IT Nation SECURE MSP+ Playbook

Book 2: Advanced

v.2020.A1.2

WISE RISE
TOGETHER 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 that are consistent with applicable federal, state and local laws.

These are provided as a free resource and are provided “as is” without warranty of any kind and 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.

Table of Contents

Introduction

Welcome to the IT Nation SECURE MSP+ Playbook 2: Advanced, affectionately known as the Green Book.

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 IT Nation SECURE team. Our goal with MSP+ Cybersecurity Framework and book series is to allow organizations to take steps enhancing and adding additional controls and practices to achieve MSP+ Certification, and then to evolve into a SECURE MSP Accredited Partner.

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+ Cybersecurity 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 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. Additional information on the MSP+ Cybersecurity Framework and downloadable guides are located at the following URL: https://www.connectwise.com/theitnation/secure/framework.

How does this fit with our Security Journey?

The IT Nation SECURE MSP 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 maturing a cyber security 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 (Fundamentals) 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 (Advanced) 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 (Master) 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

The Fundamentals book started you and the organization on a path to a governance program. The book gave you the basic set of security policies every business, regardless of size, industry, or vertical should have in place and communicated throughout the company. In addition, you should also have setup measurements for those policies to ensure they are effective and enforced.

Customized Policies

Customized set of most policies for business are developed, documented and shared within the organization.

Policies may be based upon the shared IT Nation SECURE - Security Policy Templates and examples are located here: https://docs.connectwise.com/ConnectWise_Business_Knowledge/Information_Security_Policies

From the IT Nation SECURE MSP+ Fundamentals Playbook (Yellow Book), the MSP organization should already have the following policies in place, communicated and measured.

Acceptable Use Policy	Data Back-up Policy	System Configuration Policy
Anti-virus and Malware Policy	Facility Security Policy	Telecommuting/Remote Work Policy
Data Access and Password Policy	Perimeter Security and Administration Policy	Vulnerability Identification and System Updates Policy

If the MSP organization does not currently have all the above policies implemented and communicated across the company, please do so prior to submitting for the MSP+ Certification. These policies will be included as part of the attestation package signed by your organization.

In addition to the above (Yellow Book) policies, the following policies are required for the MSP+ Certification (Green Book):

Asset Management Policy	Encryption Policy	Incident Response Policy
Change Management Policy	InfoSec Risk Assessment Policy	Internal Privacy Policy
Code of Ethics	Logging & Monitoring Policy	Service Provider Security Policy

The MSP organization may also wish to better prepare for the SECURE MSP+ Certification. As such, the following policies are required at the next maturity level in the SECURE Master Book (Blue Book):

Corporate Policy Program	HR Corrective Action Policy	Interconnect Policy
Data Classification Policy	HR Security Policy	Policy or Standard Exception Policy
Data Retention Policy	InfoSec Committee Policy	Policy or Standard Variance Policy
Software Development Policy (Optional)		

