforce personnel any actions and expectations to rapidly triage events without confusion or conflict.
- Perform periodic table-top walkthroughs, reviews, and live exercises to adapt the policies and procedures to new and emerging threats and changes to the environment.
- Use post-mortem analysis to identify deficiencies and influence necessary security spend.

Security Awareness Training

Every MSP must offer training and coaching to their workforce personnel on a variety of security risks and safe computing practices. Much of this training can be conducted in-house by security professionals or outsourced security awareness training partners that may offer online programs tailored to the needs of the organization. Such courses provide employees and contractors with a basic understanding of the potential physical and cybersecurity threats they may face in the workplace and how to respond to such threats.

Phishing

The keys to identifying phishing emails are to train on what to look for and to encourage users to pause and review incoming emails for these indicators before acting. The following are the top things to look for in phishing emails:

- The message is sent from a public email domain. For example, no legitimate organization will contact a user from an address that ends '@gmail.com'.
- The domain name is misspelled, unfamiliar, or does not match the company that would be sending the email.
- The email is poorly written or seems too personal in referencing the recipient.
- The email includes suspicious attachments and links or an attachment that was not expected.
- The message creates a sense of urgency.

It is recommended to use a service to randomly test users on their ability to identify phishing emails monthly to help determine where additional training should be focused.

Privileged Users and Administrators

Privileged users hold the "keys to the kingdom". It is imperative to train and control use of that access. Privileged credentials can give an attacker access to reams of corporate information or to multiple end client sites, destroying the MSP's reputation and wreaking havoc for multiple businesses at one time. Sensitive client information, finances, and intellectual property are often at risk in the hands of individuals who require specialized training. Effective privileged user training includes:

- Identifying who the privileged users are and what type of resources they access.
- Understanding how to mitigate insider threats.
- What are the prohibited actions?
- Management and auditing of access by privileged users.
- Clearly defined consequences of non-compliance.

Social Networks

Training users to understand what kind of information posted on social networks might adversely affect the organization's reputation or the individual's privacy is an important part of security awareness. Hackers search for public information on social networks to help piece together social engineering components like family and friend names, social networks, pets' names, birthdays, hobbies, vacations, and availability. Limiting disclosure of this information is an informed choice the users should make to protect their own privacy and security as well as the organization's security. Additionally, it is recommended to have clear policies on what type of company-related information is acceptable to post on social platforms. For example, during a security breach, ensuring sensitive information is not posted publicly by employees will aid in the ability of the organization to appropriately follow the communications plan in the incident response policy.

Social Engineering

Social Engineering is a psychological attack where a hacker takes advantage of a user to provide information or to take an action that allows a breach to occur. Social engineering basically boils down to the old con game, wherein an unsuspecting target who wants to be helpful is lured into behavior that compromises assumed protection of some resource or asset. The most common social engineering unfolds into an attack known as CEO Fraud. In these attacks, a hacker successfully poses as someone of trust or leadership at an organization and carries out an attack to exfiltrate data, extort money, or compromise the reputation of an organization. Social engineering occurs most often via phone and email, but can also occur via text, social media, or in person.

Most social engineering activities can be identified by watching for things like:

- Requests with great urgency to have the victim rush to assist.
- Requiring a password to complete an activity, where the user is not aware the password is being provided to a threat actor.

- Pressure to bypass normal protocol or security.
- The offer of receiving something too good to be true.
- Someone who asks for information they should already know or have access to.
- A request from someone familiar that sounds unlike their normal way of speaking or writing.

Malware

Cyber criminals use malware to infect computers in many ways. Malware is a malicious computer program that allows the threat actor to do whatever they want to the device. Often, this means deploying ransomware, key loggers, or remote monitoring or exfiltrating data. Malware can be deployed on mobile devices, Macs and PCs, and internet-based devices such as home security cameras or online video and audio content.

It is important to train users to understand how malware infects computers or devices and what to avoid. This includes avoiding infected or suspect websites, detecting phishing emails, blocking access to USB ports on company owned computers, keeping devices updated with current security patches and anti-malware protection, and more.

Passwords

Passwords provide access to an organization's most sensitive information. However, employees are typically not trained on the following recommended practices:

- Creating strong passwords.
- Safely storing passwords.
- Creating a unique password for each site and resource they have access to.
- Knowing when to use multi-factor authentication with a password.

In addition to having a password management policy, users should be taught best practices for password management not only for organizational protection, but also for their own privacy and security.

Mobile Devices

Mobile devices are increasingly relied upon to boost communication and productivity in MSP environments. Securing these devices and providing training on best practices for privacy and security often takes a back seat to the drive for processing requests efficiently. The most important aspects to consider within a mobile device security awareness program are:

- Securing access with password, passcode, or biometrics.
- Keeping the OS updated.
- Having the ability to track and remotely wipe (if necessary) a lost or stolen device.
- Reviewing and proper setting of privacy options.
- Backing up the device.
- Installing trusted apps only.
- Limiting or prohibiting the ability to photograph or record sensitive information.

Browsing Safely

Ensure that users are practicing safe browsing and that only well-known or trusted sites are being visited. Because even trusted sites can be hacked, it is important to consider the following recommendations for web browsing:

- Use the latest version of your internet browser and keep it up to date.
- Watch for warnings on the browser toolbar or interface.
- Make sure you understand how a domain is constructed and how to determine if the URL of a website is correct before clicking.
- In general, avoid clicking ads on websites, even on trusted websites, as they are often not filtered for malicious content by the website owners.
- Select a default browser that has a good reputation. The most common are Mozilla Firefox, Google Chrome, and Microsoft Edge.

Data Security

Data security awareness training focuses on key practices like data encryption, password management, social engineering, safe web surfing, trusted software, physical access, remote access, data disposal, and phishing. Data security encompasses many related security awareness topics and plays a crucial role in preventing breaches.

Backup Solution (Critical Systems)

One of the most known and least implemented security controls is data recovery, or specifically data backups. An organization may have many processes and utilities for backing up critical information. In smaller organizations where data backup and recovery are functions of the IT team rather than a separate department, a backup solution with a proven methodology that includes the timely recovery of critical information is especially important.

At a minimum, MSPs should perform backups of important information, software, and configuration settings of critical systems on a monthly basis. Those backups should be stored for one to three months and should be periodically tested for data restoration on an annual or more frequent basis.

What to Back Up

Within the MSP, data owners, systems administrators, IT managers, and department heads should work together to identify and draw a correlation to existing systems and applications to determine backup priorities. For example:

Which departments and data are the most important to restore first?

- Finance systems
- Business systems
- Operations
- Customer Service
- Marketing and Sales

- Information Technology

What to regularly back up?

- ERP
- EMR/EHR (Healthcare)
- Email (Exchange/O365)
- File Servers or file systems themselves
- Actual servers, workstations, laptops, etc.

3/2/1 Backup Solution

As the number of locations an organization stores its data increases, the concept of the 3/2/1 model often gets forgotten. The 3/2/1 model is the foundational concept of design when it comes to backups and managing data protection across an organization. The 3/2/1 model indicates that the organization should maintain three copies of the data stored on two different types of media with one copy stored offline.

Three Copies of Data

An organization should always have at least three distinct copies of their important data. First, an organization will have a production copy of their data that is live, running, stored, or used by workforce personnel and customers to conduct business operations. However, a good backup solution should have at least three different versions of the data saved over different periods of time. These snapshots ensure that the organization can recover from accidental data deletion or corruption that affects multiple versions of the backup library. It is recommended to keep more than three copies.

Two Storage Devices / Media

It is recommended to preserve at least two copies of data on separate storage devices that are physically independent. For example, one copy of the backup could be stored on a local server within the local datacenter in the office and a second copy could be made to an attached external USB drive and then locked in a fireproof safe. Having two different physical media is import in case of hardware failure or accidental data wipes. Additionally, some ransomware attacks use the host to scan mapped network drives and locate known backup files to eradicate or encrypt them. In such a case, having secondary backup media that does not reside on the network would be a proverbial lifesaver for the organization.

By separating these two backup copies in as many ways as possible, an organization can better protect itself against an attacker compromising both the primary and the secondary backup media. Consider adopting any (and possibly all) of the following recommendations:

Different Storage

Use a different storage type than what is used for the primary storage. An attack designed for one solution may not work on the other solution.

Segmented Environment

Use a backup system that is not directly attached or reachable via the local area network (LAN). Segmentation and the use of VLANs can help prevent compromised on-premises servers from attacking or corrupting the backups stored on a different network.

Different OS

Because most ransomware attacks have been designed to run against Microsoft Windows operating systems, consider a backup server or service that runs on a Linux platform.

Different Account

Have different (non-user and non-system administrator) credentials assigned to the backup and disaster-recovery systems. If a user account becomes compromised, then their credentials will not work to elevate an attack on the backup solution.

Immutable Storage

Consider off-site and cloud storage solutions. Many vendors offer a hosted service for immutable storage. Backups sent to their immutable storage solution cannot be changed or deleted until a set specified time. This solution also allows the organization to have a copy of their backup data stored off-site.

One Data Copy Offline

At least one copy of an organization's backup data should be stored in a separate off-site location that is physically located in a different facility, such as another office location, a third-party data vault, or a cloud-based data center. Additionally, having the data backups stored in an off-site or remote location ensures that in the unforeseen event of a man-made, natural, or geographical disaster, the impact will not affect all backup copies. When practical, this backup should be stored offline. It could be a port that gets disabled on a managed switch and isolates the backup or a purely offline backup run manually on a regular basis.

Testing of Backup & Restore

It is important to regularly test backup restoration procedures. This process involves regularly testing backup media for reliability and testing the recovery procedure to ensure that during a disaster, the process has been verified and can be replicated quickly and with minimal errors.

A good data recovery practice can be the difference between a successful cyber or ransomware attack causing massive data loss or minor downtime. In general, most cyber-attacks are focused on the compromise of data rather than the destruction of data. However, this is not always the case, especially with ransomware, a notoriously malicious extortion attack that encrypts and destroys data. Because ransomware attacks have proven to be a very successful and lucrative business model for attackers, expect to see an increase in the frequency and sophistication of these attacks across the MSP industry and with the SMB clients they serve.

Having a good data recovery practice is one of the best ways for an organization to combat ransomware. Backups are important not only to safeguard data, but also to recover the data that was encrypted via ransomware. Backing up data does not ensure its integrity and availability. Backups must be properly restored. In the event of a malware or ransomware infection, it is recommended for restoration procedures to use a version of the backup that is believed to predate the original infection.

Backup Best Practice

Consider the following recommendations for managing and conducting backups across the organization:

- Keep a hard copy of documented procedures and contact information in a separate secure location.
- Update the procedures and contact information regularly (quarterly) to incorporate any changes in SaaS, data or applications added, and workforce personnel involved.
- Ensure the backup plan includes a priority restore list.
- Ensure the backup systems are isolated and are regularly tested.
- If a local backup is required, consider putting it in cloud space using separate credentials along with multi-factor authentication (MFA).
- Ensure cloud backups have separate MFA-enabled credentials to help prevent the backups stored there from becoming encrypted or disabled.
- Test the time it takes to perform a restore from the backup systems.
- Vendor solution caveats and recommended best practices will vary greatly.
- If restoring from a cloud-hosted solution, identify any risks and plan for any potential bandwidth limitations.
- At least twice monthly, manually check and verify backup success or failure (even if the console is reporting a status green).
- Document the methodology and any specific server, drive, or file names used for testing the restoration process or on service tickets (make the notation within the ticket).
- If an incident occurs, restart the backup routine ASAP.
- Back up everything, even encrypted or infected computers as they may still be recoverable at later date.

Security Metrics

This section of the Yellow Book discusses why measuring the security controls of an organization is important and describes how to implement a baseline of metrics that make sense for your organization. Different industries require different measurement activities. For the foundational series, we are going to cover a broad range of metrics across some of your security controls. These metrics should be considered the baseline, must-have for every organization. If your MSP has additional compliance requirements for measurements, like HITRUST, PCI, or any other, then you will need to keep those metrics.

What are Security Metrics and Why Should I Care?

Simply defined, security metrics are ways organizations can judge the effectiveness of the security controls within the environment. These metrics are used by leadership to make informed decisions about the organization's security posture and ensure the controls put in place are still effective. Larger MSPs may wish to measure at different levels of the organization, choosing then to roll up the information at the executive level. This is certainly an acceptable practice and can be very useful for those MSP partners who have more than one location, as an example. Each local office has a set of measurements for themselves to evaluate and make decisions, while the numbers from all of the sites are collected as part of the larger organization and reviewed to make decisions from more of a top-down approach.

Budgets are oftentimes influenced by these measurements to ensure gaps in security controls are funded and resolved based upon the risk the gaps pose to the organization. By measuring the controls, gaps become very apparent. This leads to the questions, what is the impact to the business and what is the priority to resolve the gaps? At which point, the leadership and budget owners can determine how best to proceed. The gaps should be captured in a plan of actions and milestones along with the risk, impact, and priority.

Plan of Action and Milestones

As mentioned previously in the Security Program section, a Plan of Action and Mitigation (POAM) is designed to help MSP organizations identify, assess, prioritize, and monitor the efforts to correct and mitigate any security weaknesses, deficiencies, or vulnerabilities identified within programs and systems. As a tool, the POAM:

- Enables a disciplined and structured approach to mitigating risks in accordance with the priorities of the responsible party and the assigned information system owner.
- Contains the findings and recommendations of a security assessment report and any identified items from ongoing security assessments
- Is maintained throughout the lifecycle of the system or service.
- The Center for Development of Security Excellence provides an excellent Job aid as a reference example of how a POAM can be used as a tool that can be adopted by the

MSP organization. Following is a link to an example POAM: https://www.cdse.edu/documents/cdse/CDSE_POAM_Final_Job_Aid.pdf

What Should We Be Measuring?

The Yellow Book captures the foundational set of measurements every organization—regardless of location—should implement to ensure the security controls introduced throughout the entire Yellow book series are effectively managed and administered. As stated previously, your MSP may have other measurements already implemented due to regulatory or compliance requirements like HITRUST or PCI. If you are already measuring controls within your organization, use this as a guide to ensure there are no gaps. There will be additional measurements as the MSP continues down the security journey. The additional measurements are covered in the Green and Blue book series.

For the baseline security practices, the MSP organization should measure the following objectives:

Infrastructure Measurements

- Servers
  - Vulnerability Scanning
  - Patching (OS & Applications)
  - Standard Secure Configuration (Configuration Management)
- Client Devices
  - Standard Secure Configuration
  - Endpoint Protection
  - Patching (OS & Applications)
- Perimeter Security
  - Secure Firewall Configuration
  - Monitoring and Alerts

Governance Measurements

- Policy Compliance
  - Policy Review
  - Personnel Security
- Security Awareness Training
  - End User Training
  - Executive and Management Training
- Password Compliance (includes MFA)
  - Complexity
  - Age
  - MFA enabled
- Security vs Infrastructure Budget
- Risk Assessments

We are utilizing NIST SP 800-55 Rev.1 as the reference material for the minimum security requirements. In addition, ITN Secure has populated the minimum metrics in each of the requirement areas below. If your organization wishes to enhance these numbers or add additional metrics to look at other security controls, please do. We only ask that all organizations achieve the baseline to move onto the enhanced control sets within the Green and Blue books.

Measurement Objectives

SPECIFICATIONS FOR MINIMUM SECURITY REQUIREMENTS

Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems), and the types of transactions and functions that authorized users are permitted to exercise.

Measure 3: Access Control (AC) (system-level)

Field	Data
Measure ID	Remote Access Control Measure 1 (or a unique identifier to be filled out by the organization)
Goal	• *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • *Information Security Goal:* Restrict information, system, and component access to individuals or machines that are identifiable, known, credible, and authorized.
Measure	Percentage (%) of remote access points used to gain unauthorized access NIST SP 800-53 Controls: AC-17; Remote Access
Measure Type	**Effectiveness**/Efficiency
Formula	(Number of remote access points used to gain unauthorized access/Total number of remote access points) *100
Target	This should be a low percentage defined by the organization.
Implementation Evidence	1. Does the organization use automated tools to maintain an up-to-date network diagram that identifies all remote access points (CM-2)? o Yes Δ No 2. How many remote access points exist in the organization's network? 3. Does the organization employ Intrusion Detection Systems (IDS) to monitor traffic traversing remote access points (SI-4)? o Yes Δ No 4. Does the organization collect and review audit logs associated with all remote access points (AU-6)? o Yes Δ No 5. Does the organization maintain a security incident database that identifies standardized incident categories for each incident (IR-5)? o Yes Δ No

	6. Based on reviews of the incident database, IDS logs and alerts, and/or appropriate remote access point log files, how many access points have been used to gain unauthorized access within the reporting period?
Frequency	Collection Frequency: Organization defined (example: monthly)
	Reporting Frequency: Organization defined (example: quarterly)
Responsible Parties	• Information Owner: Computer Security Incident Response Team (CSIRT) • Information Collector: System Administrator or Information System Security Officer (ISSO) • Information Customer: Chief Information Officer (CIO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	Incident database, audit logs, network diagrams, and IDS logs and alerts
Reporting Format	Stacked bar chart, by month, which illustrates the percentage of remote access points used for unauthorized access versus the total number of remote access points

Awareness and Training (AT): Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the information security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the information security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information-security-related duties and responsibilities.

Measure 4: Awareness and Training (AT) (program-level)

Field	Data
Measure ID	Security Training Measure 1 (or a unique identifier to be filled out by the organization)
Goal	• *Strategic Goal:* Ensure there is a high-quality workforce supported by modern and secure infrastructure and operational capabilities. • *Information Security Goal:* Ensure that organization personnel are adequately trained to carry out their assigned information-security-related duties and responsibilities.
Measure	Percentage (%) of information system security personnel that have received security training NIST SP 800-53 Controls: AT-3: Security Training
Measure Type	Implementation
Formula	(Number of information system security personnel that have completed security training within the past year/Total number of information system security personnel) *100
Target	This should be a high percentage defined by the organization.
Implementation Evidence	1. Are significant security responsibilities defined with qualifications criteria and documented in policy (AT-1 and PS-2)? Yes No 2. Are records kept of which employees have significant security responsibilities (AT-3)? Yes No 3. How many employees in your agency (or agency component, as applicable) have significant security responsibilities (AT-3)? 4. Are training records maintained (AT-4)? (Training records indicate the training that specific employees have received.) Yes No 5. How many of those with significant security responsibilities have received the required training (AT-4)? 6. If all personnel have not received training, state all reasons that apply (AT-4): • Insufficient funding • Insufficient time • Course unavailable

	• Employee has not registered • Other (specify)
Frequency	Collection Frequency: Quarterly Reporting Frequency: Annual
Responsible	• Information Owner: Organization defined (example: Training Manager)

Audit and Accountability (AU): Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so that they can be held accountable for their actions.