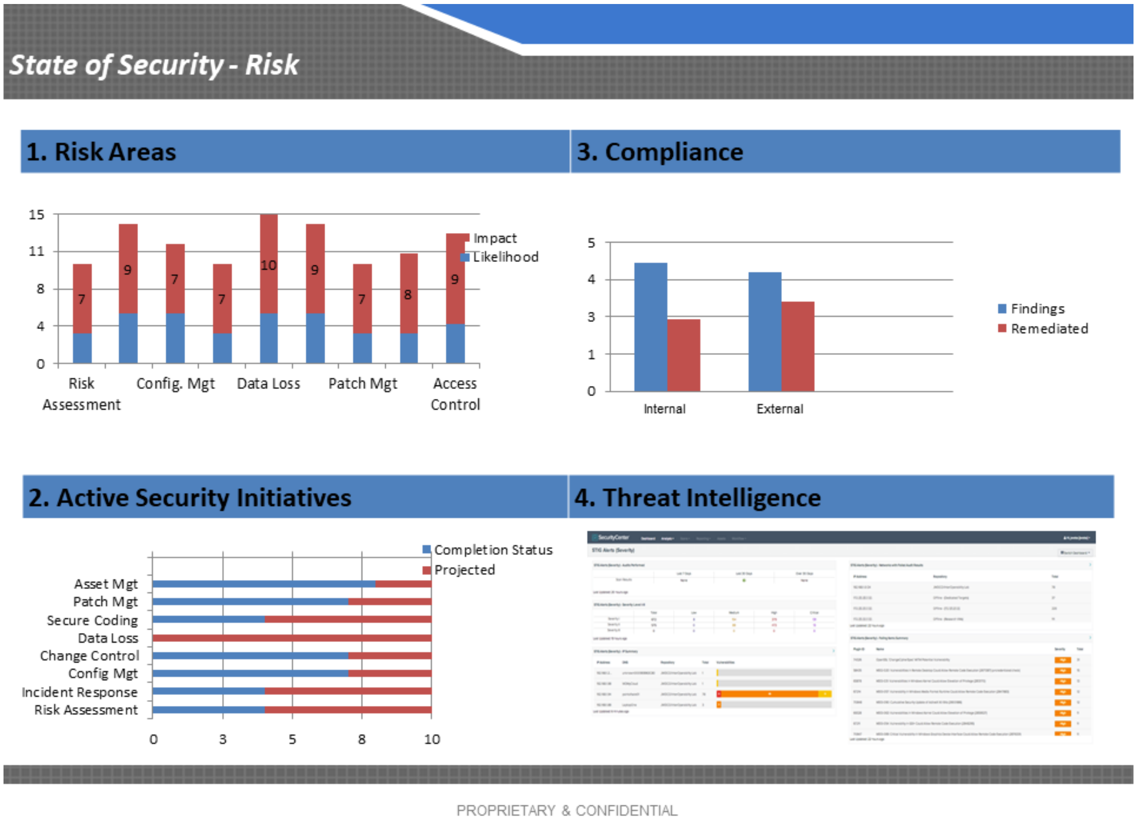
The Software Development Policy is optional and is only required for those MSPs who develop software. This is a recommended policy for any MSP who is developing software or plans to develop software.

Examples for all of the policies can be found on ConnectWise University at the following link: https://docs.connectwise.com/ConnectWise_Business_Knowledge/Information_Security_Policies

Policy Effectiveness

Efforts underway to establish a uniform program for the creation, revision and management of policies and supporting documents and processes across the MSP organization.

Policies only work if you can measure their effectiveness within the organization. Measurements, as we defined in the Fundamentals book, help the organization determine whether policies are working. Use these recommended measurements and check them monthly. Consider making a dashboard and publishing them to the organization. These dashboards are a useful tool to inform and educate the organization. Additional measurement templates are located within the **Security Measurements chapter of the Security Program section** within this document. Also, the following provides a sample overview of a Security Program Dashboard for measuring, tracking, and reporting on key initiatives.