Measure 5: Audit and Accountability (AU) (system-level)

Field	**Data**
Measure ID	Audit Record Review Measure 1 (or a unique identifier to be filled out by the organization)
Goal	• *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • *Information Security Goal:* Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity.
Measure	Average frequency of audit records review and analysis for inappropriate activity NIST SP 800-53 Controls: AU-6: Audit Monitoring, Analysis, and Reporting
Measure Type	Effectiveness/**Efficiency**
Formula	Average frequency during reporting period
Target	This should be a high frequency defined by the organization.
Implementation Evidence	For each system: 1. Is logging activated on the system (AU-2)? ○ Yes Δ No 2. Does the organization have clearly defined criteria for what constitutes evidence of "inappropriate" activity within system audit logs? ○ Yes Δ No 3. For the reporting period, how many system audit logs have been reviewed within the following time frames for inappropriate activity? Choose the nearest time period for each system (AU-3 and AU-6): • Within the past day • Within the past week • 2 weeks to 1 month • 1 month to 6 months • Over 6 months
Frequency	Collection Frequency: Organization defined (example: daily) Reporting Frequency: Organization defined (example: quarterly)

Responsible Parties	• Information Owner: Organization defined (example: System Owner) • Information Collector: Organization defined (example: System Administrator) • Information Customer: Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	Audit log reports
Reporting Format	Bar chart showing the number of systems with average audit log reviews in each of the five categories within the Implementation Evidence field

Certification, Accreditation, and Security Assessments (CA): Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Measure 6: Certification, Accreditation, and Security Assessments (CA) (program-level)

Field	Data
Measure ID	C&A Completion Measure 1 (or a unique identifier to be filled out by the organization)
Goal	• *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • *Information Security Goal:* Ensure all information systems have been certified and accredited as required.
Measure	Percentage (%) of new systems that have completed certification and accreditation (C&A) prior to their implementation NIST SP 800-53 Control: CA-6: Security Accreditation
Measure Type	**Effectiveness**/Efficiency
Formula	(Number of new systems with complete C&A packages with Authorizing Official [AO] approval prior to implementation)/(Total number of new systems) *100
Target	This should be a high percentage defined by the organization.
Implementation Evidence	1. Does your agency (or agency component, if applicable) maintain a complete and up-to- date system inventory? Yes No 2. Is there a formal C&A process within your agency (CA-1)? Yes No 3. If the answer to Question 2 is yes, are system development projects required to complete C&A prior to implementation (CA-1)? Yes No 4. How many new systems have been implemented during the reporting period? 5. How many systems indicated in Question 4 have received an authority to operate prior to implementation (CA-6)?
Frequency	Collection Frequency: Organization defined (example: quarterly) Reporting Frequency: Organization defined (example: annually)

Responsible Parties	• Information Owner: Organization defined (example: Authorizing Official [AO]) • Information Collector: Organization defined (example: System Owners) • Information Customer: Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	System inventory, system C&A documentation
Reporting Format	Pie chart comparing the percentage of new systems with AO-approved C&A packages versus new systems without AO-approved C&A packages

Configuration Management (CM): Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective information system development life cycles; and (ii) establish and enforce information security configuration settings for information technology products employed in organizational information systems.

Measure 7: Configuration Management (CM) (program-level)

Field	Data
Measure ID	Configuration Changes Measure 1 (or a unique identifier to be filled out by the organization)
Goal	• *Strategic Goal:* Accelerate the development and use of an electronic information infrastructure. • *Information Security Goal:* Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
Measure	Percentage (%) of approved and implemented configuration changes identified in the latest automated baseline configuration NIST SP 800-53 Controls – CM-2: Baseline Configuration and CM-3: Configuration Change Control
Measure Type	Implementation
Formula	(Number of approved and implemented configuration changes identified in the latest automated baseline configuration/Total number of configuration changes identified through automated scans) *100
Target Implementation Evidence	This should be a high percentage defined by the organization. 1. Does the organization manage configuration changes to information systems using an organizationally approved process (CM-3)? ○ Yes Δ No 2. Does the organization use automated scanning to identify configuration changes that were implemented on its systems and networks (CM-2, Enhancement 2)? ○ Yes Δ No 3. If yes, how many configuration changes were identified through automated scanning over the last reporting period (CM-3)? 4. How many change control requests were approved and implemented over the last reporting period (CM 3)?
Frequency	Collection Frequency: Organization defined (example: quarterly) Reporting Frequency: Organization defined (example: annually)

Responsible Parties	• Information Owner: Organization defined (example: Configuration Manager) • Information Collector: Organization defined (example: Information System Security Officer (ISSO), System Owner, System Administrator) • Information Customer: Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), Authorizing Official [AO], Configuration Control Board)
Data Source	System security plans, configuration management database, security tool logs
Reporting Format	Pie chart comparing the percentage of approved and implemented changes documented in the latest baseline configuration versus the percentage of changes not documented in the latest baseline configuration

Identification and Authentication (IA): Organizations must identify information system users, processes acting on behalf of users or devices, and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Measure 9: Identification and Authentication (IA) (system-level)

Field	Data
Measure ID	User Accounts Measure 1 (or a unique identifier to be filled out by the organization)
Goal	• *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • *Information Security Goal:* Identify and authenticate all system users in accordance with information security policy.
Measure	Percentage (%) of users with access to shared accounts NIST SP 800-53 Controls – AC-2: Account Management, AC-3: Access Enforcement, and IA-2: User Identification and Authentication
Measure Type	Effectiveness/Efficiency
Formula	(Number of users with access to shared accounts/Total number of users) *100
Target	This should be a low percentage defined by the organization.
Implementation Evidence	1. How many users have access to the system (IA-2)? 2. How many users have access to shared accounts (AC-2)?
Frequency	Collection Frequency: Organization defined (example: monthly) Reporting Frequency: Organization defined (example: monthly)
Responsible Parties	• Information Owner: Organization defined (example: System Owner, System Administrator) • Information Collector: Organization defined (example: System Administrator) • Information Customer: Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	Configuration Management Database, Access Control List, System-Produced User ID Lists
Reporting Format	Pie chart comparing the percentage of users with access to shared accounts versus the percentage of users without access to shared accounts

Planning (PL): Organizations must develop, document, periodically update, and implement system security plans for organizational information systems that describe the security controls in place or planned for the information systems, and the rules of behavior for individuals accessing the information systems.

Measure 14: Planning (PL) (program-level and system-level)

Field	Data
Measure ID	Planning Measure 1 (or a unique identifier to be filled out by the organization)
Goal	• *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • *Information Security Goal:* Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for information systems, and the rules of behavior for individuals accessing these systems.
Measure	Percentage (%) of employees who are authorized to access to information systems only after they sign an acknowledgement that they have read and understand the rules of behavior
	NIST SP 800-53 Controls – PL-4: Rules of Behavior and AC-2: Account Management
Measure Type	Implementation
Formula	(Number of users who are granted system access after signing rules of behavior/Total number of users with system access) *100
Target	This should be a high percentage defined by the organization.
Implementation Evidence	1. How many users access the system (AC-2)? 2. How many users signed the rules of behavior acknowledgement (PL-4)? 3. How many users have been granted access to the information system only after signing the rules of behavior acknowledgement?
Frequency	Collection Frequency: Organization defined (example: quarterly) Reporting Frequency: Organization defined (example: annually)
Responsible Parties	• Information Owner: Organization defined (example: System Owner, Information System Security Officer [ISSO])
	• Information Collector: Organization defined (example: System Administrator, System Owner) • Information Customer: Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	Repositories containing rules of behavior records
Reporting Format	Pie chart comparing the percentage of users who have signed the rules of behavior acknowledgement form prior to being granted information system access versus those users who have accessed the system without signing the rules of behavior acknowledgement form

Personnel Security (PS): Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established information security criteria for those positions; (ii) ensure that organizational information and information systems are protected during personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational information security policies and procedures.

Measure 15: Personnel Security (PS) (program-level and system-level)

Field	Data
Measure ID	Personnel Security Screening Measure 1 (or a unique identifier to be filled out by the organization)
Goal	• *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • *Information Security Goal:* Ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions.
Measure	Percentage (%) of individuals screened before being granted access to organizational information and information systems NIST SP 800-53 Controls – AC-2: Account Management and PS-3: Personnel Screening
Measure Type	Implementation
Formula	(Number of individuals screened/Total number of individuals with access) *100
Target	This should be a high percentage defined by the organization.
Implementation Evidence	1. How many individuals have been granted access to organizational information and information systems (AC-2)? 2. What is the number of individuals who have completed personnel screening (PS-3)?
Frequency	Collection Frequency: Organization defined (example: quarterly) Reporting Frequency: Organization defined (example: annually)
Responsible Parties	• Information Owner: Organization defined (example: Human Resources) • Information Collector: Organization defined (example: System Administrators, System Owners, Information System Security Officer [ISSO]) • Information Customer: Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	Clearance records, access control lists

Reporting Format	Pie chart comparing the percentage of individuals screened versus the total number of individuals

Risk Assessment (RA): Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Measure 2: Vulnerability Management (program-level)

Field	Data
Measure ID	Vulnerability Measure 1
Goal	• *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • *Information Security Goal:* Ensure all vulnerabilities are identified and mitigated.
Measure	Percentage (%) of high vulnerabilities mitigated within organizationally defined time periods after discovery NIST SP 800-53 Controls: RA-5; Vulnerability Scanning
Measure Type	Effectiveness/Efficiency
Formula	(Number of high vulnerabilities identified and mitigated within targeted time frame during the time period /Number of high vulnerabilities identified within the time period) *100
Target	This should be a high percentage defined by the organization.
Implementation Evidence	1. Number of high vulnerabilities identified across the enterprise during the time period (RA-5). 2. Number of high vulnerabilities mitigated across the enterprise during the time period (RA-5).
Frequency	Collection Frequency: Organization defined (example: quarterly) Reporting Frequency: Organization defined (example: quarterly)
Responsible Parties	• Information Owner: Chief Information Officer (CIO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Owner • Information Collector: System Administrator or Information System Security Officer (ISSO) • Information Customer: Chief Information Officer (CIO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	Vulnerability scanning software, audit logs, vulnerability management systems, patch management systems, change management records

Reporting Format	Stacked bar chart illustrating the percentage of high vulnerabilities closed within targeted time frames after discovery over several reporting periods

System and Services Acquisition (SA): Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ information system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate information security measures to protect information, applications, and/or services outsourced from the organization.

Measure 1: Security Budget (program-level)

Field	Data
Measure ID Goal	Security Budget Measure 1 • *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • *Information Security Goal:* Provide resources necessary to properly secure information and information systems.
Measure	Percentage (%) of the organization's information system budget devoted to information security NIST SP 800-53 Controls – SA-2; Allocation of Resources
Measure Type	Impact
Formula	(Information security budget/Total organization information technology budget) *100
Target	This should be an organizationally defined percentage.
Implementation Evidence	1. What is the total information security budget across all organization systems (SA-2)? 2. What is the total information technology budget across all organization systems (SA-2)?
Frequency	Collection Frequency: Organization defined (example: annually) Reporting Frequency: Organization defined (example: annually)
Responsible Parties	• Information Owner: Chief Information Officer (CIO), Chief Financial Officer (CFO), Senior Organization Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]) • Information Collector: System Administrator or Information System Security Officer (ISSO), budget personnel • Information Customer: Chief Information Officer (CIO), Senior Organization Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), external audiences (e.g., Office of Management and Budget)
Data Source	Exhibit 300s, Exhibit 53s, organization budget documentation

Reporting Format	Pie chart illustrating the total organization information technology budget and the portion of that budget devoted to information security

System and Communications Protection (SC): Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and information systems engineering principles that promote effective information security within organizational information systems.

Measure 18: System and Communications Protection (SC) (program-level)

Field	Data
Measure ID	System and Communication Protection Measure 1 (or a unique identifier to be filled out by the organization)
Goal	• *Strategic Goal:* Accelerate the development and use of an electronic information infrastructure. • *Information Security Goal:* Allocate sufficient resources to adequately protect electronic information infrastructure.
Measure	Percentage (%) of mobile computers and devices that perform all cryptographic operations using FIPS 140-2 validated cryptographic modules operating in approved modes of operation NIST SP 800-53 Control – SC-13: Use of Validated Cryptography
Measure Type	Implementation
Formula	(Number of mobile computers and devices that perform all cryptographic operations using FIPS 140-2 validated cryptographic modules operating in approved modes of operation/Total number of mobile computers and devices) *100
Target	This should be a high percentage defined by the organization.
Implementation Evidence	1. How many mobile computers and devices are used in the organization (CM-8)? 2. How many mobile computers and devices employ cryptography (CM-8)? a. How many mobile computers and devices employ FIPS 140-2 validated encryption modules (SC-13)? b. How many of those mobile computers and devices perform all cryptographic operations using FIPS 140-2 validated cryptographic modules operating in approved modes of operation (SC-13)?

	3. How many mobile computers and devices have cryptography implementation waivers (CM-8)?
Frequency	Collection Frequency: Organization defined (example: quarterly) Reporting Frequency: Organization defined (example: annually)
Responsible Parties	• Information Owner: Organization defined (example: System Owners, Information System Security Officer [ISSO])
	• Information Collector: Organization defined (example: System Administrators, System Owners, Information System Security Officer [ISSO]) • Information Customer: Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	System security plans
Reporting Format	Pie chart illustrating the number of mobile computers and devices that perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation as a percentage of the total number of mobile computers and devices

System and Information Integrity (SI): Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories, and take appropriate actions in response.

Measure 19: System and Information Integrity (SI) (program-level and system-level)

Field	Data
Measure ID	System and Information Integrity 1 (or a unique identifier to be filled out by the organization)
Goal	• *Strategic Goal:* Accelerate the development and use of an electronic information infrastructure. • *Information Security Goal:* Provide protection from malicious code at appropriate locations within organizational information systems, monitor information systems security alerts and advisories, and take appropriate actions in response.
Measure	Percentage (%) of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated NIST SP 800-53 Controls – SI-2: Flaw Remediation
Measure Type	Implementation and Effectiveness/Efficiency
Formula	(Number of vulnerabilities addressed in distributed alerts and advisories for which patches have been implemented, determined as non-applicable, or granted a waiver/Total number of applicable vulnerabilities identified through alerts and advisories and through vulnerability scans) *100
Target	This should be a high percentage defined by the organization.
Implementation Evidence	1. Does the organization distribute alerts and advisories (SI-5)? ○ Yes Δ No 2. How many vulnerabilities were identified by analyzing distributed alerts and advisories (SI-5)? 3. How many vulnerabilities were identified through vulnerability scans (RA-5)? 4. How many patches or workarounds were implemented to address identified vulnerabilities (SI-2)? 5. How many vulnerabilities were determined to be nonapplicable (SI-2)? 6. How many waivers have been granted for weaknesses that could not be remediated by implementing patches or workarounds?
Frequency	Collection Frequency: Organization defined (example: weekly)

	Reporting Frequency: Organization defined (example: monthly)
Responsible Parties	• Information Owner: Organization defined (example: Computer Security Incident Response Team [CSIRT]) • Information Collector: Organization defined (example: Information System Security Officer [ISSO], System Owners) • Information Customer: Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	Vulnerability scans, POA&Ms, repositories of alerts and advisories, risk assessments
Reporting Format	Stacked bar chart with total number of applicable vulnerabilities composed of percentages of number of vulnerabilities addressed in distributed alerts and advisories for which patches have been determined as nonapplicable, have been implemented, have had a waiver granted, or other

Security Life Cycle/Review

Organizations are constantly evaluating and selecting a variety of information security services - both people and technology - to maintain and improve their security program and architecture. These services range from policy development to data loss prevention (DLP) solutions.

When implementing information security services, consider factors such as service provider qualifications, operational requirements, the type of service, and the ability to deliver adequate protection to the organization.

This volume aids in the selection, implementation, and management of the information security service using the six phases of the IT Security Life Cycle defined in **NIST SP 800-35**.

The six phases of the IT Security Life Cycle are:

- Phase 1: Initiation - The organization determines if it should investigate whether implementing an IT security service might improve the effectiveness of the organization's IT security program.
- Phase 2: Assessment - The organization determines the security posture of the current environment using metrics and identifies the requirements and viable solutions.
- Phase 3: Solution - Decision makers evaluate potential solutions, develop the business case, and specify the attributes of an acceptable service arrangement solution from the set of available options.
- Phase 4: Implementation - The organization selects and engages the service provider, develops a service arrangement, and implements the solution.
- Phase 5: Operations - The organization ensures operational success by consistently monitoring service provider and organizational security performance against identified requirements, periodically evaluating changes in risks and threats to the organization, and ensuring the organizational security solution is adjusted as necessary to maintain an acceptable security posture.
- Phase 6: Closeout - The organization ensures a smooth transition as the service ends or is discontinued

Here are some recommendations from NIST for organizations looking to select IT security services:

- Develop objective business cases.
- Develop strong, specific service agreements.
- Use metrics throughout the life cycle to help evaluate performance and progress.
- Ensure you have an appropriate transition period of the service.
- Maintain the technical expertise to understand and manage the security service being implemented.

Phase 1: Initiation

The Initiation phase is triggered by an event that warrants a change to the current environment and the need to identify viable service solutions. The trigger falls into one of six categories:

1. Strategy/mission
2. Budgetary/funding
3. Technical/architecture
4. Organizational
5. Personnel
6. Policy/process

The service life cycle is initiated by business, IT, IT security managers, or some combination of these. The decision to acquire a new security service or product should lead you to obtain the most appropriate security services, at the most appropriate level, in the most appropriate service arrangement in order to support the business function. The next phase of the life cycle, Assessment, is where you determine whether the most appropriate security service is provided internally or externally.

Phase 2: Assessment

The Assessment phase steps include baselining the existing environment, analyzing opportunities and barriers, and identifying options and risks.

To get an understanding of the baseline environment, decision makers need to use metrics and Total Cost of Ownership (TCO) principles to ensure accurate data is used for decision making. The TCO is the purchase price of an asset plus the costs of operation. Assessing the total cost of ownership allows you to get a big picture look at what the product is and what its value is over time. You should also add the risks of implementing or not implementing a product or service to the equation. The item with the lower TCO is the better value in the long run.

This data also sets performance targets and cost estimates for service agreements in later phases.

With the full cost of services in mind, business owners can begin to determine the opportunities and barriers.

Phase 3: Solution

Before specifying a solution, business owners must develop a business case for each product or service being considered. The business case provides the costs, benefit, and organizational risk perspective for each solution being considered. Comparing these costs, benefits, and organizational risk aids business owners in choosing the right solution.

There might be some disagreement and discussion among business owners, but, in the end, there must be a consensus. A solution can only succeed if all business, IT, or IT security managers buy in to the solution.

Phase 4: Implementation

At this point in the process, it is time to develop the implementation plan. This plan provides the roadmap for your organization to move from the current environment to the future desired environment.

The implementation plan should include the following:

- Project management roles and responsibilities
- Budget and scope
- Implementation process
- Risk mitigation plans
- Exit strategies
- Transition management

Implementation

Now it is time to turn your strategies/plans into actions in order to accomplish your new solution implementation goals and objectives. It takes critical actions to move your plan from a document stored on your network to actions that drive security.

The following implementation tips help your project be successful and get to the next phase of the Information Security Life Cycle.

- Ownership of the project: Ensure there is an implementation owner with executive support, and that those implementing the product or service have a stake and responsibility in the plan.
- Over communicate: The plan should be communicated to all key stakeholders. Everyone should understand their roles and responsibilities in the implementation.
- Do not forget long term goals: Consumed by daily operating problems, owners and managers can lose sight of long-term goals. Make it a point to regularly review and update the implementation plan.
- Have a meaningful plan: The vision, mission, value statements, and steps should be concise and supported by the employees working on the plan.
- Talk strategy: Keep strategy a part of your regular messaging to your company.
- Provide progress reports: Have a method to track progress and other processes that are important. Make sure everyone can feel momentum in the implementation.
- Drive accountability: Accountability and high visibility help drive change. This means that each measure, objective, data source, and initiative must have an owner.
- Empowering the team: Although accountability may provide strong motivation for improving performance, employees must also have the authority, responsibility, and tools necessary to impact relevant measures. Otherwise, they may resist involvement and ownership.

Phase 5: Operations

The Operations phase begins once the product or service is fully implemented. During this time the company, security, and newly implemented solution is monitored to ensure the solution meets the company requirements. This continues until a trigger occurs, initiating the close out of this life cycle and necessitating the next security product or service implementation. Throughout this phase, the project manager should ensure the product or service meets stated service levels and complies with internal security policies and procedures.

The Operations phase is like the Assessment phase in that data should be collected to capture the performance level of the new product or service. During this phase, the desired future arrangement becomes the current arrangement. The set targets should be compared to the metrics gathered in this phase.

The product or service evolves as it matures. Monitoring and measuring the product or service allows IT stakeholders to evaluate the company's performance and find ways to improve, even if the targets are met. The world of IT security products and services is ever-changing. Arrangements and agreements need to evolve with these changes.

Phase 6: Closeout

Severing ties and finding replacement services may prove difficult as more services move into the cloud and the number of business that rely upon such hosted services as part of their critical infrastructure grows. For many organizations who rely upon third-party vendors and cloud services in order to stay in business, where one service ends, another service must begin.

When entering into a service agreement with a provider, you should have an exit plan. This exit plan should have several strategies on how to disengage from those services if it becomes necessary. For example, your contract might only be for a specific amount of time; knowing the service's expiration date can help plan for a migration to a new service provider or platform.

Nevertheless, there will always be issues with outside organizations due to their financial situation, natural or man-made disasters, global pandemics, etc. In such cases, the service provider may suddenly have to close shop or, without warning, go out of business. MSP owners and operators must be aware and prepared for these potential situations when relying on outside entities to host critical MSP business operations and client services.

When prepared in advance, services closeout with a proper exit strategy provides the MSP organization with lessons learned for any future cloud-based or IT security service implementations.

Risk Management Program

Risk is oftentimes nebulous to a technical organization. The focus is often more aligned to technical solutions defined by applications and hardware; this is not enough to secure an organization. The solutions lack an understanding and reasoning for implementation. You must ask questions like, "Which security controls are being implemented with this solution?," "Are there any gaps that are still exposed?," and "Are the processes used exposing the organization to risk?"

Risk management is not a "one size fits all" solution. Each organization is different and unique, requiring a strategy and analysis with business buy-in, direction, and oversight. If you have completed the governance items, then you have the foundation in place to begin defining, identifying, analyzing, and mitigating risk within your organization. Risk has many different facets the organization needs to consider such as vulnerabilities in technology, applications, and third-party vendors, as well as a human element.

Lastly, threats are constantly evolving and morphing. For this reason, the organization must review the risk posture on a regular cadence. Changes in personnel, processes, technology, and all the other items mentioned above can have both positive and negative impacts to the risk posture as well. It is critical each member of the organization understands this impact through adherence of the policies, security awareness training, and response exercises. Executives, directors, managers, and leads also play a very important role in this process.

Define a Vulnerability Analysis and Resolution Strategy

As you learned in the Governance section, all programs need direction through a well thought out and defined strategy. Not all strategies are created equal, nor does one strategy fit for each organization. However, there are some commonalities for starting the program, which we cover in this section. As stated in previous sections, the information contained here is just the minimum common elements. To ensure you meet compliance and regulatory requirements, you must enhance these elements and potentially add more to fulfill those requirement objectives. You also must enhance elements to achieve the next level of the certification program.

Vulnerability management is a key component in understanding your organization's overall risk. Organizations need to understand how vulnerabilities impact the overall weaknesses within your environment. Use a risk-based approach to make appropriate decisions on how and when to mitigate those weaknesses in a prioritized manner. We should clarify here that vulnerabilities encompass more than simple system and application patching; they are flaws in design (hardware, software, and architecture), coding (operating systems, applications, firmware), and process (missed steps, insecure procedures).

The Analysis and Resolution Strategy should encapsulate all these items. To achieve success, you must have a good foundational program.

What is Analysis and Resolution Strategy, and How do We Develop One?

To begin the process, the organization must determine the scope of vulnerability management, determine the approval method for vulnerability assessment, and assign resources to the activity. Once these items have been accomplished, you can develop a program plan. This includes:

- Defining and documenting the plan
- Defining the measurements for effectiveness
- Defining the training
- Determining which tools align to the strategy
- Identifying which sources of information to use for the vulnerabilities
- Defining roles and responsibilities
- Engaging with stakeholders
- Planning a revision process

Vulnerability Management Program

At the core of any vulnerability management program lies the fundamental process of software management. Most vulnerabilities are software "bugs" that can be exploited and possibly lead to a compromise in confidentiality, information, or availability. As such, an MSP organization should take the time to understand all the software used within their environment. The first step in vulnerability management involves documenting software, the version or patch level of software, where the software is installed, who has access to the software, and if the software is currently under vendor maintenance and support.

Once the software across the organization has been identified, research may be required to determine if there are any know vulnerabilities that exist for the version that is currently installed and used by the workforce personnel in daily business operations. Then you must prioritize each of the identified vulnerabilities and decide upon a course of action to either patch or mitigate the most critical vulnerabilities and the most exposed systems. It is impossible to address all identified vulnerabilities, so it is beneficial to evaluate the risk in order to prioritize the time, talent, and funding resources required to address the most critical issues.

Much of the initial analysis may be conducted with automated tools and vulnerability scanners that can help identify and actively manage (track, report on, correct) the security configuration and patching of servers, desktops, and laptops. Additional vulnerability management tools and techniques that can provide insight into vulnerabilities may already be deployed or utilized across the organization. Such activities may include:

- **Configuration Management**: In addition to vendor software "bugs," poor configuration management due to misconfigured settings or lack of patching can easily lead to an openly exploitable vulnerability. This in turn can directly impact the business operations and services provided to existing clients. Using a vulnerability scanner to search for such configuration issues helps to identify the issue and gives you the opportunity to securely

correct them.

- **Antivirus Monitoring:** With the focus on identifying, catching, and removing known and potential malware within the network and host systems of the MSP organization, many vendor endpoint protection solutions also capture and log what files and executables are launched from a host. Such information may assist with the identification of installed software. Additionally, such endpoint protection solutions offer several tactics to protect the host and the attached network from specific threats (Trojans, ransomware, spyware, etc.) looking to take advantage of vulnerabilities that may exist on the host system. The exploit is then blocked by the protection software.

- **Penetration Testing:** During a penetration test, the most common vulnerabilities identified are often a direct result of poor configuration of a software application or an operating system. It is common to find many default configurations that have been configured and deployed in order to deliver speed and compatibility over any security concerns. Such an organizational mindset makes it much more difficult to securely implement new technologies from existing workforce personnel or outside consultants without the aid of subject matter experts.

Having secure configurations and creating the core capability of a vulnerability management program starts by having dedicated subject matter experts. These experts can review the configurations for new and existing systems and applications. Such workforce personnel should not only be well versed in performing penetration tests and vulnerability scans, but also should be able to interpret and effectively communicate the results of these tests. This helps to manage (track, report on, correct) security configuration and patching as part of the overall vulnerability management program.

Patch Management Program

In order to detect and correct security weaknesses, MSP organizations must manage the security life cycle of all software they use. In particular, IT must regularly check that they use only the most current versions of each application and operating system to ensure all relevant patches are promptly installed.

Planning, testing, implementing, and auditing patch management software should be part of a regular security regimen. Legacy systems running on operating systems that are no longer supported by the vender may place the MSP organization at risk. At a minimum, the system administrators and network personnel should make the effort to keep all operating system (OS) software up to date, properly licensed, and fully supported. IT teams should commit to the following:

- Create a comprehensive inventory of host systems
- Invest in upgrades

- Patch vulnerabilities regularly

Vulnerabilities are frequently discovered in all sorts of software, including the host operating system as well most every software solution. Once discovered, malicious individuals or groups quickly organize to take advantage of the opportunity to exploit newly published vulnerabilities in order to attack computers and networks with these weaknesses. Additionally, in order to gain control over vulnerable machines, malicious actors can take advantage of vulnerabilities in web-based applications by performing injection exploits, including buffer overflows, SQL injection attacks, cross-site scripting, and click-jacking of code.

It is a core security best practice to only run current, vendor-supported operating systems for which security patches are made available in a regular and timely fashion. When released by the vendor, available security patches should be properly tested and then applied to production systems on a schedule appropriate to the severity of the risk they mitigate. Never test on production systems.

Business Continuity and Disaster Recovery

When business is disrupted, it can cost money. Lost revenues plus extra expenses often deliver a reduction in profits. Insurance does not cover all the costs associated with a disruption and cannot replace any lost revenue from customers that leave and go to a competitor. For the MSP organization, a business continuity plan is essential. The U.S. Department of Homeland Security's Ready Program provides information on how to prepare for, respond to, and mitigate emergencies, including natural and man-made disasters. The following outlines a suggested business continuity plan divided into four steps:

Step 1: Business Impact Analysis (BIA)
Conduct a business impact analysis to identify time sensitive or critical business functions and processes and the resources that support them.

- Develop a questionnaire
- Conduct a workshop to instruct business function and process managers how to complete the BIA
- Receive completed BIA questionnaires
- Review BIA questionnaires
- Conduct follow-up interviews to validate information and fill in any information gaps

Step 2: Recovery Strategies
Identify, document, and implement strategies to recover critical business functions and processes.

- Identify and document resource requirements based on BIAs
- Conduct gap analysis to determine gaps between recovery requirements and current capabilities
- Explore recovery strategies with management approval

- Implement strategies

Step 3: Plan Development
Organize a business continuity team and compile a business continuity plan to manage a business disruption.

- Develop plan framework
- Organize recovery teams
- Develop relocation plans
- Write business continuity and IT disaster recovery procedures
- Document manual workarounds
- Assemble plan
- Validate the plan and gain management approval

Step 4: Testing and Exercises
Conduct training for the business continuity team. Conduct testing and exercises to evaluate recovery strategies and plans.

- Develop testing, exercise, and maintenance requirements
- Conduct training for business continuity team
- Conduct orientation exercises
- Conduct testing and document test results
- Update business continuity plan to incorporate lessons learned from testing and exercises

Here are some additional sources available for business continuity planning:

- Ready Business Toolkits - The Ready Business Toolkit series includes hazard-specific versions for earthquake, hurricane, inland flooding, power outage, and severe wind/tornado. Toolkits offer business leaders a step-by-step guide to build preparedness within an organization.
- Professional Practices for Business Continuity Professionals - DRI International (non-profit business continuity education and certification body)
- Continuity Guidance Circular 1, Continuity Guidance for Non-Federal Entities - Federal Emergency Management Agency, CGC 1
- Open for Business® Toolkit - Institute for Business & Home Safety

Third-Party and Vendor Risk Program

Mirroring the reflection of the MSP model of services, most every organization has come to rely upon external vendors for products and services that are vital to their operations. As such, the number of service disruption and data breaches attributed to third-party vendors has steadily been rising as more companies conduct their business within cloud-hosted services. Many

organizations have realized that it is no longer sufficient to only secure their internally controlled infrastructure and services; they now must also assess and evaluate the security policies and procedures of their third-party vendors.

It is a fundamental best practice for MSPs to conduct a third-party vendor risk/security assessment. This assessment helps you gather necessary information and documentation to ensure that the third-party has the proper security mechanisms in place to protect their services and ensure the risks are acceptable.

A vendor risk management questionnaire is designed to help organizations identify potential weaknesses among third-party vendors and partners that could possibly result in a loss of contracted services or breach of sensitive data.

There are standard best practices and questions you can use as a starting point for the high-level items in your questionnaires. At a minimum, there are a few fundamental questions and documentation items to consider when verifying or requesting information from the third-party vendor as part of a risk assessment:

Third-Party Vendor Governance and Organizational Structure Questions

- Who is responsible for cybersecurity in the organization?
- Does the organization have a Chief Information Security Officer (CISO)?
- Is there a cross-organizational committee that meets regularly on cybersecurity issues?
- Does the organization conduct a cybersecurity exercise that includes senior executives?
- How does the organization identify and prioritize the most critical assets?
- How does the organization specifically protect customer information?
- Has the organization ever experienced a significant cybersecurity incident? Please define and describe it.
- What types of cybersecurity policies does the organization currently have in place?
- Does the organization outsource any IT or IT security functions to third-party service providers? If so, who are they, what do they do, and what type of access do they have?
- Within the organization, how frequently are employees trained on IT security policies?
- Are automated assessments used to track employee knowledge and compliance?

Third-Party Vendor Security Controls and Technology Questions

- How does the organization currently inventory authorized and unauthorized devices and software?
- Has the organization developed secure configurations for hardware and software?
- How does the organization assess the security of the software that is develop in-house or acquired from a vendor?
- What processes does the organization use to monitor the security and use of wireless networks?
- Does the organization have data recovery capabilities?

- Does the organization employ the use of automated tools to continuously monitor to ensure malicious software is not deployed?
- Describe the processes and tools the organization uses to reduce and control administrative privileges.
- What processes does the organization have in place to prevent the exfiltration of sensitive data, particularly sensitive customer data?
- How does the organization plan and prepare for a cybersecurity incident? What processes are in place to respond to an incident? Does the organization regularly practice scenarios for such incidents?
- Does the organization regularly conduct external and internal tests to identify vulnerabilities and attack vectors, including penetration testing, red team exercises, or vulnerability scanning?
- From whom does the organization receive cyberthreat and cyber vulnerability information? How is that information used?
- How does the organization manage remote access to connect to the corporate network?
- Does the organization have a removable media policy and controls to implement the policy?
- How does the organization monitor for unauthorized personnel, connections, devices, and software?
- Describe the process the organization has in place to communicate security incidents that are affecting our data.

Incident Management Program

Is your MSP organization prepared to respond to a data breach or a cyber attack? If not, be ready because it will happen someday. How you immediately react and respond to a breach is of critical importance. Having a working incident management program is the best chance your organization has in defending itself from suffering any long-term damage or loss of reputation from a cyber incident. Creating an incident response program for your organization does not have to be a drawn-out, daunting process. An incident management program must start with a plan.

According to the National Institute of Standards and Technology (NIST), an incident response plan simply provides "the instructions and procedures an organization can use to identify, respond to, and mitigate the effects of a cyber incident." Following are some best practices for developing an incident response plan:

- Develop the plan as a systematic approach taken by the entire organization to prepare for, detect, contain, and recover from a security breach
- Practice the plan - in an attack, it is critical to respond quickly in an organized manner
- The plan supports responding to incidents systematically, so the appropriate actions are taken
- The plan helps minimize the loss or theft of information and disruption of services
- The plan allows for the information gathered to help further secure you against future incidents

The following terms are often used interchangeably when discussing Incident Management Terminology. According to NIST:

- A **security event** is a change in the everyday operations of a network or information technology service, indicating that a security policy may have been violated or a security safeguard may have failed.
- A **security breach** is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential, or unauthorized logical IT perimeter. A security breach is also known as a security violation.
- A **data breach** is a security incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. Data breaches may involve financial information such as credit card or bank details, personal health information (PHI), Personally identifiable information (PII), trade secrets of corporations or intellectual property.

When properly implemented across an MSP organization, an incident management program will help reduce the time and expense associated with an incident. To do so, an MSP needs to

understand threats to their environment and prevent common vulnerabilities. Knowing what systems are identified and monitored as well as being alerted to new cyber threats and receiving notice to new patches for system and application vulnerabilities will help the organization manage threats and be better prepared in case of an incident.

- Utilize open community repositories, such as the National Vulnerability Database (https://nvd.nist.gov/), to ensure that known vulnerabilities are addressed.
- Determine what cyber events the organization currently monitors.
- Confirm that a business impact assessment (BIA) is complete and current.
- Use what resources are available and already exists within the organization in order to identify, mitigate and monitor threats.

With the primary focus on the protection of data and critical assets, an incident management program response process will include many different activities, such as:

- Performing secure backups of data and critical systems
- Leveraging system logs and security alerts to detect malicious activity
- Maintaining identity and access management standards to avoid compromise
- Devoting attention to patch management

Every MSP organization must have proper processes and procedures in place in order to reduce the risk of cyber threats. An incident management program will include the planning and processes of business functions and activities, identify, and establish workforce personnel roles, and include written and shared documentation in order to be used to mitigate cybersecurity risks across the organization. Your incident management program must have clearly outlined, actionable steps a response team can quickly follow when an incident occurs. However, response plans also need to be flexible to support a wide range of incidents. If a rigid, complex process must be followed, any unplanned scenarios may result in the response team unable to properly deal with the new problem.

There are basically three core elements to consider when an MSP organization is looking to develop and incident response program:

Incident Response Policy

Policies set the standard of behavior for activities; such examples include:

- Statement of Management Commitment
- Purpose and Objectives of the Policy
- Scope of the Policy
- Organizational Structure and Definition of Roles, Responsibilities, and Levels of Authority
- Severity Ratings of Incidents
- Performance Measures
- Reporting and Contact Forms

Incident Response Plan

Plans are the guidelines in which management has outlined how to fulfill policy requirements; examples:

- The Organizations Mission, Strategies, and Goals for Incident Response.
- Senior Management Approval Process for Execution
- Approach to Incident Response
- Communication Plan with the Organization and Other Organizations
- Metrics for Measuring Effectiveness

Incident Response Procedures

Procedures are the specific step by step instructions to execute individual process as part of a plan, examples:

- Standard Operating Procedures (SOP) for action
- Specific Technical Processes
- Checklists for Evaluation
- Forms Used During Response
- Documented Response Procedures—Minimizes Errors During Pressure Filled Response Processes

Additionally, frequent updates to your incident response program and plans also helps with your flexibility to adapt, address and manager new threats. If your organization formally reviews their incident response plans every six months, then the stakeholders and response teams will be better prepared to adapt to emerging cybersecurity issues and attacks that may target your organization and your clients. Having a strategy and processes in place with a proper method to assess risk and threats to the organization, will serve as the driver for the adoption of new technology and services to deal with those threats that may harm your business or your customers.

Executive / Board / Owner Oversight

Poor communications, lack of leadership, and lack of board oversight often hinder the development of an effective incident management program. Successfully raising executive / board / owner / leadership awareness on the critical importance of adopting and championing an incident management program and response planning should elevate the importance across the entire MSP organization. Having the top-level involvement and support of senior management will allow you to recruit the most qualified candidates and workforce personnel for your security and response teams and foster the creation of processes and information channels that will help you manage an incident effectively. The security culture of your MSP organization will be driven from the attitudes, examples, and tone provided at the top and cascade throughout the rest of the organization including department leaders and individual team members.