State of Security - Risk

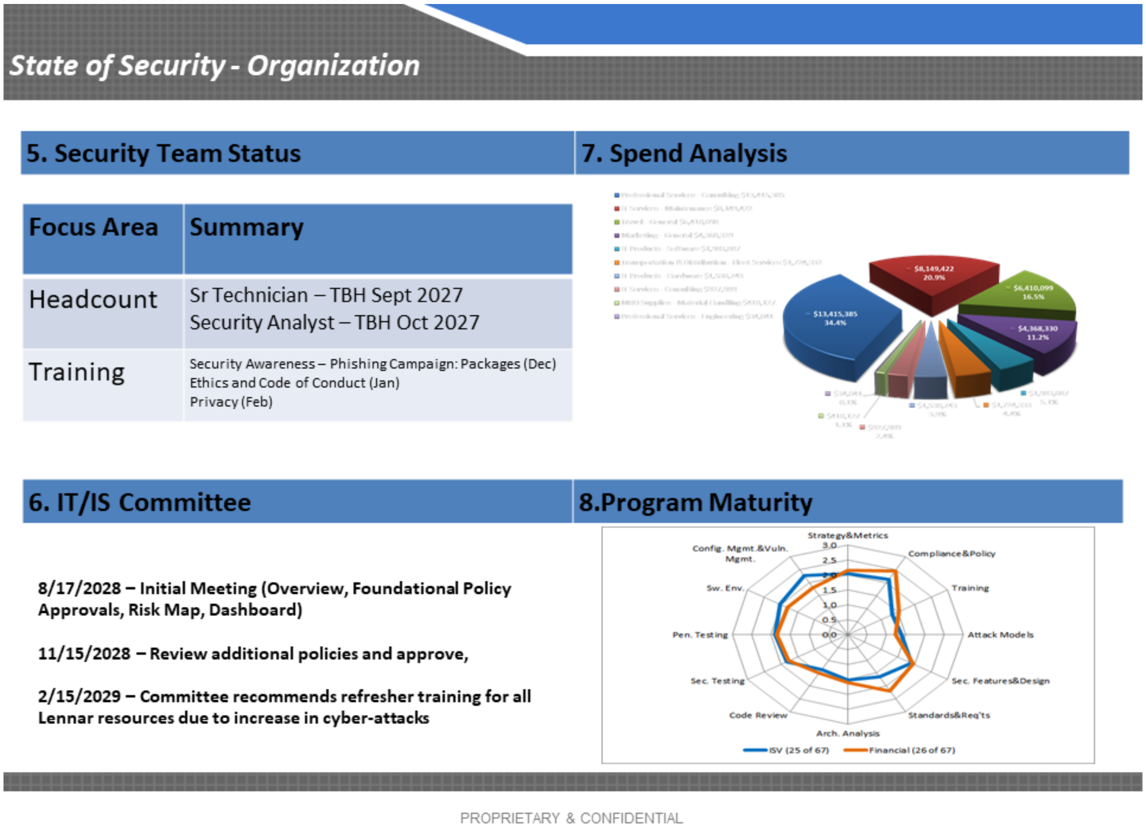
1. Risk Areas

3. Compliance

2. Active Security Initiatives

4. Threat Intelligence

PROPRIETARY & CONFIDENTIAL



State of Security - Organization

5. Security Team Status

Focus Area	Summary
Headcount	Sr Technician – TBH Sept 2027 Security Analyst – TBH Oct 2027
Training	Security Awareness – Phishing Campaign: Packages (Dec) Ethics and Code of Conduct (Jan) Privacy (Feb)

7. Spend Analysis

Professional Services - Consulting
IT Services - Maintenance
Travel - General
Marketing - General
IT Products - Software
Transportation & Distribution - Fleet Services
IT Products - Hardware
IT Services - Consulting
MRO Supplies - Material Handling
Professional Services - Engineering
$13,415,385
34.4%
$8,149,422
20.9%
$6,410,099
16.5%
$4,368,330
11.2%

6. IT/IS Committee

8/17/2028 – Initial Meeting (Overview, Foundational Policy Approvals, Risk Map, Dashboard)

11/15/2028 – Review additional policies and approve,

2/15/2029 – Committee recommends refresher training for all Lennar resources due to increase in cyber-attacks

8.Program Maturity

PROPRIETARY & CONFIDENTIAL

Notice that such reports are labeled as proprietary and confidential as they may contain restricted information and should have a limited distribution to key stakeholders.

Privacy Program

Now that the fundamentals of your Privacy Program are in place; internal Privacy Policy, Data Retention protocols and employee education, it is time to continue to build on the program and begin working on an informal external facing Privacy Policy.

The internal Privacy Policy needs to be formalized and signed off on by everyone in the company and an informal external Privacy Policy needs to be developed. Additional training and improvements to the existing Privacy Program will be made and security controls will be put in place for monitoring and actively protecting sensitive and confidential data including Personally Identifiable Information (PII).

Guidelines for a Breach Response Plan will be created, and an informal breach response plan will begin to take shape. Initial training and awareness of the breach plan for both employees and clients that might be impacted by a breach need to take place.

By now you should have a good understanding of your business policies and are familiar with the products and services you offer and understand who your customers are. This information will serve to help build your Privacy Program.

Formal Internal Privacy Policy / Data Protection Policy

The MSP organization provides internal privacy and security notices consistent with applicable laws, regulations, and standard business practices.

The Privacy Policy addressed a variety of privacy topics specific to the way you want privacy to be implemented in your company. It laid out the types of data your company controls which need to be protected, the proper methods for handling those types of data, security controls relevant to privacy and the procedures that make sense for your company.

Your informal internal privacy policy covers these areas as documented in the Fundamentals Book:

- Handling client/customer information
- Email and internet usage guidelines
- Employee records – personal information, payroll information, etc.
- Internal systems and access
- Mobile devices
- Established laws and regulations
- Consequences for violating the policy
- Report a breach

This probably took a significant amount of time and consideration as you developed the informal policy, but now you are well on your way to formalizing your Privacy Policy. You will see some of these areas are covered in other policies, such as the use of internal systems and access to these systems. This should be covered in your Acceptable Use Policy. The use of mobile devices would be covered in the Mobile Device Management Policy. This work does not need to be duplicated but should be referenced in the Privacy Policy.