Roles and Responsibilities

Know the key stakeholders and what key roles within the MSP organization who should care and be involved in a security incident. The responsible stakeholders and roles may change depending on the type of incident and the targeted resources of the organization. Stakeholders likely include department managers, senior management, partners, customers, and legal. With the involvement of diverse responsibilities, roles, and individual personalities, the addition of business politics, resistance, negotiation, and ignorance may blend into the overall response activities. A fully functioning security incident management program may involve the following roles:

- **Legal Counsel** to provide oversight and legally sound guidance on activities to perform or avoid as well as produce any legal briefs and proceedings
- **Executive Management** for the highest-level decision-making from the executive/board/owner
- **Program / Project Management** to provide oversight and application of knowledge of data, information, processes, organizational structure, workforce skills, and analytical expertise, as well as systems, networks, and data flows to manage the incident response lifecycle
- **IT and Security** teams for technical knowledge, experience, guidance and execution of the initial incident response and containment actions
- **Compliance** to assist with incident oversight and follow up activities, as well as any breach notification or incident reporting that may be required to regulation entities
- **Business Operations** for business direction and communications across business units, departments, and teams
- **Human Resources** for enabling internal communications and assisting with workforce personnel security policies that may have been violated during the incident
- **Public Relations** (internal role or external firm) with expertise and experience in dealing with cybersecurity incidents and with preparing messaging for both internal and external communications
- **Outside Consultants** with specialized skills and expertise who can provide support for digital forensics, incident response, and security testing
- **Vendors** such as internet service providers (ISPs), cloud service providers, hosting providers, software as a service (SaaS) providers and managed security service providers (MSSPs)
- **Business Partners and Stakeholders** that depend and rely upon your services or have integrated technical ties to your service data or IT environment

Within an organization, an incident response team analyzes information, discusses observations and activities, and shares important reports and communications with invested parties. The amount of time the team members may spend on their assigned responsibilities and team activities wholly depends upon the business being in a state of calm or a state of crisis. When team members are not actively investigating or responding to a security incident, the Execution Team and the Steering Team should meet at least every quarter, in order to review any identified or emerging security trends and to possibly update incident response procedures to address any potential risk to the organization. The more information the incident response teams can provide to the executive leadership, the more executive support and participation will follow. Such top-level support of the Incident Response Program can prove to be very powerful to the organization, especially when needed most -- during a crisis or immediately thereafter.

IR Execution Team

The Incident Response Execution Team is responsible for:

- Determining the scope of the attack
- Mitigating the immediate issues concerning a data breach
- Identify the Consequences of the Breach

The Incident Response Execution Team is made up of the following members:

- Primary Incident Response Leader (Defined by Plan)
- Internal IT/InfoSec
- MSP Representatives
- Third-Party Vendors

IR Steering Team

The Incident Response Steering Team is responsible for:

- Make policy changes
- Strategic level decisions
- Release funds for the Incident Response Effort

The Incident Response Steering Team is made up of the following members:

- Primary Incident Response Leader (Defined by Plan)
- Business Owner
- Top Level Management
- HR
- MSP Leadership Representative
- Legal Council
- Public Relations
- CISO

Team Training for Incident Response

An incident response plan is not worth much if it's only on paper, it must be put to the test. Conducting a planned (or unplanned) security exercise, running through the plan and identifying weak spots will go a long way to validating that your incident response team is ready and able to handle a real incident. Creating and managing an incident response plan for your MSP organization involves regular program updates and workforce personnel training. Based upon the Payment Card Industry (PCI-DSS), at a minimum, your organization should take the following steps for training workforce personnel responsible for incident response:

- Test your incident response plans at least once every year
- Assign certain workforce personnel to be available 24/7 in order to work with "off-hours" incidents
- Appropriately and frequently train your staff responsible for handling incident response activities
- Set up alerts from intrusion-detection systems (IDS), intrusion-prevention systems (IPS), and file-integrity monitoring systems
- Implement an internal review process to update and manage your incident response plan to address any recent industry and/or organizational changes

Training your workforce personnel in both the tools and business processes they need will help your IT professionals and staff identify, diagnose, and respond to a cybersecurity incident. In addition to training your team on any existing technology solutions you may have in your organization for logging, monitoring, and alerting, there are many vendors offer specialized training programs and courses in the art of threat hunting and digital forensics that may allow your team to better learn how to analyze, protect, and defend both your business operations and those of your customers.

Communications Plan

The incident response plan should make it crystal clear as to who the incident response team should communicate with, via what means of communication, and specifically what data should be conveyed. Communications is a crucial and often overlooked part of the incident response process. When establishing a response plan, there should be specific guidelines on what level of detail to communicate across the organization including IT management, senior management, affected departments and outside the organization including affected customers, the press and the public.

In communication with internal employees, partners, or customers, it is highly recommended to be prepared to answer all the following standard questions:

- How were you not protected from this?
- How did this happen?
- What about the firewall and anti-virus we had?
- What data did they get?

- How do we keep this from happening again?

When it comes to engaging the Media and dealing with Public Relations keep in mind the following three fundamentals:

- What to Say
- What NOT to Say
- How to Say It

What Makes Effective Key Messages

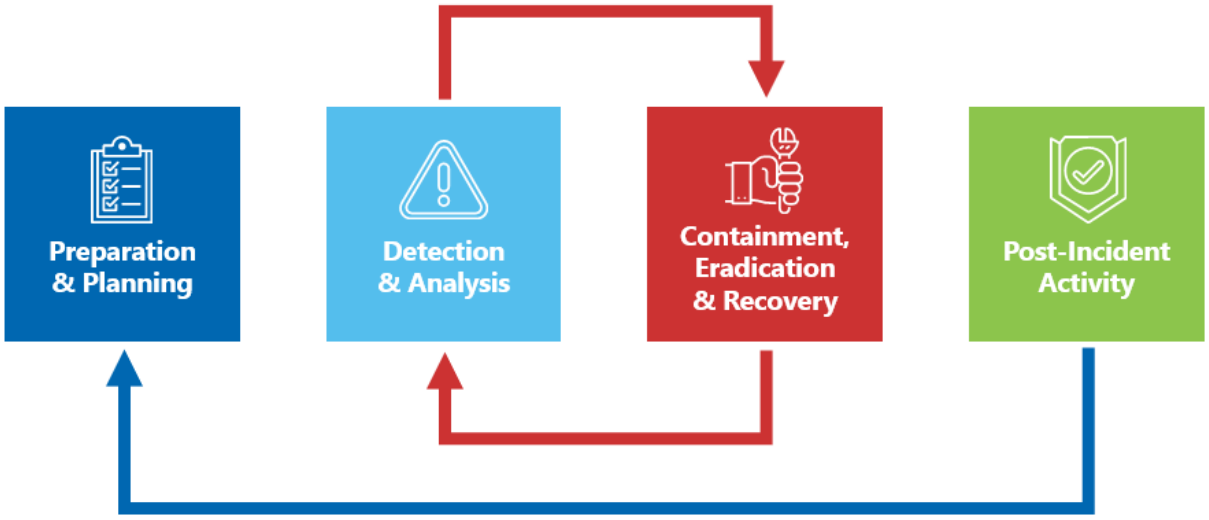
- Limit key messages to 3-5 specific points that address the issue at hand
- Keep answers short and to the point
- Repeat your key messages throughout any interview
- The messaging is not a script; it is a tool

When in doubt as to what to say, memorize and use the following statement:

> "We are unable to respond to that question until we complete our investigation."

Incident Response Life-Cycle

No plan survives contact with the enemy. However, having a flexible incident response program with documented and well-practiced plans should allow your MSP organization to address most any suspected cyber incident throughout a logical series of phases. Within each phase, there are specific areas of need that should be considered by the MSP organization.



Incident Response Lifecycle (NIST)

According to the National Institute of Standards and Technology (NIST), the incident response lifecycle can be broken down into the following phases:

Preparation & Planning

Preparing is one of the most essential incident response activities that an MSP organization must undertake. You need to be prepared to respond to the worst thing that can happen to your business. Preparation is the key to the survival of your business and involves investing work into identifying the start of an incident, how to recover, how to get everything back to normal, and how to create and established security policies.

Additionally, part of your preparation is properly training your workforce personnel and incident response teams in the IT systems, technology, tools, investigative techniques, business processes, and procedures required for their role and responsibilities.

Considerations for Preparation & Planning:

- Proper documentation to support response
- Putting polices, plans, and procedures in place
- Training on the execution

Detection & Analysis

During Detection and Analysis, the team is analyzing symptoms or Indicators of Compromise

(IoCs) that might identify an incident and determining whether systems or data has been breached. In order to stop an incident, you first need to detect and identify any irregular indicators of activity within your environment. Then, analyze and determine the exact nature and scope of the incident.

You can speed up the alerting, identification, and analysis process if you have security monitoring deployed and filtering logs and events into a central location, such as a Security Information and Event Management (SIEM) solution or Endpoint Detection and Response (EDR) solution.

Considerations for Detection & Analysis:

- Profile systems to understand normal behavior
- Create a log retention policy
- Perform event correlation
- Compare logs from differing sources to see the scope of an attack
- AV or EDR may see an infection on a system and point to a cause
- The Firewall logs may show the full source and scope of an intrusion
- Keep all system clocks synchronized
- Document all findings (start immediately upon suspicion of an incident)
- Who discovered the incident?
- When was the incident discovered or reported?
- Where was the incident first discovered or located?
- What impact does the incident currently have on business operations and what is the scope?
- Has the incident source been discovered or is there a suspected point of entry?

Containment

Containment activities encompass any number of actions you take after the initial investigation of the incident to stop the spread and understand the method of attack. Your response should include steps to immediately stop any identified damage, exploitation, or breach in order to limit possible spread to other networks and hosts within your MSP environment and to your customers.

Collecting and preserving evidence, blocking firewall ports, logging access, isolating, and patching systems may play a large part of your containment phase. It's good practice to perform further analysis on the cybersecurity incident while you monitor the effectiveness of your containment measures.

Considerations for Containment:

- Potential damage to and theft of resources
- Need for evidence preservation (legal and insurance)

- Impact on service availability
- Time and resources needed to implement
- Effectiveness of containment strategy and activities
- Duration of the solution (emergency workaround vs. permanent solution)

Cybersecurity emergencies, such as ransomware or unauthorized access, never happen at a convenient time. Cyber-attack responses often require the organization to make a lot of important decisions in a small amount of time.

Recommendations for Emergency Containment:

- Run scans to identify unexpected or high-risk ports/services
- Isolate infected/compromised systems
- Deny all international traffic in the firewall
- Deny all inbound traffic across RDP and other remote access tools to the client site (open RDP is a massive security risk).
- Check all security and system logs for unusual activity
- Do not power down machines unless you have made specific plans for it (malicious autorun commands could cause the spread of threats on boot up).
- Test your backups
- Never assume the attacker is gone

Eradication

After containment, further eradication efforts are often required in order to completely remove the underlying components of the incident and to mitigate any identified vulnerabilities exposed during the incident. If the incident resulted in an attacker gaining access and entry from one system and then spreading into other systems across your connected MSP infrastructure, then you will have more actions to take.

Both containment and eradication efforts must be applied with speed and accuracy to prevent the attacker from regaining access, disrupting your activities, and maintaining their presence within your networked systems. You must spend sufficient time monitoring to ensure the security and integrity of your networked systems and successful eradication efforts.

Sample Eradication and Recovery Steps for an Impacted Site

- Seek and receive authorization in writing from the client/insurance provider to begin eradication/remediation.
- Establish a CLEAN network segment.
- Clean/Rebuild a domain controller of the infection (do not reconnect to the infected network).
- Define CLEAN – Does this require a rebuild/restore? (scan all machines with multiple tools).

- Disable Autorun and Windows Task Scheduler on all systems (GPO).
- Reset all device passwords (verbal communication of change).
- Bring up/clean one server at a time (only required servers).

Recovery

Your MSP organization must implement the recovery process to restore and return any compromised hosts, applications, or networks back to normal operations. Your organization's recovery plan must define actions needed to rebuild infected systems, replace compromised files, reset passwords, patch systems, and secure network perimeters.

It is a best practice to include steps for confirmation and verification in order to validate that vulnerabilities identified from the initial attack and compromise have been properly patched or remediated. Such validation may be conducted as part of an independent (third-party) penetration assessment, or pen test, of the removed systems.

Sample Eradication and Recovery Steps for an Impacted Site

- Any system with activity that looks like a threat and could not be identified should be wiped and rebuilt.
- Maintain forensic data needed by insurance and investigators.
- Tighten down the network to restrict the same attack from happening again.
- Restart backup routine ASAP.
- Use a phased approach so that remediation steps are prioritized.
- For a larger organization, this can take weeks or months—do not rush.

Post Incident Activity

An essential part of responding to a cybersecurity incident is to document, communicate and build upon lessons learned. This step provides the opportunity for your MSP organization's key stakeholders and workforce personnel to reflect on the overall experience and learn how to better respond to future security events and incidents.

No process is perfect for every scenario. Some scenarios cannot even be fathomed until they have occurred. The threat landscape is always evolving so your incident response process will naturally need the occasional update. You should also document and share any lessons learned with your MSP business units and perhaps, with your customers.

Have an overview and debrief with stakeholders to help grow and mature your incident response program. During the debrief activity:

- Review and document the entire incident.
- Perform a root cause analysis.
- Identify steps to prevent the incident or similar incidents in the future.

- Fully debrief with any impacted client.
- Work to design a budgeted security plan to better defend against this type of attack in the future.

Executive, Board and Owner Responsibility

IT security governance is the system by which an organization directs and controls IT security. IT security governance should not be confused with IT security management. IT security management is concerned with making decisions to mitigate risks; governance determines who is authorized to make decisions.

Governance specifies the accountability framework and provides oversight in order to ensure that risks are adequately identified and mitigated, while management ensures that controls are implemented to mitigate risks. Governance ensures that security strategies are aligned with business objectives and consistent with regulations. Management recommends security strategies.

One of the first things a company should do is outline its Organizational Policy Statement, which is also referred to as the master security policy. This statement describes the strategic functions of the organization and enacts company policy. it should come across as an essential part of a long-term strategic plan for the organization.

An Organizational Policy should protect the company's finances, reputation, and assets. it must detail how the business and its assets should be governed so your organization can allocate resources based upon their risk.

Having a Governance Framework or standard in place ensures you have goals that can be measured against current performance. It provides shareholders with oversight and reassures them that risk is being adequately mitigated. Our latest article highlights the characteristics and many benefits of adhering to frameworks, guidelines, and standards. Click here to read it and discover our recommendations.

Information Security Governance should not only align the framework against the company's strategic objectives but also ensure that it complies with local and international regulatory laws. Overall, it is an essential part of a business' risk management strategy, and it will have a direct impact on the course that the company will take over the long term.

The following strategic solutions better position an MSP organization to ensure successful security governance:

Take a Holistic Approach to Strategy

Before implementing Information Security Governance, get a unified view of how security has impacted your organization. A company-wide survey can help scope out what data needs to be protected. This can also help get early buy-in from key stakeholders.

Questions to address include:

- What data needs to be protected?
- Where are the risks?
- What strategic policies should be created?
- Which teams should be responsible for carrying out these policies?

Security strategy is also about aligning and connecting with business and IT objectives. Get input from all stakeholders across the organization — from the IT, sales, marketing, operations, and legal departments — to understand their concerns and challenges, as well as to assess their skills and expertise.

Avoid cookie-cutter solutions and working in silos, which may create more obstacles and fragmented security solutions. A holistic approach makes sure that the leadership — the creators of Information Security Governance — gain more levels of control and visibility.

Create Awareness and Training Throughout the Organization

Setting Information Security Governance and then walking away can bring negative results, such as a lack of adoption, misunderstanding of policies, roles and responsibilities, and security vulnerabilities. Continuous adherence to security governance requires awareness, education, and training for all involved.

Security is not just a concern for IT. It is everybody's responsibility.

- Are your employees bringing their own devices to work?
- Are they using approved apps?
- What are their attitudes toward handling the company's sensitive data?

Frequent company-wide surveys, security seminars, and education on security best practices keep security in mind for all employees.

Although developed by the board of directors, executive management, and steering committees, Information Security Governance is for all employees in the organization. Governance creates policies and assigns accountabilities, but each member is responsible for following the security standards.

Awareness, training, and education for security best practices must be continued. For example, an organization can send team members to security training conferences to learn the latest industry techniques. These team members can then share their new knowledge with the larger organization.

Monitor and Measure

Information Security Governance requires constant assessment and measuring.

- What policies are working?
- Which policies are not?

- Which teams or individuals are not following the security policies?
- Are the number of security incidents having an impact on the company's reputation to customers and partners?

Measuring the performance on Information Security Governance efforts makes sure that objectives are being achieved and resources are managed appropriately.

- How often do you test your security measures?
- How often do data breaches occur?
- What is the response time for incidents?
- Which security policies are working, and which ones are not?

For example, an organization might hold mock data breach scenarios to see how well the teams hold up. The results can showcase what a company needs to work on and what they have nailed down.

Establish Open Communication between All Stakeholders

It's vital that all stakeholders feel they can communicate directly with leadership. Working in silos risks obfuscating important security governance communication.

If a data breach occurs, do employees at any level of the organization feel comfortable enough letting the leadership know? Or will they attempt to shield the top from any negative news?

Open communication promotes trust while augmenting visibility throughout the organization. To further enhance engagement, consider creating a steering committee comprised of executive management and key team leads to review and assess current security risks. Members might include leaders from the IT, finance, PR, marketing, legal, and operations departments.

Regular steering committee meetings can make sure that there is ongoing adherence to the security policies. For example, if a new security policy is created, department leads, who are part of the steering committee, can make sure their teams implement the policy.

Promote Agility and Adaptability

The digital landscape is evolving rapidly as new platforms impact the way we do business. Your Information Security Governance must be open to adaptation. An organization should monitor and measure the overall strength of the security policies. Questions to ask include:

- What's working?
- What's not working?
- What can we change?

For example, an employee in the IT security trenches may have the hands-on experience and insights on the effectiveness of a particular security policy. If the leadership is receptive to hearing feedback and suggestions, there should also be agility in making those changes.

Security Architecture

The MSP organization must work from the top down to instill the concept that security belongs to everyone and should be integrated as part of the culture.

Relating to the overall IT Architecture and business strategy of an MSP organization, Security Architecture can best be defined as the planned assembly policies, standards, best practices, technology solutions, and security controls intended to preserve and maintain the confidentiality, integrity, availability, accountability, and assurance of systems and data. Additionally, a well-designed security architecture not only considers security risks and mitigations, but also includes the blending of people, process and technology.

According to the National Institute of Standards and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, an organization should undertake the design and development of a security architecture for information systems that:

- Describes the overall philosophy, requirements, and approach to be taken regarding protecting the confidentiality, integrity, and availability of organizational information.
- Describes how the information security architecture is integrated into and supports the enterprise architecture.
- Describes any information security assumptions about, and dependencies on, external services.

Additionally, an organization must perform periodic reviews their security architecture and provide updates to mitigate any issues or to address any future business initiatives. Any changes to the overall security architecture are to be reflected as revisions within supporting documentation.

An MSP provides access to technology and services for their clients. Understanding the relationship between your business strategy and technology puts you in an ideal position to design, implement, and develop your own security architecture that better protects your internal operations and client services. This understanding leads into the strategy of security architecture design by way of the creation of policies, standards and procedures, detailed technical design documents, vendor product evaluation and selection, development and testing, production implementation, support documentation and training, as well as the ongoing need to monitor, manage and measure the multiple components against the MSP business needs and vision.

Making the selection of a point product to "bolt-on" and address a specific security need is easy. However, an MSP that has insight into their business goals and vision will be able to justify and implement proper security controls linked directly to identified risks and serve to mitigate such risk. By aligning security needs with business needs, the roadmap to the creation of a robust security architecture is "built-in" to the organization.

Reference Architecture

Every MSP organization has employees and workforce personnel with varying levels of security knowledge, but each MSP organization will likely have a diverse cybersecurity vision and a unique technology infrastructure to meet the needs of their business and clients. An MSP that provides services to a hospital or medical provider will almost certainly have a more focused security model than an MSP that provides services to a chain of restaurants.

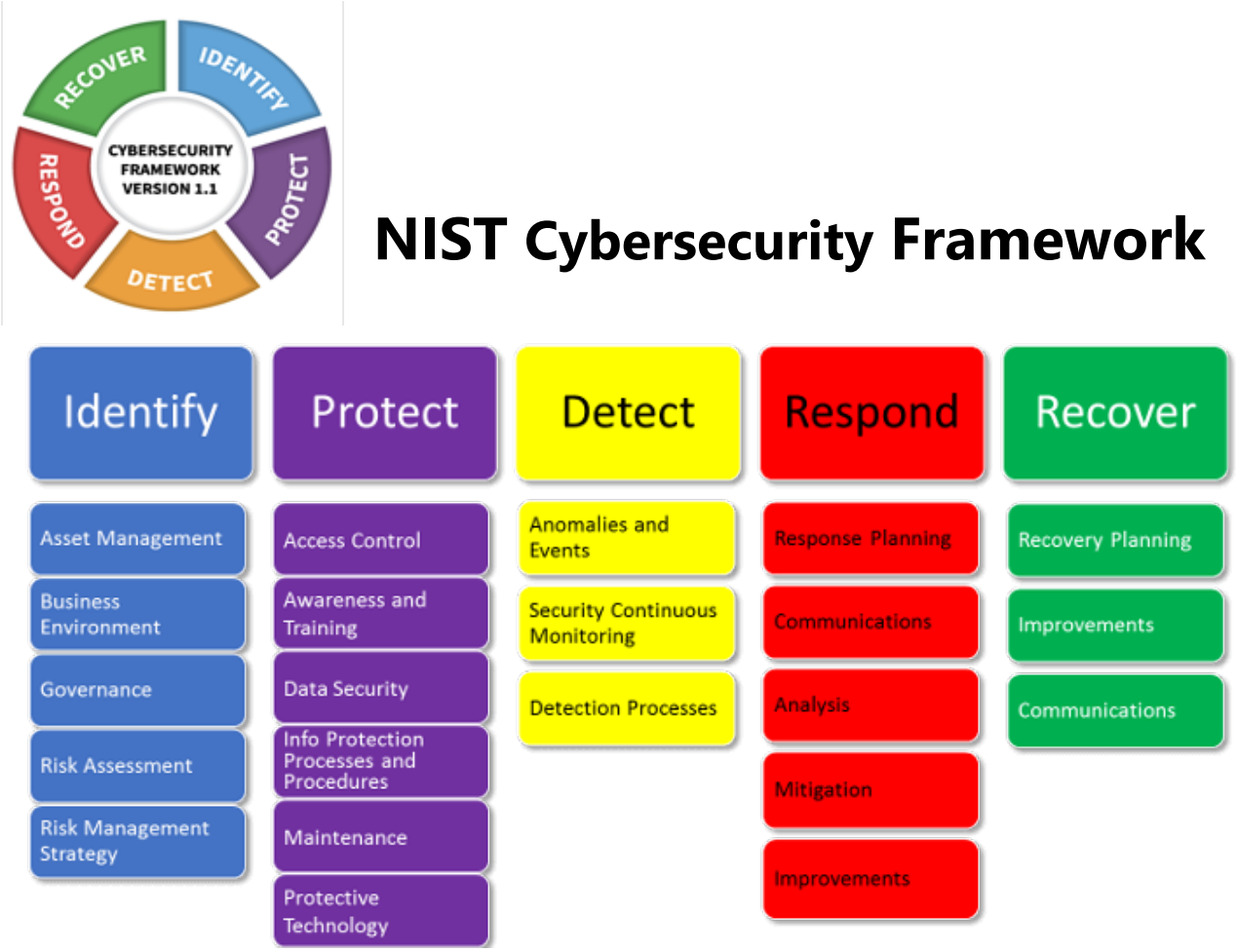
For all MSPs, their specific security and privacy requirements revolve around ensuring that the systems and data of their clients remains protected and secure while also ensuring that their own administrators and engineers do not unintentionally put that protection and security at risk.

Historically, security architecture has been focused upon protecting network perimeters with minimal focus upon the internal applications and data. With the rise of cloud computing and a remote workforce, the intricacy and complexity of implementing security controls across all access points, systems, and services has grown more difficult over time. With a standards-based implementation of a Zero Trust architecture, the complexity of planning an architecture model should improve overall cybersecurity without sacrificing the experience of the end user from any location.

Zero Trust is a security architecture concept of isolation, segmentation, or compartmentalization of the different parts that make up the interconnected assembly of technology and services to limit the effects from external cyber-attacks or unintentional configuration changes. A Zero Trust architecture strongly rests upon a collection of components and capabilities for identity management, asset management, application authentication, network segmentation, and threat intelligence.

A standards-based approach to implementing a Zero Trust architecture should begin with a nod to the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF can serve as a reference model for many Zero Trust architecture elements that an MSP can use to better understand, manage, and reduce its cyber security risks. NIST CSF assists organizations in determining which activities are most important to assure critical operations and maintain service delivery. This, in turn, helps prioritize investments and maximize the impact of every dollar the business spends on cybersecurity.

The NIST CSF framework has a common language to address cybersecurity risk management and is especially helpful in communicating both inside and outside the organization. Improving communications, awareness, and understanding among IT planning and operations, as well as senior executives of organizations, is crucial to establishing a vision for security architecture and planning.



NIST Cybersecurity Framework (CSF)

The NIST CSF is flexible by design. It can evolve to address shifting trends with cybersecurity threats, business processes, and emerging technologies. The NIST CSF sees successful cybersecurity as an active, continuous loop of response to both threats and solutions. Additionally, the NIST CSF works great for smaller or unregulated businesses across many different industries and verticals. Since the five high-level categories of NIST CSF (Identify, Detect, Protect, Respond, and Recover) allow for easier understanding and reporting of complex topics, NIST CSF is often used as a business reporting tool to inform senior leadership of security activities.

Many of the aspects of the IT Nation SECURE MSP+ Cybersecurity Framework and Zero Trust architecture models are derived from the NIST CSF. They have been customized to specifically address the business and security needs of the MSP and the services they provide to their clients. Additionally, the government of the United Kingdom (HMG) adopted a Minimum Cyber

Security Standard that was incorporated into its overall Government Functional Standard for Security for departmental security and (de facto) government contractors. The structure of the HMG Security Policy Framework (SPF), referenced by the Minimum Cyber Security Standard, is almost identical to the U.S. NIST CSF with five primary functions – Identify, Protect, Detect, Respond, and Recover.

Both U.S. and HMG frameworks emphasize the importance of data protection and provisioning access to a last-privileged (zero-trust) model. They both also drive continuous improvement in order to be ready for the next cyber-attack. To help secure the HMG's dependency upon its supply chain, the Minimum Cyber Security Standard asserts that vendors and suppliers meet the requirements defined within the U.K. Cyber Essentials. Operated through the U.K. National Cyber Security Center (NCSC), Cyber Essentials is an assurance and controls framework program designed to protect business from the most common internet-based threats and demonstrates their commitment to cybersecurity.

If a company or MSP intends to do business with the U.K. Government, and the company or MSP manages any aspect of personal and sensitive information, then that company or MSP cannot even bid on the contract without having completed Cyber Essentials certification.

Another influencer on the creation of the IT Nation SECURE MSP+ Cybersecurity Framework and certification is Australia's Essential Eight. The Australian Cyber Security Centre (ACSC) compiled a list of thorough, research-based mitigation strategies that organizations can use as starting points to improve their overall cyber security and flexibility. While there is no single, guaranteed mitigation strategy, the Essential Eight identified eight essential mitigation strategies that should be implemented to make it more difficult for cyber attackers to compromise systems. The Essential Eight offers guidance through a maturity model that steps through the mitigation strategies of application control, application hardening, patching applications, patching operating systems, configuring Microsoft Office, administrative controls, multi-factor authentication (MFA) and performing daily backups.

The Essential Eight is focused more on the day-to-day use of most office workers. It suggests minimal activities an organization should do. When compared to the NIST CSF, the Essential Eight does not really offer the more significant guidance NIST CSF provides to organizations for developing, testing, and communicating policies and procedures around network access and management, end-user education, and many other critical cybersecurity functions.

Zero Trust Architecture

There is no such thing as a one-size-fits-all approach to security, and each framework feeds into an overall security architecture based upon the needs of your MSP business and the specific needs of your customers. The core of the security architecture needs to be the zero trust model.

The U.S. National Institute of Standards and Technology (NIST) offers the following definitions of zero trust and zero trust architecture:

> ***Zero Trust*** provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a compromised network. ***Zero Trust Architecture*** is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a ***Zero Trust Enterprise*** is the network infrastructure (physical and virtual) and operational policies that are in place as a product of a Zero Trust architecture plan.

Across the internet, there are many publications, guides, and vendors attempting to document and define the doctrines of deploying a zero-trust architecture across an organization. Much of this guidance can be distilled down into the following principles:

- **Know, Understand and Document Your Assets and Architecture**
  In order to establish the foundation and harvest the benefits from a zero trust model, each resource and component of your architecture must be mapped throughout the computing services and data accessed. This includes all users, devices, services, and data sources that access or traverse your network.

- **Trust No Device**
  Uniquely identify, manage, and patch devices owned by your organization in order to foster secure asset management and vibrant visibility into the services and data the devices access. When connecting to resources or services provided by your organization, devices that are discovered to be compromised, have known vulnerabilities, and not managed by your organization may be treated in a different manner than those devices owned, managed, and secured by your organization. Within a bring your own device (BYOD) model, the security confidence and trust of the personal device is much lower. A personal device may only be allowed to access some resources and services, but not others.

- **Trust No Network**
  It is a best practice to not trust any network between the device and the service it is accessing. This includes your local company network. Assume that you have a malicious actor or device on your internal network. Incorporate policies and a network design that support communication in the most secure manner available through the authentication of all connections and the encryption of all network traffic.

- **Create Accounts Linked to Individuals**
  From within a single directory or identity service, enable granular access controls and create specific roles for each user. Ensure the directory or identity service can also be

utilized by all resources, services, and data - both internal and external to your organization.

- **Authenticate and Authorize Prior to Access**
  Systems and services, both internal and external to your organization, may be available for access directly over the internet, so the authentication of user requests requires a much stronger mechanism as opposed to the use of a simple username and password combination. A zero trust model requires the use of multi-factor authentication (MFA) and continuous monitoring with possible reauthentication and reauthorization throughout user interaction. This is defined and enforced by policy that attempts to attain a blended balance of security, availability, usability, and funding.

- **Define Data Access Policies**
  Control access requests to your services and data resources with policies. Resource access and action permissions policies can vary based on the sensitivity of the resource/data. A least privilege principle should be applied in order to limit both visibility and accessibility while protecting your data in transit with encryption.

- **Monitor Devices and Services to Improve Security**
  On any given day, most devices and services are exposed to network attack. An organization should monitor and collect device logs and network traffic data to ensure availability and performance. An organization should also analyze the collected data to identify rogue devices and malicious activity. The collected data and analytics can serve to help you improve security policy creation and enforcement.

Product Security

MSP organizations utilize a myriad of in-house / on-premise software and cloud-based SaaS. Additionally, there are many MSP organizations that develop and produce their own software solutions, appliances, or services. The functions of product security across your organization should be incorporated within a software development life cycle (SDLC). A SDLC includes existing design control, coding standards, quality testing and, release processes. Bringing your SDLC in alignment with your adopted security policies, standards, and practices allows you to produce solutions to better protect, not only your own business interests, but also the business and data security needs of your customers.

Core Security Concepts	Gathering Security Requirements	Secure Design Principles	Secure Coding Practices	Security Testing Tools & Techniques	Final Security Review Plan	Security Patch Management
Assurance Methodologies	Building Checklists & Defining Security Gages	Design Level Security Controls	Code Security Analysis	Security Defect Handling	Security Review & Response Processes	Handling 3rd Party Library Upgrades
Standards & Frameworks	Product Security Baseline	Threat Modeling	Secure Code Review	Security Metrics Development	Supply Chain Risk Mgmt.	Disposal Policy

- **Security Training and Awareness**
  Confirm that that every person in your organization understands the adopted security best practices and policies. Developers, engineers, and product manages will need specific training and guidance on security standards and requirements to write secure code and to implement security by design.

- **Security Requirements Review**
  In addition to the business requirements and functional needs necessary for development, it is also essential to define any security requirements during the early stages of development as part of the life cycle practice adopted by your organization. Keep in mind that security requirements will always need to be updated in response to functional changes, additional product features, updated regulatory requirements, or the evolving threat landscape.

- **Asset Catalog and Management**
  Identifying and documenting your applications and supporting assets remains a core life cycle practice and one of the first steps to securing your software and services infrastructures. Since many applications rely upon support from authentication domains, databases, IT infrastructure, third-party plugins, APIs, etc., an understanding of the application and its dependences remains principal to its successful operation and future development.

- **Security Design Review**
  Software and service design reviews remain a methodical, comprehensive, and well-documented examination process of all the components that have gone into the development of a product or solution. Such reviews are regularly scheduled throughout the development process in order to validate the design against specified requirements and previous development activities. The design review also helps with identifying any problems that may impact further development or meeting requirements.

- **Manual Code Review**
  With respect to security, a manual code review is the time-consuming process of reading source code line-by-line in order to potentially identify vulnerabilities. A manual review of source code is a tedious process performed by a software developer that must be trained in the review process and has the knowledge, experience, perseverance, and endurance required to complete the task. Throughout the manual review process, any flaws or vulnerabilities discovered will need to be documented and addressed in order to improve the security posture of your application or services provided.

- **Automated Vulnerability Testing**
  There are several common and open source tools that can be used to perform an analysis of the code you develop for your product and services. As a baseline security practice, your organization should use automated tools to perform vulnerability assessments of your code to discover any issues with injection, cross-site scripting, outdated libraries, broken authentication, or exposed data. Any identified vulnerabilities should be fixed or surrounded with mitigating controls.

- **Patch Management**
  Software maintenance, updates, and patches are all part of a life cycle practice. Your developers and product managers will need to actively prioritize the balance between the release of new features (enhancements) with that of patching security vulnerabilities (bug fixes).

- **Integration and Deployment**
  Application and services code development has a life cycle and your code will need to be protected and controlled throughout its development and deployment. You will need a system in place to maintain version control. Such validation may be managed by documenting a provable chain of custody or utilizing code signing or hashing. Additionally, your organization may run a testing or staging environment that mirrors your production environment where code can be promoted from development into testing into production after passing the requirements for each stage.

- **Secrets Management**
  To secure your product, application or services, Account IDs, passwords, tokens, security sensitive data and controls need to be protected with encryption during storage and while in transit. Access to such information should be limited to granted to only certain developers and engineers as a need to know basis. For example, your developers may not need access to the production accounts and password, but your support engineers may need to have production access for troubleshooting. Additionally, it is a good security practice to expire and rotate any keys, tokens, or passwords on a regular basis.

You should also log any changes for monitoring and auditing.

- **Third-Party Libraries**
  The use of third-party code or open-source libraries for development is a great way to save a good deal of time. However, adding such libraries and lines of code to your own product may introduce unforeseen vulnerabilities. There is no way to assure that the third-party entity that developed the code followed good security practices. Additionally, an organization will need to consider the licensing of third-party or open-source libraries and how they may be used within and resold as part of your own product. The use of third-party or open-source libraries should be part of your asset catalog to be monitored and managed for risk as appropriate.

- **Security and Risk Assessment**
  Prior to production launch and periodically, it is good security practice to hire a security professional to simulate the actions of a malicious hacker in order to perform an analysis of your software and systems via a penetration test (Pen Test). This type of assessment is conducted to discover potential vulnerabilities (e.g. coding errors, system configuration issues, buffer overflows, memory faults, or other environmental weaknesses) and can provide useful feedback on elements that may have been missed during development. Additionally, penetration tests and assessments are frequently conducted in conjunction with automated vulnerability testing tools and manual code reviews in order to provide a more comprehensive analysis.

- **Incident Response / Vulnerability Management**
  Everything eventually breaks. As part of your product security program, you will want to prepare an incident response plan in order to properly address new and emerging threats and vulnerabilities that are discovered over time. Your organization should create a standardized playbook with identified points of contact that outlines the protocols and procedures for responding to an incident. After the incident is addressed, any software maintenance, updates and patches should fall under the established patch management process, migrating a fix from development, to testing, and production.

- **Documentation and Training**
  Documentation in the form of a User's Guide or Administrator's Guide is standard as part of a delivery package for most software products and services. Your organization may also want to publish additional whitepapers that highlight best practices, features, or case studies to further inform the user about your offering. Training curriculum and classes may also be developed to deliver to your users. In addition to basic security awareness training, developers, engineers, and product managers will need specific security training and guidance on the backend operations and integrations.

- **Security Champions / Stakeholder Review**
  The best way to cultivate a security culture within your organization is to have security representatives from all departments across of your organization come together as a stakeholder or champions group. Your security champions need an established channel of communications and should meet regularly to share new ideas, receive training, review projects, and report information back to their departments. By establishing a partnership between development, engineering, and other business units, each security champion brings certain knowledge to the table as part of a feedback loop. This helps to bridge any gaps in communication and foster a better understanding of business needs and priorities.

- **Establish Metrics**
  The success of a product security program is defined by the metrics your organization deems important to the program. It is important to establish criteria that allows developers and engineers to fully understand the risks associated with common security issues, how to easily identify and properly correct security flaws found during development, and how to follow security and secure coding standards throughout the entire life cycle of the project.

- **Strategic Roadmap**
  Producing a roadmap of future, more mature versions and patch releases of your product allows your organization to present and prioritize any capital, initiatives, time, and resources needed. Roadmaps are a tool for the business to use in order to help ascertain their return on investment (ROI) and to help identify any additional risk the product vision may bring when aligned with other business initiatives.

Product Compliance

MSP organizations utilize a myriad of in-house / on-premise software and cloud-based SaaS. Additionally, there are many MSP organizations that develop and produce their own software solutions, appliances, or services. Depending upon the location or industry in which the product or service is being sold or utilized, there will be several laws and regulations you must comply with in order to operate. In short, your product compliance program should cover and monitor your policies, legal regulations, established standards, and documented requirements that apply to your solutions.

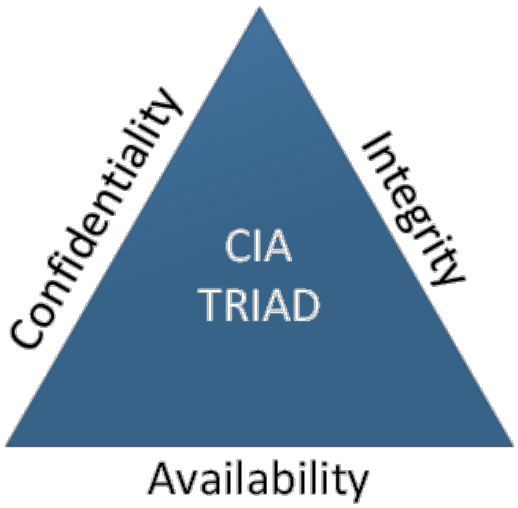
The following list contains a few of the most common governmental laws, industry regulations, directives, and standards that have the most impactful cybersecurity controls surrounding data and systems.

- National Institute of Standards and Technology - Cybersecurity Framework (NIST CSF) (U.S.)