As with all your policies, do not leave room for interpretation in the policy. Make sure you spell out completely the control and what it means to the employee. If you have monitoring systems in place for email and internet usage it should be communicated in the policy, so your employees are aware there are measures in place to ensure compliance with the policy.

Once you have your formal Internal Privacy Policy finalized, depending on the structure of your company, it should be reviewed by executive management, a compliance team, and owners. With their approval it is time to distribute.

Document Management Systems are the best way to receive, track, manage and store your policies. If this is not available, you can use a file sharing system you have in place. It is important to have some way for employees to sign the document and a way to store those signed documents for future reference and compliance requirements.

Informal External Privacy Policy / Privacy Notice

The MSP organization provides external privacy and security notices consistent with applicable laws, regulations, and standard business practices.

These days almost every company collects personal data from their customers and even their prospects. If that is the case with your company, you will need an external Privacy Policy or Privacy Notice that your customers and prospects have access to read as it is most likely required by law.

Note: Privacy Policy, Privacy Notice and Disclosure Statement are often used interchangeably.

Under privacy law, a privacy statement discloses the ways a company gathers, uses, discloses, and manages a customer's or employee's data.

On an ongoing basis data stewards (principally the IT staff) are responsible for keeping this data private and secure.

Information privacy policies are important to compliance officers, IT staff, and within the organization -- if a customer informs the company they do not want their personal data collected or shared, companies must uphold that decision and follow the procedures within the privacy policy.

In companies where the personal data collected is extremely sensitive, such as financial, medical, and insurance, employees must ensure information is not inadvertently shared by practicing privacy protections defined in the Privacy Notice.

Who should create the privacy ?

A privacy policy is an internal matter which governs employee conduct with sensitive information and could have a significant impact on outside stakeholders, third-party business partners and your customers. To thoroughly cover all areas of privacy in your company, a team of IT, Compliance, data stewards of sensitive information, Legal, and third-party business partners who may want to use this data for marketing should be involved in the creation of the policy.

What is covered in the policy?

Privacy overlaps marketing/public relations, legal/compliance, and IT functions. For this reason, the cross functional team should address these elements:

- Collection and usage of customer information
- Commitments to stakeholders and customers
- Sharing of customer information
- Process for sharing customer information with third parties
- Data protection and security
- Login information
- Privacy compliance
- Data retention
- Marketing and communication

By working as a collaborative team your company can successfully develop and build a Privacy Policy which meets the needs of your company. Companies should check with their legal counsel, regulators, and auditors to determine what needs to be included in areas of information privacy.

Many state and federal regulatory systems exist to protect the privacy of personal data and if you fit into any of these categories than you must additionally account for the regulations within each regulation. Here are just a few:

- **HIPAA** – Health Insurance Portability and Accountability Act
  The Privacy Rule under HIPAA states a healthcare provider, or "covered entity," has permission to use patient data if it's related to "treatment, payment, and health care operations." However, using the data for marketing purposes or selling the PHI requires explicit authorization.
- **GDPR** – General Data Protection Regulation
  At its core, GDPR is a set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy.

- **CCPA** – California Consumer Privacy Act
  The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States.

Many other states are creating their own version of privacy laws and more are soon to follow. The US does not yet have a federal-level general consumer data privacy law or a data security law. It is only a matter of time until a federal-level privacy law comes about in the United States.

Available for External Consumption

At this point the Privacy Policy needs to be in a stage where it can be made available to customer s and external third parties. It does not need to be formally posted on your website or part of any contracts with customers, it just needs to be available to share if required.

There a lot of great resources to search which provide examples of privacy policies, including the ConnectWise University: https://docs.connectwise.com/ConnectWise_Business_Knowledge/Information_Security_Policies.

Documented Policy Reviews

The MSP organization must review their policies, standards, exceptions, and variances at least annually to address any necessary changes.

A documented review of security controls in place and monitoring of these controls are needed to actively protect PII and sensitive or confidential data within the MSP organization

As will all policies, it is also important to revisit, modify and update if needed on an annual basis, or as your business changes. You may bring on a new customer and store types of confidential data you were not previously storing or addressing in your Privacy Policy. This would require a modification of the policy and redistribution of the policy to your employees.