- National Institute of Standards and Technology - Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5) (U.S.)
- National Institute of Standards and Technology - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST SP 800-171 Rev. 2) (U.S.)
- Office of the Superintendent of Financial Institutions (OSFI) Memorandum (Canada)
- Center for Internet Security Controls (CIS Controls)
- International Organization for Standardization - Standards for Information Security Management Systems (ISO/IEC 27001)
- International Organization for Standardization - Standards for Risk Management (ISO 31000)
- American Institute of CPAs (AICPA) - Service Organization Control (SOC) 2 Type II
- Health Insurance Portability and Accountability Act (HIPAA) / Health Information Technology for Economic and Clinical Health Act (HITECH) (U.S.)
- Federal Information Security Modernization Act of (FISMA) (U.S.)
- Security of Network Information Systems (NIS) Directive (EU)
- General Data Protection Regulation (GDPR) (EU)
- California Consumer Privacy Act (CCPA) (California, U.S.)
- Payment Card Industry Data Security Standard (PCI-DSS)

CIA Triad

As mentioned previously, confidentiality, integrity, and availability stand as the vital components of an effective cybersecurity program. Often cited as the 'CIA Triad,' the concepts of confidentiality, integrity, and availability are the guiding principles that many organizations use in order to tailor their compliance programs.



Confidentiality
Confidentiality is achieved by preventing or limiting the disclosure of information to unauthorized individuals or entities. Confidentiality of data may be addressed through physical or logical access controls, user identity and access management, and encryption.

Integrity
Integrity can be achieved by ensuring the accuracy and completeness of the data or systems that provide services. At a minimum, integrity involves monitoring the modification or deletion of files. Additionally, there are a variety of software tools and utilities available for integrity checking that compare hashed values and / or generate log entries upon the modification or deletion of files.

Availability
Availability ensures that reliable access to data and services is there when it is needed. Implementing high availability systems throughout your security architecture is one way to safeguard availability of data and services. High availability systems are intended to be fault tolerant and designed to prevent disruptions from power outages, hardware failures, and denial-of-service attacks.

Key components for an MSP to consider when assessing product compliance and designing a robust security architecture with a march towards compliance include:

- Visibility -- monitoring for change, performance, availability, auditability, and logging
- Access Control -- policies, identities, groups, granular controls, authentication, Multi-Factor Authentication (MFA), Single Sign-On (SSO)
- Secure Configuration -- lockdown based upon user profiles, consistent enforcement of policies and access controls, log management controls, user interface controls
- Auditability – tracking issues / vulnerabilities, reporting, security / risk scoring

Compliance stands as a critical chunk of any MSP cybersecurity strategy. An MSP environment with baseline security controls and point solutions may not necessarily meet all the needs for regulatory compliance and may not keep the most persistent cyber attackers from penetrating the organization. However, such controls serve as a vital foundation for implementing a solid cybersecurity architecture and compliance program.

People & Process

A healthy security architecture is built on three pillars—people, processes, and technology. Since technology and security architecture have been addressed within the above sections, the multiple roles of people and business processes throughout your MSP organization will need to be examined as well.

People Are the Worst

Due to the complexity of technology solutions (e.g., software, systems, services and platforms) modern companies routinely use to conduct their business, the operational risks posed by workforce personnel and human error are the greatest threat to your cybersecurity and protected data. The risk from the people in your workforce personnel far surpasses your risk from malicious actors and cyber attacks. However, having an experienced workforce knowledgeable about your business can also be an asset to your organization. They can be the first line of defense against such malicious activities.

People Can Be the Best

Regular security awareness training can serve as the foundation to help create a strong culture of cybersecurity across your organization. When senior management and executives commit to developing a positive culture around cybersecurity and invest in training for the roles and responsibilities of their personnel, the alignment with process and technology will blend to better protect your organization. Having a top-down approach for your cybersecurity culture may allow your organization to retain and rely upon those employees with the institutional knowledge and capability to maintain the security or your data and operations.

If you employ the right people with a positive attitude, relevant experience, and necessary qualifications and equip them with specific operational and cybersecurity training needed to be successful, the security culture will grow and flourish across your organization. To support the organization, specific security roles and responsibilities will need to be defined in order to limit access to only the systems and data needed to perform the job. In your MSP organization, consider the following roles and the level of access each would need in order to function without raising the risk of exposing protected data in the event of a breach.

- End Users
- Contractors
- Helpdesk
- DEV Ops
- Server / Systems Operations
- Security Operations
- Network Operations
- Third-Parties

No Plan Survives Contact with the Enemy

Every MSP organization must have proper processes and procedures in place in order to reduce

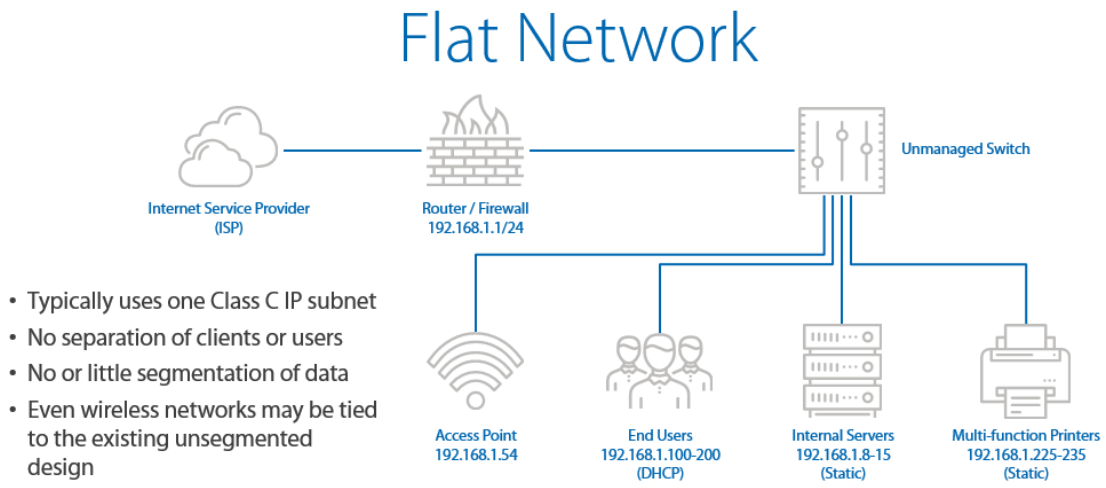
the risk of cyber threats. Processes define the business functions and activities, establish workforce personnel roles, and must exist in documentation in order to mitigate cybersecurity risks. As cyber threats constantly evolve and change, processes will need to be revisited and updated in order to address new threat vectors. Additionally, having a strategy and a process in place with a proper method to assess risk and threats will serve as the driver for the adoption of new technology and services to deal with those threats that may harm your business or your customers.

It is paramount that every MSP organization have a cyber incident response plan in place with repeatable procedures and a well-defined, orchestrated approach to handling a cybersecurity incident from discovery to recovery. The goal of the incident response plan and procedures is to quickly recover any disrupted business processes in the most efficient way possible. Efficient response processes are only viable if the MSP organization has invested the time and effort to fully examine and document their IT assets, security architecture, and service dependencies. With prior emphasis on governance, policy development, adoption of standards, and implementation of technology aligned with risk tolerance and business objectives, everything blends into the critical processes designed to enhance the visibility and insight into your organization, shorten threat response times, and minimize the impact to your business and customers.

Secure Network Topology

This section will discuss what good should look like for your network environment to ensure minimum impact and damage in the likely event of a cybersecurity threat.

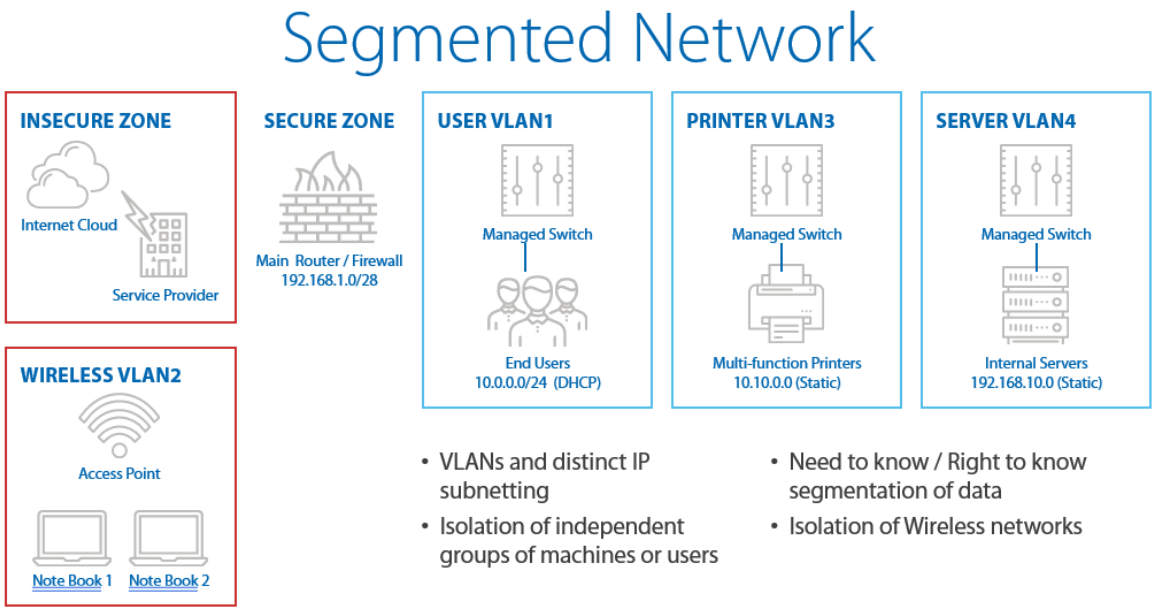
What is Not So Good



Flat networks, like the one above, will cause significant damage and impact to your business. This is also true for your clients. An attacker only needs access to one system within the flat

network to discover all of the other devices and potentially gain access to them and their information. A better network design is below.

What Good Looks Like



Segmentation provides better management and control over your network infrastructure. You will need to deploy a managed switch or switches depending upon the number of segments you need. As an example, an MSP with a workbench should segment that space from all other areas of the business and consider it unsecure. In addition, your internet facing tools should be segmented in a DMZ to prevent those applications, like your Remote Management and Monitoring (RMM) solution, from being used to launch an attack against you.

Case Studies

The following are a few examples of cases from the field that highlight some of the danger and disruption that may occur to an MSP organization that operates without employing basic, fundamental security best practices – many of which have been highlighted within the IT Nation SECURE MSP+ Fundamentals Yellow Book.

Case Study: Never Leave RDP Open to the Internet

The Remote Desktop Protocol (RDP) is a convenient way for one computer to connect to another computer across a network which allows a user to login to a graphical, remote desktop session and use the remote computer as if they were at a physical keyboard and monitor. By default, RDP client software is part of the base install of Microsoft Windows client OS (Windows XP / 7 / 8 10) and can be configured to run as a service on Windows and UNIX/Linux servers.

Since the release of Microsoft NT Terminal Services in the 1990s, the use of RDP was rapidly adopted by many IT professionals to remotely manage their own servers without the need to get up from their desk and enter the server room. RDP helped organizations lower the cost and complexity of addressing support issues. As it matured, the platform quite literally laid the foundation for the modern MSP industry that currently thrives on the capacity to remotely manage client computers without the need for an onsite physical presence.

Due to the convenient nature of RDP, over the past couple of decades, countless servers have been deployed and configured to allow RDP access. Unfortunately, an improperly secured server hosting RDP services can be an organization's most dangerous vulnerability – especially when directly open to the internet. By default, the RDP service listens for inbound connections over TCP/UDP port 3389, and the Internet is constantly scanned for those listening ports to identify potential hosts as targets for attack and compromise. A quick search on Shodan, a search engine for internet-connected devices, reveals that the number of devices exposing RDP to the Internet has grown over the past months since March 2020. An upward trend easily explained due to the pandemic as many organizations have moved their office workforce to a remote workforce. Link to Shodan RDP search: https://www.shodan.io/search?query=RDP

One may believe that the use of RDP may be safe when account credentials include the use of complex passwords. While this may be true to a degree, there are many user accounts with compromised credential that can be purchased in bulk from dark web marketplaces. With thousands of "hacked" enterprise accounts available for malicious attackers to purchase and use, the complexity of passwords does not offer much protection as RDP can be vulnerable to "brute force" password guessing attacks that can easily be scripted with "hacked" credentials. Such attacks and ultimate access via RDP services may lead to a ransomware infestation or a data breach for the organization.

The IT Nation Secure team has witnessed many bad things happen over RDP services open to the public internet without the use of a VPN or multi-factor authentication (MFA). The team has

seen everything, including attackers obtaining access to a full Microsoft Windows Domain Administrator account by guessing the password for an account used for a vulnerability scanning platform where "scanner" was the account password. As part of the Domain Administrator group within Active Directory, the scanning account had rights to use RDP and could easily remote into the organization. After access had been obtained, the attacker worked to gather information and establish additional accounts to maintain their administrative access and privileges.

The attacker used their newly found access to spread ransomware across most of the servers and workstations across the organization. As a result, the organization was unable to conduct regular business operations over a two-week period. To make matters worse, the attacker had laterally moved across the network to the backup servers, removed all backup files, and then encrypted the backup servers leaving the organization without a way to recover the infected servers, applications, and critical data.

The following list provides a few recommended mitigating actions to adopt to avoid this scenario:

- Never Leave RDP Open to the Internet (block external RDP access from the public Internet by dropping inbound TCP/UDP port 3389 connection attempts at the firewall).
- Require the use of a VPN gateway for users to connect remotely to the organization.
- Implement the use of multi-factor authentication (especially for all accounts that require remote access or need to use RDP).
- Limit the use of RDP to only those workforce personnel who require access to perform their daily work.
- Do not allow service accounts with domain administrator-level privileges to have the rights to access RDP.
- Limit the number of failed login attempts an account can perform and lock the account after a certain number of failed attempts.
- Employ network segmentation and establish VLANs to better isolate and protect critical systems and data.
- Plan for the worst-case scenario and utilize the 3 / 2 / 1 backup methodology to ensure that 3 copies of the data are stored on 2 different types of media with 1 copy stored off-site.

Case Study: Let's Go Phishing

Phishing involves the use of email messages and trickery by a malicious party to entice an email user to fall for a scam that may potentially reveal private or sensitive information (e.g. financials, passwords, credentials, etc.). Such attacks can be very damaging to an organization when the credentials of a systems administrator are compromised as a result of a successful phishing venture.

Spear phishing is very similar to regular phishing but involves sending phish emails to a well-researched individual to present the email as originating from a trusted, known source, thereby being safe to open and the contents legitimate. With the use of social media sites for both personal and business networking (e.g. LinkedIn, Facebook, Twitter, etc.) as well as event and conference listings proudly displaying the names and titles of panelists and presenters, socially active IT professionals will find it increasingly difficult to maintain a low profile. Spear phishing excels at compromising high-profile targets as detailed reconnaissance work is key for a malicious actor to successfully spear a target.

A systems administrator within a large enterprise organization was specifically targeted and spear phished with an email message that appeared to be from one of the conference organizers at an where the systems administrator was to present during a session. The email looked legitimate and stressed some urgency due to some last-minute changed in the schedule of events and asked the systems administrator to open a PDF attachment to view the changes and to confirm their schedule.

Once the systems administrator clicked on the attachment, they unknowingly infected their computer by installing a remote access trojan (RAT) keylogger that collected typed information and data from the compromised computer to send back to the attackers. Unfortunately, what appeared to be a PDF attachment in the email was just an image of a PDF attachment that was embedded with a hyperlink to a URL to download the RAT malware. To further enhance the legitimacy of the ruse, after the RAT was quickly downloaded, the systems administrator's browser was redirected to the real schedule page of the conference website.

Once the RAT was installed and called home, the attackers began to take advantage of the access provided by way of the system administrator's elevated access and permissions to map the internal network and search for additional systems to compromise. Before being discovered, the attackers were able to exfiltrate over a gigabyte of data files and had scanned the network attempting to identify business-critical systems. The compromise was identified later the same day the systems administrator received and opened the spear phishing email.

In this case, the financial organization was fortunate as the RAT malware infection and compromise was limited to only the computer used by the systems administrator. Additionally, the organization, invested in appropriate security monitoring and logging platforms along with a full-time staff of analysts and subject matter experts skilled in the cybersecurity arts of digital forensics and incident response. From the initial alerts, the response team was able to quickly identify the computer of the systems administrator as the source of a large volume of outbound traffic to a sketchy IP address located in a foreign county and as the source for a port scan walking the hosts on the internal network.

Since the financial organization had the technology and the expertise to identify the source of the alerts, take the compromised computer offline, and temporarily suspend the systems administrator's user account; they were able to minimize the loss of information and contain the

attackers from engineering additional compromise. Upon further analysis, the exfiltrated information was a dump of the systems administrator's local documents folder that contained some personal data, several network diagrams, and sensitive details surrounding several IT projects.

Often it is the user who is the weakest link within any established cybersecurity practices. Even though the victim of the spear-phishing attack was a seasoned IT professional, they fell for a very elaborate ruse designed to solicit the expected action of clicking on an attachment (from a trusted source) with familiar subject matter. Under such circumstances, the only protection one may have is to develop an unhealthy amount of paranoia. However, after this incident, the financial organization stepped up their security awareness training with a laser focus on providing their workforce personnel the practical lessons and specific examples of how to spot a well-crafted phish or spear phish email. The value of security awareness training and simulation tests cannot be stressed enough. Organizations must enable their workforce personnel to constantly be diligent when it comes to spotting the signs of a fraudulent email.

In addition to providing security awareness training, the financial organization also invested in the following technologies and programs that allowed them to identify and contain and mitigate the incident:

- Security Event and Information Management (SIEM) tools to collect logs and events from network boundary protection devices (e.g., firewalls, web gateway, intrusion prevention systems (IPS), etc.) to show the exfiltration connection to an IP address located in another county.
- Event logs from the endpoint protection software located on the infected computer (though the endpoint protection software did not block the installation of the malware) were able to block and alert on the attempts to make connections to other hosts computers.
- A well-organized security program in place with a competent security response team that effectively utilizes their tools to identify, triage, and contain the incident.

MSP+ Education Program

The MSP+ Education Program provides the training and resources for MSPs to successfully meet the Security Fundamentals baseline for participation in the MSP+ Framework. MSPs that embark on the SECURE MSP+ journey better position themselves for business resilience and successful growth in today's cybercrime landscape.

ConnectWise Certify Fundamentals courses should be considered the launching pad for the MSP+ Security Journey. Skills, solutions, and processes learned in the Fundamental Education serve to guide the MSP to self-assess their maturity levels within each attribute of the Security Journey and enable the MSP to create their own roadmap to move into the next levels identified to be most critical.

The Security Journey is reviewed in both the Certify Cybersecurity Fundamentals for Sales and Certify Cybersecurity Fundamentals for Engineers courses, as well as available for review in-depth via the ConnectWise University. At the Fundamental level of the MSP+ Cybersecurity Framework, the goal is to move the MSP from Orange through Yellow in maturity.

MSPs can focus the ConnectWise Certify Fundamental Education based on two specific roles within the MSP: The Engineers (technical) role and The Sales role. The Certify Fundamental courses specific to each role provide the necessary baseline education to align team members within the MSP on cybersecurity risk management, security solutions, policies, processes, and secure implementations.

There are no pre-requisites for the ConnectWise Certify Fundamental courses, but it is recommended that the participants have familiarity with the MSP industry and common MSP vendor solutions.