Policy updates and approvals

Privacy policy updates should be immediately issued upon completion and approval. The approval signature list for these updates should be agreed to within the company and should be fully executed before any policy update is be placed into effect. All policy updates should be issued immediately with education and training for employees affected by the policy. For each policy, a historical record of all updates should be maintained.

Policy training and signoffs by employees

As part of the new employee orientation process, employees being placed into positions that involve privacy issues should be required to receive training, read policies, and sign off that they have read and understand all policies concerning privacy before they begin their assignments. A record of all employee signoffs should be maintained.

Audit cycles and regulatory compliance

Companies should check with their legal counsel, regulators, and auditors to determine what needs to be audited in areas of information privacy. In some cases, companies might also have internal audit procedures that their own audit and compliance teams perform. As part of the audit and compliance process, companies should take steps to ensure their privacy policies are kept up to date with the latest regulatory and compliance rules and policy updates are issued on a timely basis to customers, business partners, and other stakeholders.

Continuous Improvements

There are many methodologies used to bring structure to the process of identifying and putting in place opportunities for improvement. Six Sigma, Kaizen and Lean are some of the more popular methods. At the center of these, though, is the idea of continuous improvement.

The models reflect the idea organizations should work on incremental improvements to services, products, and processes, and in this case policies. Guided by these concepts, fundamental continuous improvement can be implemented into a company's policies.

- Improvements should not only happen when a paradigm changes or major changes to your business but can be based on small changes.
- Continuous Improvement relies greatly on your employee's valuable input, they know and understand your business.
- Incremental improvements are generally inexpensive to implement compared to all out change.

Making continuous improvement to your company's privacy policies ensures continued compliance with ongoing regulations and protection of sensitive information.

Protocols Defined for Data Retention

The MSP organization has implemented a data identification and classification schema and data retention standards as required by applicable data privacy laws, regulations, and standard business practices.

Computers and inexpensive storage have made hoarding data easier now than it has ever been in the history of mankind. They highlight the natural human bias towards saving everything until our closets are full to overflowing.

Should all those outdated documents and files nobody has touched in years be kept in storage? Well, it is conceivable, possible, and not completely beyond imagination, that someone, someday, may want one of them. So, let us save everything, "just in case." Besides, data storage is incredibly inexpensive these days.

"Just in case" is a terrible policy. A single, unnecessary file or email could contain:

- Data a hacker could use to attack your company or your customers
- Malware lying dormant that could be triggered upon access or movement
- Details and facts to be discovered and used against you in court

You must weigh the potential value of storing data against the costs and risks of storing that date.

Files should be erased when they no longer serve a business purpose and there are no legal or regulatory retention requirements.

Privacy regulations have had a major impact on data retention programs, as has the rising expectations of customers to have more control over their own information.

Determine which privacy regulations your company must comply with and read through those regulations to pull out the retention periods of the types of data you store as a company.

You must classify documents and files into categories for retention and erasure. Start by identifying data that must be retained for specific periods, followed by data whose destruction is mandated by laws or regulations.

Next steps for the business is to determine which documents and files can be categorized as "should be saved," "should be erased," and "whatever" categories. Decide on retention and erasure rules for these files. The MSP organization must weigh the possible future business value of the information against the potential risk of fines and expenses resulting from a data breach.

Some documents and files may be classified based on multiple classification criteria. For example, all spreadsheets created by the finance department and stored on the SharePoint server may be retained, but you may want to erase all emails more than three years old, containing the words "confidential" or "personal," and not covered by another retention requirement.

Companies then must specify how data will be protected and retained. The Data Retention Policy should include retention periods for each classification and steps for handling files at the end of the required retention policy.

It is also important to monitor and report on data retention and erasure activities. This is needed both to satisfy auditors and regulators and to collect data to improve these activities. As with all policies and processes, continuous improvement is an important part successfully securing your company.

Don't get burned by data you are not legally or regulatory required to retain. Let it go.

Guidelines for a Breach Response Plan

The MSP organization has a data breach response plan that provides detailed instructions to follow in the event of a security breach.

When building your data breach response plan, make sure to research and refer to any applicable regulatory compliance governing your location, industry, or services. When improving and maturing your data breach response plan, follow the information contained within the section labeled Incident Management Program contained within this document.

There are many laws worldwide relating to breach disclosure. Generally, the laws define "personal information" as an individual's first initial or name and last name, in addition to one or more of the following data elements when the name or data element is unencrypted.

- Social Security number;
- Driver's license or state ID number; or,
- Account number, credit or debit card numbers in combination with the required password or access code.

Some places have varied this definition, however. For example, in addition to these data elements, The State of Arkansas breach notification law includes medical information in its definition of "personal information" and the State of North Dakota's law includes mother's maiden name, employer-assigned ID numbers and electronic signatures.

A great resource to research breach notification laws is the Mintz Matrix. This useful resource allows one to click on a U.S. state and display detailed breach notification law information.

- Mintz Matrix – U.S. State Data Security Breach Notification Laws https://www.mintz.com/mintz-matrix

Your company must establish and maintain a security incident management response process for systems which could impact your company's customers, vendors, and confidential data.

You must determine who the point person or persons is (the investigator) who must be notified immediately of any suspected or real security incident involving:

- Confidential Data (based on your Data Classification Policy) which may include, but is not limited to, PHI, PII, employee and customer data
- Critical or Severe Alerts
- Possible violations of Federal or State law
- Possible violations of client for vendor contracts
- Misuse of your company's computing assets

Term Usage – Security Incident vs. Breach

The term, breach, is normally associated with an unauthorized disclosure of unprotected PII or PHI. Until a breach condition has been declared, the appropriate term to use in the escalation process is, security incident. If a breach condition is declared and there is a possibility it contains PII or PHI, then your Breach Notification Policy will be incorporated into the response.

Whether it is a Security Incident, or a Security Breach follow the Incident Response procedures in the Incident Response section below.

Informal Breach Response Plan

If it is a Security Breach additional steps should be implemented and followed.

Breach Investigation
Name an individual to act as the investigator of the breach. The investigator shall be responsible for the management of the breach investigation, completion of the risk assessment, and coordinating with others in your company as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel.)

Risk Assessment
For breach response and notification purposes, a breach is presumed to have occurred unless you can demonstrate that there is a low probability that the data has been compromised based on, at minimum, the following risk factors:

- The nature and extent of the data involved. Consider Social Security numbers, credit cards, financial data.
- The unauthorized person who used the data.
- The extent to which the risk to the data has been mitigated. Can you obtain the unauthorized person’s satisfactory assurances that the data will not be further used or disclosed or will be destroyed?

The evaluation should consider these factors, or more, in combination to determine the overall probability that data has been compromised.

Based on the outcome of the risk assessment, you will determine the need to move forward with breach notification. The investigator must document the risk assessment and the outcome of the risk assessment process. All documentation related to the breach investigation, including the risk assessment, must be retained for a minimum of six years.

Notification: Individuals Affected
If it is determined that breach notification must be sent to affected individuals. Notice to affected individuals shall be written in plain language and must contain the following information:

A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

A description of the types of unsecured data that was involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).

Any steps the individuals should take to protect themselves from potential harm resulting from the breach.

A brief description of what you are doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, email address, website, or postal address.

Notification: HHS and Media
In the event a breach of unsecured Protected Health Information (PHI) affects 500 or more of your customers, HHS will be notified at the same time notice is made to the affected individuals, in the matter specified on the HHS website. If fewer than 500 of your customer's PHI is affected, you must maintain a log of the breaches to be submitted annually to the Secretary of HHS no later than 60 days after the end of each calendar year, in the manner specific on the HHS website.

Media In the event the breach affects more than 500 residents of a state, prominent media outlets serving the state and regional area will be notified without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. The notice shall be provided in the form of a press release.

Delay of Notification Authorized for Law Enforcement Purposes
If a law enforcement official states to you that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, you may delay the notification to individuals if they provide that notification in writing. If not in writing, you can delay posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

Training and Awareness

As soon as you suspect an incident has occurred, before even communicating up that there is an issue, employees should be trained on the basics of how to respond. Here are the steps you should train them to follow:

- **Power Off**
  Make sure they know to power down the machine in question. Do not forget about the ethernet cord either! Make sure they know to disconnect the ethernet cord if they are connected and not just using Wi-Fi. Power may also be delivered via the ethernet cord, so training should include the procedure to unplug both the ethernet and the power cord.
- **Do Not Delete Files**
  Do not delete any files or make changes. If you delete a possible malicious file, you will delete the audit trail along with the evidence that will allow a cyber forensic investigator to determine the root cause of the incident and what data may have been lost. The findings of the investigator could have huge consequences within a legal situation such as a lawsuit or an insurance claim. The best practice is to isolate the machine and power it down and wait for the experts. Teach your employees to respond logically, not emotionally. It is not their job of the employee remediate the problem – it is their job to detect and protect further expansion of an incident. Such situations should be part of the awareness training for workforce personnel.