ConnectWise Certify Fundamental Education Baseline

A combination of both the Engineer and Sales roles participating in the Fundamental Education will net the best results, as it is recommended that 100% of the technical personnel (Engineers) and 100% of the Sales personnel pass the Certify training in the ConnectWise Certify Fundamental Education Program before moving into the MSP+ Advanced Educational Program.

The Partial/Ad Hoc nature of the Fundamental Level MSP renders itself to simple, baseline security education. Overall Governance status of this Fundamental level MSP would be described as having minimal InfoSec policies in place, being arbitrarily communicated and employee acknowledged. The Privacy and Security programs would include an understanding of and guidelines for a Breach Response Plan, Security Awareness Training, Vulnerability Management, DR/BC Plans, Security Architecture, and Incident Response Management. Education and resources to achieve the baseline understanding of guidelines for the ConnectWise Certify Fundamentals status would be included in the Certify Fundamentals courses, the detailed Fundamentals books, the ConnectWise University, and via security industry resources.

MSP+ Fundamental Education Resources

Education specific to MSP and SMB environments combined with industry-recognized cybersecurity training and certifications makes for a valuable, immediately applicable, and appreciable breadth of cybersecurity knowledge.

Because everyone learns differently, several types of cybersecurity training and resources are available to the MSP community. At the Fundamental level, a combination of resources is recommended:

- The MSP+ Fundamental book
- ConnectWise Certify Cybersecurity Fundamentals for Sales and ConnectWise Certify Cybersecurity Fundamentals for Engineers courses
- Online learning via ConnectWise University
- Industry-recognized bodies of knowledge

Certify Cybersecurity Fundamentals Certification Courses

Participating in MSP-specific cybersecurity courses designed to focus on MSP roles allow for peer learning and knowledge sharing within and outside of the coursework. When possible, pair education between the Engineers team members and the Sales team members in complimentary programs, rather than relying on technical cybersecurity knowledge alone to fortify the MSP. This sets up the MSP for success heading into the MSP+ Advanced and Master Education Programs.

The ConnectWise Certify Cybersecurity Fundamentals certification courses are designed to achieve most of the learning required in the Fundamental level of the MSP+ Framework. Offered as full-day cybersecurity classes, both tracks are available at no charge to MSPs and each track tests the knowledge of the participant at the end of the course. For more information on the **Certify Cybersecurity Fundamentals for Sales** and **Certify Cybersecurity Fundamentals for Engineers** courses, see the following sections below.

ConnectWise University – Online Resources

To provide for fluctuating time availability of the MSP technical and sales team members, online learning specific to MSP roles is available via the ConnectWise University. A large section of the ConnectWise University is dedicated to cybersecurity, and offers the following types of learning:

The Security Journey

The Security Journey is a framework for growing a security practice in your business and industry. It helps you understand where you are in the journey and how to navigate through it with the ABCDs in each phase: Attitudes, Behaviors, Consequences, and Discussion.

The journey consists of four distinct phases. Each phase focuses on developing a security practice for your business going from beginning knowledge to establishing a practice that'll protect your company from harm.

The goal of this course is to define the security journey and guide you through each phase to get you to start implementing security practices into your company.

The Partner Kit Library > Security
A Partner Kit is a collection of resources that teach you how to implement a service or process using a ConnectWise® product. Kits are packed with expert business insights and recommended practices. They might include videos, white papers, articles, Blueprints, or other tools that help you tackle processes like onboarding, organizing service boards, or even marketing. A kit has been created to focus on cybersecurity.

Staying ahead of cybersecurity threats can be a challenging job for technology professionals. Building a security practice can be a complex (even daunting) endeavor for MSPs. ConnectWise has teamed up with industry-leading security providers to offer solutions and integrations designed to reduce the risk of external attacks, with the protection of user accounts and endpoints. That said, there are industry best practices and paths to achieve a maturity model that is right for you. This partner kit helps you make sure that your practice is positioned for success.

Security Video Library
Understanding the basics of NIST, Putting NIST into Practice, Building your TSP Cybersecurity Practice, and many more videos and courses are available within the online library.

Not using ConnectWise solutions yet, and unable to access ConnectWise University? Contact your account rep for more information.

Industry Resources

Several free additional resources are available to MSPs that are specific to supporting SMBs. This list is not meant to be inclusive but assists in moving the MSP forward to obtain fundamental level cybersecurity knowledge to help meet the SECURE MSP+ Fundamental Education baseline.

- NIST Frameworks https://www.nist.gov/cyberframework
- NIST for MSPs https://www.nccoe.nist.gov/projects/building-blocks/managed-service-providers
- CIS v7.1 for SMBs https://www.cisecurity.org/controls/cis-controls-list/
- NCSA https://staysafeonline.org/
- SANS https://www.sans.org/security-resources/?msc=main-nav
- The MSP vendor community has many free webcasts and resources found on their websites, newsletters, etc.
- ISACA https://www.isaca.org/resources
- Computer Emergency Readiness Team Coordination Center (CERT/CC) https://www.kb.cert.org/vuls/
- Multi-State Information Sharing & Analysis Center (MS-ISAC) https://www.cisecurity.org/ms-isac/

- National Council of Information Sharing and Analysis Centers https://www.nationalisacs.org/member-isacs
- US-CERT National Cyber Awareness System https://www.us-cert.gov/ncas

Next Steps

Once the MSP+ Cybersecurity Framework Fundamental requirements are met, MSP staff can look forward to improving their cybersecurity posture and growth opportunities by moving into the Advanced and Master levels of the MSP+ Cybersecurity Framework. An overview of the MSP+ Educational Resources for the Advanced and Master levels can be found in the following sections below.

Certify Fundamentals for Engineers

This section provides an overview of the Certify Cybersecurity Fundamentals for Engineers course description and purpose, as well as where the course fits into the MSP+ Cybersecurity Framework.

This full-day course covers the baseline knowledge of Cybersecurity from the perspective of a technical (Engineer) role within an MSP.

Technical knowledge for IT support is only a small portion of how Information Security and Information Technology need to adapt and work together in the MSP+ Cybersecurity Framework. Understanding what good looks like for secure implementations inclusive of people, process and technology is key to successful adoption of security practices within the MSP Security Journey roadmap.

Ideally, all MSP team members that serve in a technical or service delivery capacity will complete the Certify Cybersecurity Fundamentals for Engineers course, so a common language, baseline skillset, and alignment of objectives take shape within the MSP.

In the MSP+ Cybersecurity Framework, the Certify Cybersecurity Fundamentals for Engineers will specifically address most of the baseline education requirements. The complementary Certify Cybersecurity Fundamentals for Sales course is described in the following sections.

Certify Cybersecurity Advanced for Engineers and Certify Cybersecurity Master for Engineers are the next levels of MSP Specific education required within the MSP+ Cybersecurity Framework and are described in more detail in the Next Steps section of this book.

Complementary industry cybersecurity certifications to the Fundamentals courses are also listed in the Next Steps section of this book.

Certification holders can demonstrate a baseline knowledge of fundamental level Engineer-specific cybersecurity practices along with resources needed to meet most of the Fundamental requirements of the MSP+ Cybersecurity Framework. CEUs (up to 8) are available from some certification bodies for participation in this course.

This full-day course covers the basics of MSP+ Cybersecurity Framework, NIST 800-53, and an overview of the CIS 20 Controls with a deep dive into the first six basic controls:

- A secure onboarding process
- • An overview of the cybersecurity technologies and solutions ecosystem and the problems for which they each solve
- The principles of security architecture
- Understanding risk and business impact and how the technical and physical assessment process determines outcomes for the risk conversation
- A basic overview of the concepts behind malware analysis and intrusion detection
- Incident response planning (before, during and after an incident)

Pre-requisites for the ConnectWise Certify Fundamental Education Program do not exist, but it is recommended that the participants have familiarity with the MSP industry and vendor solutions.

Learning Objectives

Security Journey – Understand the different phases of maturity as they apply to attributes of a SECURE MSP+ practice, where the MSP fits into each phase, to identify key areas for improvement, and what level of maturity the MSP desires to have within each attribute, as an overall objective.

Security Culture – Understand the critical areas of awareness, behavior modification, discussion, and culture transformation in support of a SECURE MSP+ practice.

Governance – Understand what governance is for an MSP and the role it plays in risk management.

Cybersecurity 101 – Understand basic cybersecurity concepts and definitions.

Frameworks – Understand what a Framework is, how it applies to the MSP+ Cybersecurity Framework. As well as which ones are most commonly used on both a global and national basis, how they complement or intersect with each other, and why Frameworks are important.

NIST Overview – Identify the core areas and functions of NIST 800-53 and NIST for MSPs and how these areas of the Framework apply to MSPs and their SMB clients.

Controls – Understand the three areas of security controls, an overview of industry-standard CIS 20 Controls, and varying degrees of rigor within control implementation.

Security Architecture Principles – Understand how to apply security architecture principles and identify components of a security architecture.

Secure Onboarding Process – Understand components of a secure onboarding process checklist and implementation of priority items.

Risk Management – Understand risk management concepts and methodologies.

Risk Assessments – Understand the varying types of assessments, their purposes, and use-case scenarios, and the role of Engineers in the assessment process.

Building your Stack – Understand how to select, implement, and support cybersecurity solutions.

Malware Analysis – Understand the different types of malware, malware analysis concepts, and methodologies.

IDS Concepts – Recognize the methodologies and techniques for detecting host and network-based intrusions via intrusion detection and intrusion prevention technologies.

Incident Response – Understand the incident response and handling methodologies.

Coursework Description

At the Fundamental level of the ConnectWise Certify Fundamental education, MSP technical team members must understand and appreciate how their choices, actions, and thought processes affect the overall security posture of the environments they support. The Learning Objectives selected for review as part of the Certify Cybersecurity Fundamentals for Engineers course provide the baseline understanding of how people, process and technology align to create a SECURE MSP+ and SMB profile, and empower the Engineer to make informed and consistent choices behind their decisions and actions.

Cybersecurity Journey

What is the Cybersecurity Journey and why is it important?

The Security Journey is a framework for growing a security practice in your business and industry. It helps you understand where you are in the journey and how to navigate through it with the ABCDs in each phase: Attitudes, Behaviors, Consequences, and Discussion.

The journey consists of four distinct phases. Each phase focuses on developing a security practice for your business going from little knowledge to establishing a practice that'll protect your company from harm.

The goal is to define the security journey and guide you through a high level of each phase to get you to start implementing security practices into your company.

Cybersecurity Culture

What is Cybersecurity Culture and why is it important?

The culture of an organization refers to the beliefs, norms, values, assumptions, knowledge, and attitudes of its team members. In the context of cybersecurity, influencing these attributes of the individuals and the team in aggregate directly corresponds to the successful adoption of security solutions and practices. Understanding what influences these cultural attributes and how to best incorporate those influential activities into the daily communications, processes, and leadership initiatives is key to building a security-focused organization.

Governance

Why is Governance important to understand?

Governance within an organization is broadly defined as the rules that run that organization, including the policies, standards and procedures that are used to set the direction (strategy) and control the organizations activities.

In cybersecurity governance, it is important that the organization objectives and strategy are aligned with the info sec policies, so that the resources appropriated to mitigate risk (controls) are suitably matched with the company mission and priorities.

Governance: Cybersecurity 101

Why is understanding Cybersecurity 101 important?

Cybersecurity 101 encompasses the fundamental security concepts such as CIA (confidentiality, integrity and availability), PPT (people, process and technology), Frameworks and Controls. Understanding the concepts themselves and how they intersect, complement, and layer with each other is crucial to designing an effective risk management program.

Governance: Frameworks

What is a Framework and why is it important?

Cybersecurity Frameworks are a system of standards, guidelines and best practices to manage risks that arise in a digital world. The Cybersecurity Framework helps to prioritize risk mitigation strategies where vulnerabilities and threats might affect the ability for an organization to achieve their objectives. Frameworks should provide for flexible and cost-effective approaches to promote the protection and resilience of the organization.

Governance: Overview of NIST 800-53

What is NIST 800-53 and why is it important?

The NIST 800-53 Framework is the gold standard in cybersecurity frameworks in the United States and it is respected worldwide. The overview of this framework serves to provide a basic understanding of what the framework contains, how it works, how it is applied, and how it intersects with and complements additional frameworks and regulations.

Additionally, NIST's 2019 publication on Improving Cybersecurity of Managed Service Providers and subsequent publication on PR.IP-4 Backups is important to understand for implementation and support purposes. As each additional publication is released, in depth curriculum and resources will be added to Certify Fundamentals for Engineers coursework, to ensure continual improvement for MSPs as they pertain to current NIST guidelines.

Governance: Controls

What is a control and why is it important?

Cybersecurity controls are grouped into three areas: Administrative, Technical and Physical. Understanding the difference between these types of controls, the purposes they serve, how and why layers of controls are important, and the varying degrees of control implementation serves to enable MSP Engineers to identify and recommend appropriate solutions to mitigate risk. Technical controls are explored in depth in the Certify Cybersecurity Fundamentals for Engineers coursework.

Security Architecture

What is Security Architecture and why is it important?

Understanding the difference between network styles (flat, segmented) and the pros and cons of each will help the MSP identify infrastructure design that does or does not meet risk management objectives set by their SMB clients.

Secure Onboarding Process

What is the Secure Onboarding Process and why is it important?

The secure onboarding process has been developed for MSP engineers as a guide to incorporating the highest priority security solutions and processes within the MSP and their SMB clients. The checklists of these functions are broken into three key areas:

- Things you can do this month
- Things you can do within six months
- Things you can do within 12 months

The Certify Cybersecurity Fundamentals for Engineers coursework walks through all three sets of checklists but focuses in on the key elements to successfully incorporate the activities and processes in the "Things you can do this month" checklist.

This coursework also includes resources for Core Solution System Hardening guidance for ConnectWise security solutions.

Risk Management

What is Risk Management and why is it important?

Risk Management is a process aimed at balancing opportunities for gain (revenue, resources) while minimizing vulnerabilities and loss. The management of risk to information resources is a fundamental function of the MSP to understand and incorporate into their thought processes, communications, recommendations and implementations.

Having a baseline understanding of how to address risk and business impact in conversations and assessments as part of risk management is key to an MSPs successful deployment of security solutions.

Risk Assessments

What is a Risk Assessment and why is it important?

MSPs are commonly unable to distinguish between the activities included in varying forms of assessments: Network Assessment, Security Assessment, Vulnerability Assessment, and Penetration Testing. Understanding the problems each type of assessment solves for and use-case scenarios is important, as well as what is included in each type of assessment.

In the Certify Cybersecurity Fundamentals for Engineers coursework, we explore the role of the Engineer in the Security Assessment process.

How to Build Our Stack

What is the How to Build Our Stack coursework and why is it important?

Putting together a comprehensive security solution stack is a challenge for many MSPs. This coursework guides the process for determining what solutions go into the stack, considerations on margins and pricing, implementation best practices and support resources needed for those solutions. Additionally, scalability challenges are reviewed in this training.

Malware Analysis

What is Malware Analysis and why is it important?

Understanding the different types of malware and the attack process is integral to an Engineers success in supporting the identification, protection, detection, response and recovery of an organization's assets.

Intrusion Detection Concepts

What are Intrusion Detection Concepts and why are they important?

MSPs support environments that extend well beyond the office walls and firewalls that historically served to protect the organizational assets. Understanding the difference between intrusion detection and intrusion prevention, as well as the capabilities, purpose and proper configuration of SIEM solutions guides the Engineer to successfully recommend and implement protection according to the needs of the organization.

Incident Response Planning

What is Incident Response Planning and why is it important?

MSPs struggle to simply keep up with new technology, new threats, and ongoing security program improvement. Being able to confidently manage an incident response program is integral to establishing trust and leadership through the cybercrime landscape with their SMB clients. The fusion of training to key aspects of the incident response alongside a playbook to follow, helps the Engineer to understand their role in management of an incident.

Topics such as policy creation, plan development and preparation, detection and analysis of incidents, identification, containment, remediation, and recovery from the incident are explored as a baseline.

Next Steps

Once the ConnectWise Certify Fundamental requirements are met, MSPs can look forward to improving their cybersecurity posture and growth opportunities by moving into the Advanced and Master levels of the MSP+ Cybersecurity Framework. An overview of the MSP+ Educational Resources for the Advanced and Master levels can be found in the following sections below.

Certify Cybersecurity Advanced for Engineers (Green Book)

This program takes Engineers into real-world tactical and planning exercises covering the full 36-point checklist for a secure onboarding process; conducting an assessment to determine risk and business impact; and blue team exercises. Labs and scenario projects are included.

Similar Courses: CompTIA Security+, (ISC) SSCP, Microsoft MTA Security Fundamentals

Certify Cybersecurity Advanced for VCIOs (Green Book)
This program takes Owners and Sales Management Professionals into real-world governance strategy planning exercises to establish a real-world risk management program. Highlights include asset value determination, scenario planning, business impact analysis, budget and resource planning, and scalability strategies. Labs included.

Similar Courses: GIAC Information Security Fundamentals, ISACA CSX Fundamentals

Certify Cybersecurity Master for VCIOs (Blue Book)
This program takes Owners and Security Program Managers from creation of real-world risk management program with continuity and planning exercises, to 3rd party risk management and establishing KPIs. Labs included.

Similar Courses: (ISC) CISSP, ISACA CISM

Certify Fundamentals for Sales

This section will provide an overview of the Certify Cybersecurity Fundamentals for Sales course description and purpose, as well as where the course fits into the MSP+ Cybersecurity Framework.

This full day course covers the baseline knowledge of Cybersecurity from the perspective of a sales role within an MSP.

Sales knowledge for IT solutions and support is only a small portion of how Information Security and Information Technology need to adapt and work together in the MSP+ Cybersecurity Framework. Understanding what good looks like for risk-based conversations, conducting assessments, presenting on solutions and ongoing secure governance is key to successful adoption of security practices within the MSP Security Journey roadmap.

Ideally, all MSP team members that serve in a sales capacity will complete the Certify Cybersecurity Fundamentals for Sales course, so a common language, baseline skillset and alignment of objectives takes shape within the MSP.

In the MSP+ Cybersecurity Framework, the Certify Cybersecurity Fundamentals for Sales will specifically address some of the baseline education requirements. The complementary Certify Cybersecurity Fundamentals for Sales course is described below.

Certify Cybersecurity Advanced for Sales and Certify Cybersecurity Advanced for VCIOs are the next levels of MSP Specific education required within the MSP+ Cybersecurity Framework and are described in more detail in the Next Steps section below.

Complementary industry cybersecurity certifications to the Fundamentals courses are also listed in the Next Steps section of this section.

Certification holders will have proven a baseline knowledge of fundamental level Sales-specific cybersecurity practices along with resources needed to meet some of the Fundamental requirements of the MSP+ Cybersecurity Framework. CEUs (up to 8) are available from some certification bodies for participation this course.

This full day course covers the basics of NIST 800-53 plus the NIST for Managed Services Providers overview; the Cybersecurity Controls with a deep dive into the administrative controls; the fundamentals of the risk conversation and the security assessment process; an overview of cybersecurity technologies and solutions in the MSP ecosystem; how to build a cybersecurity sales roadmap and measure outcomes; discovering the underlying pain and risks to compel an open conversation around cybersecurity; using a risk-based or product-based conversation to convey the threat landscape and determine ownership of risk; addressing the most common objections of SMBs; delivering a live customized version of a risk presentation or security awareness training; and business outcomes that include a review of assessment tools and reporting, essential security package recommendations and how to have the budget and priority conversation.