- **Communicate Up**
  Your employees should have a structure in place of who is in the “need to know” chain about a possible breach incident. After communicating up, they need to be informed of their actions while the responding manager raises the communication of the breach with the rest of the MSP organization. These the following workforce personnel should be in the “need to know” chain:
  - Their direct manager
  - The IT leader
  - Executive management or the owner of the company
  - (Possibly) Workforce personnel responsible for the physical security of the company – security guards, administrators, etc.

Since digital attacks can sometimes coincide with physical attacks. It is a good practice where building security should be notified to not accept visitors while a breach response is active. This is especially true if the office location resides in a larger multi-tenant building.

Everyone in the MSP organization needs to have a common understanding when it comes to reducing risks and responding to incidents, which is why it is important to have these procedures as part of Security Awareness Training. Knowing how to respond to an incident and potential breach is important for all workforce personnel to know. Make sure they are trained and know what to do when they suspect an incident.

Security Program

The content of the IT Nation SECURE MSP+ Advanced Playbook (Green Book) should serve as a guide for an MSP organization to build upon the essential security fundamentals as outlined within the Yellow Book to help mature an overall security program across business operations and services. 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 mature cybersecurity and compliance practices to better address the unique risks, threats, and attacks that accompany the shared services model within the MSP community.

Security Culture

The MSP organization has made efforts to adopt security as part of the company culture.

Every business has a culture. Some, like ConnectWise, enjoy making the workday fun, allow t-shirts and shorts, have Friday get togethers in the late afternoon, etc. Others take a more traditional approach. Regardless, the culture of the company is paramount to its success and growth. It also leads to a better workplace environment in most cases. Adding security to an existing culture is not difficult, it takes time and education. It also starts with a commitment from the business and its leadership.

Leadership should have a clear understanding of the current security posture with the starting metrics from the Fundamentals book. Using those measurements, the organization can communicate the importance of security to the organization. This is one way to add security to the culture and there are many more. Find a formula that works for your individual and unique organization, nurture it, grow it, and it will become fruitful.

Documented Security Plan

The MSP organization has developed, documented, and performed periodic updates to an overall security plan that describes system boundaries, system environments, security requirements, and the relationships with or connections to other systems.

The security plan defines many things for the systems and applications within the MSP organization. This plan should help the MSP identify all the systems and applications within their organization, who is responsible (owner, for the applications, database, etc.), and the security controls for the environment. As an alternative, the MSP organization may wish to consider creating a separate security plan for each segmented network, with one overall security plan that outlines interoperability along with the security controls required to keep everything separate.

At a minimum, the security plan should have the following items:

1. High level overview or summary
2. Individual Positions responsible
    a. Owner

   b. CISO or CSO
   c. If there is an Application, then Application Owner
   d. If there is a Database, then the DBA
3. Summary of the System Purpose
4. Detailed Network Diagram of the Boundary
   a. Might be the whole environment or could be individual network segments
5. Detailed Data Flow Diagram, if processing, storing, or transmitting sensitive information (PII, PHI, PCI, etc.)
6. Inventory of the Devices in the Boundary
   a. System/Server Name
   b. OS including version
   c. CPU
   d. RAM
   e. # of Disks, their Type and Size
   f. Type of information stored, processed or transmitted, if sensitive
7. Detail description of the security controls, how they protect, are measured, and evaluated for effectiveness
8. Description of the training provided to employees and contractors
9. Description of the controls for third-party vendors and the plan to manage their risk
10. Description of the auditing for the systems and devices within the organization
11. Detailed description of how the security controls will be used to safeguard the organizations systems and devices
    a. When those controls fail, how the organization will respond
    b. Reference should be made to the Incident Response Plan
    c. Reference to the Business Continuity and Disaster Recovery Plan

The Security Plan should also include a version history, be reviewed at least annually, and updated whenever a major change has been made to the environment that impacts the systems, applications, or controls. The Security Plan document should be considered highly confidential due to the sensitive information contained within its pages. As such, the MSP organization should allow designated workforce personnel (with a need to know) access to the Security Plan and supporting content. For those partners who have regulatory or compliance requirements for customers, the IT Nation SECURE team has created sample reference documents within the ConnectWise University and the IT Nation SECURE MSP+ Advanced Playbook (Green Book) can

be located and downloaded from the following URL:
http://www.connectwise.com/advanced-playbook/

Also, the MSP+ Cybersecurity Framework and Supporting Fundamentals Playbook (Yellow Book) can be downloaded from here: https://www.connectwise.com/theitnation/secure/framework

Security Awareness Training

The MSP organization provides training and coaching to workforce personnel on a variety of security risks and safe computing practices.