Pre-requisites for the ConnectWise Certify Fundamental Education Program do not exist, but it is recommended that the participants have familiarity with the MSP industry and vendor solutions.

Learning Objectives

Security Journey – Understand the different phases of maturity as they apply to attributes of a SECURE MSP+ practice, and where the MSP fits into each phase, in order to identify key areas for improvement and what level of maturity the MSP desires to have within each attribute, as an overall objective.

Security Culture – Understand the critical areas of awareness, behavior modification, discussion and culture transformation in support of a SECURE MSP+ practice.

Governance – Understand what governance is for an MSP and the role it plays in risk management.

Cybersecurity 101 – Understand basic cybersecurity concepts and definitions.

Frameworks – Understand what a framework is, where the MSP+ Cybersecurity Framework applies, which other frameworks are commonly used on both a global and national basis, how they complement or intersect with each other, and why frameworks are important.

NIST Overview – Identify the core areas and functions of NIST 800-53 and NIST for MSPs and how these areas of the Framework apply to MSPs and their SMB clients.

Controls – Understand the three areas of security controls plus an overview of industry standard CIS 20 Controls and varying degrees of rigor within control implementation.

Risk Management – Understand risk management concepts and methodologies.

Risk Assessments – Understand the varying types of assessments, their purposes and use-case scenarios and the role of the salesperson in the assessment process.

Cybersecurity Technologies – Understand how to select, implement and support cybersecurity solutions.

Sales Roadmap – Understand the qualifying questions that help to build out a good client discovery, preparing to present to a client or prospect, how to present on Cybersecurity Risk or Security Awareness Training, and objection handling.

Business Outcomes – Understand how to create an Action Plan from the Security Profile and where automation can save resources and provide for scalability in the quote, order and implementation process.

Coursework Description

At the Fundamental level of the MSP+ Cybersecurity Framework education, MSP sales team members must understand and appreciate how their choices, actions and thought processes affect the overall security posture of the environments they sell to. The Learning Objectives selected for review as part of the Certify Cybersecurity Fundamentals for Sales course provide the baseline understanding of how people, process and technology align to create a SECURE MSP+ and SMB profile, and empower the Salesperson to make informed and cost effective choices behind their recommendations for security solutions.

Cybersecurity Journey

What is the Cybersecurity Journey and why is it important?

The Security Journey is a framework for growing a security practice in your business and industry. It helps you understand where you are in the journey and how to navigate through it with the ABCDs in each phase: Attitudes, Behaviors, Consequences, and Discussion.

The journey consists of four distinct phases. Each phase focuses on developing a security practice for your business going from little knowledge to establishing a practice that'll protect your company from harm.

The goal is to define the security journey and guide MSPs through a high level of each phase to get you to start implementing security practices into your company.

Cybersecurity Culture

What is Cybersecurity Culture and why is it important?

The Culture of an organization refers to the beliefs, norms, values, assumptions, knowledge and attitudes of its team members. In the context of cybersecurity, influencing these attributes of the team as individuals and in aggregate, directly corresponds to the adoption of security solutions and practices. Understanding what influences these cultural attributes and how to best incorporate those influential activities into the daily communications, processes and leadership initiatives is key to building a security-focused organization.

Governance

Why is Governance important to understand?

Governance within an organization is broadly defined as the rules that run that organization, including the policies, standards and procedures that are used to set the direction (strategy) and control the organizations activities.

In cybersecurity, it is important that the organization objectives and strategy are aligned with the info sec policies, so that the resources appropriated to mitigate risk (controls) are suitably matched with the company mission and priorities.

Governance: Cybersecurity 101

Why is understanding Cybersecurity 101 important?

Cybersecurity 101 encompasses fundamental security concepts such as CIA (confidentiality, integrity and availability), PPT (people, process and technology), Frameworks and Controls. Understanding the concepts themselves and how they intersect, complement, and layer with each other is crucial to designing an effective risk management program.

Governance: Frameworks

What is a Framework and why is it important?

Cybersecurity Frameworks are a system of standards, guidelines and best practices to manage risks that arise in a digital world. The Cybersecurity Framework helps to prioritize risk mitigation strategies where vulnerabilities and threats might affect the ability for an organization to achieve their objectives. Frameworks should provide for flexible and cost-effective approaches to promote the protection and resilience of the organization.

Governance: Overview of NIST 800-53

What is NIST 800-53 and why is it important?

The NIST 800-53 Framework is the gold standard in cybersecurity frameworks in the United States and it is respected worldwide. The overview of this framework serves to provide a basic

understanding of what the framework contains, how it works, how it is applied, and how it intersects with and complements additional frameworks and regulations.

Additionally, NIST's 2019 publication on Improving Cybersecurity of Managed Service Providers and subsequent publication on PR.IP-4 Backups is important to understand for implementation and support purposes. As each additional publication is released, in depth curriculum and resources will be added to Certify Fundamentals for Sales coursework, to ensure continual improvement for MSPs as they pertain to current NIST guidelines.

Governance: Controls

What is a control and why is it important?

Cybersecurity controls are grouped into three areas: Administrative, Technical and Physical. Understanding the difference between these types of controls, the purpose they serve, how and why layers of controls are important, and the varying degrees of control implementation serves to enable MSP salespeople to identify and recommend appropriate solutions to mitigate risk. Administrative controls are explored in depth in the Certify Cybersecurity Fundamentals for Sales coursework.

Risk Management

What is Risk Management and why is it important?

Risk Management is a process aimed at balancing opportunities for gain (revenue, resources) while minimizing vulnerabilities and loss. The management of risk to information resources is a fundamental function of the MSP to understand and incorporate into their thought processes, communications, recommendations and implementations.

Having a baseline understanding of how to address risk and business impact in conversations and assessments as part of risk management is key to an MSPs successful deployment of security solutions.

Risk Assessments

What is a Risk Assessment and why is it important?

MSPs are commonly unable to distinguish between the activities included in varying forms of assessments: Network Assessment, Security Assessment, Vulnerability Assessment, and Penetration Testing. Understanding the problems each type of assessment solves for and use-case scenarios is important, as well as what is included in each type of assessment.

In the Certify Cybersecurity Fundamentals for Sales coursework, we explore the role of the Salesperson in the Security Assessment process.

Cybersecurity Technologies and Ecosystem

What is the Cybersecurity Technologies coursework and why is it important?

Putting together a comprehensive security solution stack is a challenge for many MSPs. This coursework guides the process to determine what solutions go into the stack, considerations on margins and pricing, and implementation and support resources needed for those solutions. Additionally, scalability challenges are reviewed in this training.

Qualifying Questions

Why are Qualifying Questions important?

When selling cybersecurity, one challenge for MSP salespeople is being able to determine early in the qualification process if the prospect is a good match, and to guide the conversation to stay on track and avoid pitfalls. In this segment we will review the qualifying questions found to be most applicable to MSP sales conversations.

How to Present

Why is knowing How to Present important?

Guiding prospects and clients through a roadmap designed to cultivate their understanding of the threat landscape, why it is important to them, what it is that you see and know as a cybersecurity subject matter expert, and how these threats can be addressed while having them understand their role is a proven method for communicating cyber risk to an organizations' stakeholders. Your ability to navigate this conversation in presentation format will be bolstered with the right resources and training, using two of the most effective presentation topics: Cybersecurity Risk and Security Awareness Training.

Objection Handling

Why is Objection Handling important?

Selling must always incorporate anticipation of the objections a prospect or client might bring up and how to handle those effectively. This coursework walks through the most common objections and helps to formulate impactful responses to have at the ready in your sales conversations.

Business Outcomes

What are Business Outcomes and why are they important?

Moving from the process of identifying, assessing and agreeing upon the results of the current and target security risk profile with your prospects and clients, to recommending and quoting proposed solutions is a process that your sales team must establish for consistency, automation (efficiency), and allocation of resources. This coursework explores quoting with examples of converting the profile to the action plan, what to include in the quotation process, delivery samples and how incorporating these steps into automated quotation tools helps to bolster efficiency and accuracy. Additionally, we review the ability to allocate resources for implementation as part of converting a quote to a project or service ticket, to provide for an understanding of how to scale efficiency as cybersecurity sales increase.

Next Steps

Once the MSP+ Cybersecurity Framework Fundamental requirements are met, MSPs can look forward to improving their cybersecurity posture and growth opportunities by moving into the Advanced and Master levels of the MSP+ Cybersecurity Framework. An overview of the SECURE MSP+ Educational Resources for the Advanced and Master levels can be found in the following sections below.

Certify Cybersecurity Advanced for Sales (Green Book)

This program takes Sales Professionals into real-world reconnaissance and planning exercises covering the full sales cycle from security assessment to profile creation and gap analysis to action plan presentation. Pro selling techniques, inclusive of risk and business impact scenarios to help secure the budget for cybersecurity are highlighted. Labs and competitions included.

Similar Courses: GIAC Information Security Fundamentals, ISACA CSX Fundamentals

Certify Cybersecurity Advanced for VCIOs (Green Book)

This program takes Owners and Sales Management Professionals into real-world governance strategy planning exercises to establish a real-world risk management program. Highlights include asset value determination, scenario planning, business impact analysis, budget and resource planning, and scalability strategies. Labs included.

Similar Courses: GIAC Information Security Fundamentals, ISACA CSX Fundamentals

Certify Cybersecurity Master for VCIOs (Blue Book)

This program takes Owners and Security Program Managers from creation of real-world risk management continuity and planning exercises, to third-party risk management and establishing KPIs. Labs included.

Similar Courses: (ISC)2 CISSP, ISACA CISM

Appendix A: Informative References

ACSC. The Essential Eight
https://www.cyber.gov.au/publications/essential-eight-explained

ACSC. Essential Eight Maturity Model
https://www.cyber.gov.au/publications/essential-eight-maturity-model

ACSC. Microsoft Office Macro Security
https://www.cyber.gov.au/publications/microsoft-office-macro-security

American Institute of CPAs (AICPA) - Service Organization Control (SOC) 2 Type II
https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

AT&T Business. Incident Response Steps and Frameworks for SANS and NIST
https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide

Atlassian. Get to Know the Incident Response Lifecycle
https://www.atlassian.com/incident-management/incident-response/lifecycle

Atlassian. Incident Communication Best Practices
https://www.atlassian.com/incident-management/incident-communication

Atlassian. Incident Management
https://www.atlassian.com/incident-management

Axis Communications. The Critical Role of Lifecycle Management in Maintaining Strong Cybersecurity
https://www.axis.com/blog/secure-insights/lifecycle-management-cybersecurity/

BCMMETRICS: The Critical Path: 9 Areas for Making Your BC Program a Success
https://bcmmetrics.com/business-continuity-management-guide/

Canadian Center for Cybersecurity. Baseline Cyber Security Controls for Small and Medium Organizations
https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Center for Development of Security Excellence. Job Aid: Plan of Action and Milestones (POA&M)
https://www.cdse.edu/documents/cdse/CDSE_POAM_Final_Job_Aid.pdf

Center for Internet Security (CIS). CIS Controls
https://www.cisecurity.org/controls/

CGMA. Business Continuity Management - Key Strategies and Processes
https://www.cgma.org/resources/tools/business-continuity-management.html

CIO Magazine. How to Create an Effective Business Continuity Plan
https://www.cio.com/article/2381021/best-practices-how-to-create-an-effective-business-continuity-plan.html

CSO Online. How to Build a Top-Notch Vulnerability Management Program
https://www.csoonline.com/article/3027570/taking-the-vulnerability-management-program-from-good-to-great.html

Cyberbit. 5 Free Cyber Security Training Online Courses Your IR Team Must Know
https://www.cyberbit.com/blog/cybersecurity-training/5-free-cyber-security-training-tools-ir-team-must-use/

Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (CISA)
https://www.cisa.gov/cybersecurity

Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (CISA). Alert (AQA20-073A) Enterprise VPN Security
https://www.us-cert.gov/ncas/alerts/aa20-073a

Department of Homeland Security. DHS 4300A Sensitive Systems Handbook. Attachment H: Process Guide for Plan of Action and Milestones (POA&M)
https://www.dhs.gov/sites/default/files/publications/4300A-Handbook-Attachment-H-POAM-Guide.pdf

Department of Homeland Security, National Cybersecurity Division. Recommended Practice for Patch Management of Control Systems
https://www.us-cert.gov/sites/default/files/recommended_practices/RP_Patch_Management_S508C.pdf

Emory University, Service Management Competency Center. Major Incident Roles and Responsibilities
http://smcc.emory.edu/itsm_process/major_incident/major_incident_roles_and_responsibilities.html

Everbridge. Critical Customer Communications: Best Practices
http://go.everbridge.com/rs/everbridge/images/Critical_Customer_Comms%20final.pdf

European Commission. EU Data Protection Rules / General Data Protection Regulation (GDPR)
https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en

European Union Agency for Cybersecurity. Security of Network Information Systems (NIS) Directive (EU)
https://www.enisa.europa.eu/topics/nis-directive

FDIC. Guidance for Managing Third-Party Risk
https://www.fdic.gov/news/news/financial/2008/fil08044a.pdf

General Electric. Digital Energy: Baseline Security Center-Cybersecurity Solutions
https://www.ge.com/digital/sites/default/files/download_assets/baseline-security-center-cyber-security-solutions-by-ge-digital.pdf

HHS.GOV. HITECH Act Enforcement Interim Final Rule
https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

HHS.GOV. Summary of the HIPAA Security Rule
https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

IETF. RFC 1919. Address Allocation for Private Internets
https://tools.ietf.org/html/rfc1918

InfoSecurity Group. Understanding and Managing Third Party Vendor Risk
https://www.infosecurity-magazine.com/next-gen-infosec/third-party-vendor-risk/

International Organization for Standardization - Standards for Information Security Management Systems (ISO/IEC 27001).
https://www.iso.org/isoiec-27001-information-security.html

International Organization for Standardization - Standards for Risk Management (ISO 31000)
https://www.iso.org/iso-31000-risk-management.html

Invgate. ITSM 101: 5 Ways to Improve Your Major Incident Communications
https://blog.invgate.com/itsm-101-5-ways-to-improve-your-major-incident-communications

ISS (IBM), Creating, Implementing and Managing the Information Security Lifecycle: Security Policy, E-business and You
http://www.tarrani.net/Security/securityCycle.pdf

IT Governance. The Most Common Causes of Data Breaches and How You Can Spot Them
https://www.itgovernance.eu/blog/en/the-most-common-causes-of-data-breaches-and-how-you-can-spot-them

MetricStream. 9 Best Practices to Jumpstart your Third-Party Management Program
https://www.metricstream.com/insights/best-practices-third-party-mgmt-program.htm

Micro Focus Marketplace. RACI Matrix for Incident Management
https://docs.microfocus.com/SM/9.60/Codeless/Content/BestPracticesGuide_PD/IncidentManagementBestPractice/RACI_matrix_for_IM.htm

Microsoft. Group Policy Settings Reference Guide for windows and Widows Server
https://www.microsoft.com/en-us/download/details.aspx?id=25250

Microsoft. Improving Web Application Security: Threats and Countermeasures
https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649874(v=pandp.10)

Microsoft. What's New in Windows 10 Deployment
https://docs.microsoft.com/en-us/windows/deployment/deploy-whats-new

Microsoft. Windows Security Baselines
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines

National Cyber Security Centre (UK). Cyber Essentials
https://www.ncsc.gov.uk/cyberessentials/overview

National Cyber Security Centre (UK). Zero Trust Architecture
https://github.com/ukncsc/zero-trust-architecture/

NICCS. Security Incident Response Training
https://niccs.us-cert.gov/training/search/trainace/security-incident-response-training

NIST. National Vulnerability Database (NVD) – Vulnerability Metrics
https://nvd.nist.gov/vuln-metrics/cvss

NIST. Cyber Security Framework (CSF) 1.1
https://www.nist.gov/cyberframework/framework

NIST. Federal Information Security Modernization Act of 2014 (FISMA) Implementation Project
https://csrc.nist.gov/projects/risk-management/detailed-overview

NIST, NCCoE. Protecting Your Data from Ransomware and Other Data Loss Events: Recommendations on How to Conduct, Maintain, and Test Backup Files (Extended)
https://www.nccoe.nist.gov/sites/default/files/library/supplemental-files/msp-protecting-data-extended.pdf

NIST, NCCoE. Protecting Your Data from Ransomware and Other Data Loss Events: Recommendations on How to Conduct, Maintain, and Test Backup Files (One Pager)
https://www.nccoe.nist.gov/sites/default/files/library/supplemental-files/msp-protecting-data-one-pager.pdf

NIST SP 800-35. Guide to Information Security Services
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-35.pdf

NIST SP 800-40 Rev.3. Guide to Enterprise Patch Management Technologies
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

NIST SP 800-41 Rev.1. Guidelines on Firewalls and Firewall Policy
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

NIST SP 800-53 Rev.5 (Draft). Security and Privacy Controls for Information Systems and Organizations
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf

NIST SP 800-55 Rev.1. Performance Measurement Guide for Information Security
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

NIST SP 800-61 Rev.2. Computer Security Incident Handling Guide
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST SP 800-92. Guide to Computer Security Log Management
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

NIST SP 800-100. Information Security Handbook: A Guide for Managers
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

NIST SP 900-171 Rev.2. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Office of the Superintendent of Financial Institutions (OSFI) – Canada. Outsourcing of Business Activities, Functions and Processes
https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx

OWASP. Logging Cheat Sheet
https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

PCI Security Standards Council. PCI Data Security Standard (PCI-DSS)
https://www.pcisecuritystandards.org/

Rapid 7. Introduction to Incident Response Life Cycle of NIST SP 800-61
https://blog.rapid7.com/2017/01/11/introduction-to-incident-response-life-cycle-of-nist-sp-800-61/

Rapid 7. Vulnerability Management Program Framework
https://www.rapid7.com/fundamentals/vulnerability-management-program-framework/

RSA. Incident Response: Implement a Communications Plan
https://www.rsa.com/en-us/blog/2016-01/incident-response-implement-a-communications-plan

SANS. FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics
https://www.sans.org/course/advanced-incident-response-threat-hunting-training

SANS GIAC. Framework for Building a Comprehensive Enterprise Security Patch Management Program
https://www.sans.org/reading-room/whitepapers/threats/paper/34450

SANS GIAC. Implementing a Vulnerability Management Process
https://www.sans.org/reading-room/whitepapers/threats/paper/34180

SANS GIAC. The Security Lifecycle
https://www.giac.org/paper/gsec/3018/security-lifecycle/105040

SANS GIAC. Security Lifecycle - Managing the Threat
https://www.sans.org/reading-room/whitepapers/basics/paper/592

State of California Department of Justice. California Consumer Privacy Act (CCPA)
https://oag.ca.gov/privacy/ccpa

Sutcliffe & Co. The 8 Most Common Causes of Data Breach
https://www.sutcliffeinsurance.co.uk/news/8-most-common-causes-of-data-breach/

TechTarget, SearchSecurity. Incident Response: How to Implement a Communication Plan
https://searchsecurity.techtarget.com/tip/Incident-response-How-to-implement-a-communication-plan

Tripwire. How to Build a Mature Vulnerability Management Program
https://www.tripwire.com/state-of-security/vulnerability-management/build-mature-vulnerability-management-program/

University of Pittsburg. Help using the Microsoft Baseline Security Analyzer (MBSA)
https://www.technology.pitt.edu/help-desk/how-to-documents/help-using-microsoft-baseline-security-analyzer-mbsa

US-CERT, CRR. Vulnerability Management
https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-VM.pdf