Training and Awareness campaigns are another good way to instill a security first culture within your organization. Each and every one of your employees, with the proper training and guidance, is able to provide additional eyes on your security posture. They are also the ones to provide feedback on other topics like policies or change procedures. This also makes employees the riskiest element of business operations. Proper training and measurement of their activities can reduce this risk, but it will not eliminate all the risk.

If you made it to the Advanced book, you should have already implemented the following security awareness training for all your employees:

Phishing	Social Engineering	Mobile Devices
Privileged Users and Administrators	Malware	Browsing Safely
Social Networks	Passwords	Data Security

If the MSP organization has not implemented these modules, please take the time to do so right now. These are the basics for a good security awareness training program. Please remember, each of these modules should be part of an annual training curriculum, which is documented for each and every employee. In addition, these trainings should be part of a standard new hire onboarding process. Work with human resources or the person in that role to ensure the onboarding process includes security awareness training.

Moving your security training to the next level (Advanced) includes adding the following modules to your existing baseline set. Please remember that with this new set of requirements, not all of your employees are in roles associated for taking this training. However, if an employee should transfer into a new role that has a new training requirement, please ensure they receive the new training.

(Must have all the topics from the Fundamentals playbook (Yellow Book) in addition to following security awareness training courses):

Insider Threat

Insider threat training should instruct all workforce personnel (employees, contractors, vendors, partners, etc.) who have access to business and IT assets. Such topic may include what insider threat is, how to avoid becoming a threat, and the consequences for any insider who consciously becomes a threat to the organization.

Cloud Services

Topics of training should include ant company policy or standards on the use of cloud services and software as a service (SaaS). How cloud services differ between personal-use vs. that od the organization with concepts related to risk associated with personal accounts and why multi-factor or two-factor authentication (MFA/2FA) mechanisms are critical for any organization who utilized cloud-based services.

Physical Security

Advanced physical security training to follow best practices that will help them keep people, work areas, and IT assets secure by promote awareness, such concepts may include avoiding tailgating though a door to a restricted area (piggy-backing), having a clean desk, recognizing techniques by disguised infiltrators, social engineering tactics that may stem from documents recovered from the trash (dumpster diving).

Working Remotely

More attention must be provided to educate workforce personnel on safe work practices while working remotely or working from home (WFH). The focus of training should align with company policy and standards should address the use of personal devices for business, video conferencing, file sharing and the protection of company data, ensuring the Wi-Fi router is secure, using a VPN, etc.

Encryption

Since many end users may not understand what encryption is or how it may be used within the organization to protect data rest, data in motion, laptops, VPNs, website certificates, etc. Security awareness training for encryption may best be served using demonstrations and informative graphics to help explain process flows.

Help Desk Specialized Roles

Since helpdesk and customer service personnel are the often the front-line defenders against social engineering attacks, specialized training designed to help identify such attempts. Additionally, helpdesk and service personnel will need to well-versed on existing company policy and standards in order to properly resolve user issues in a secure manner.

Senior Leadership Specialized Roles

Since company executives and senior leadership often have elevated levels of access to most systems and often work with sensitive data, they are high-value targets for social engineering and phishing attacks often designed to compromise their account credentials to either obtain money or to steal data. Specialized training for upper management should include details and scenarios that illustrate the need for security while working remotely, the mindful use of social media platforms, the use of multi-factor authentication, vulnerability assessments, incident response reporting and communication, etc.

Physical Security Measures System

The MSP organization has adopted physical security measures in order to protect and secure workforce personnel, IT systems and digital assets.

Established system designed to enforce Physical Security

Physical security is vitally important and depending upon the information stored, processed or transmitted by the organization, may be a breach vector that can be exploited. Using the Security Plan(s) from above, the organization should review the physical security requirements associated with each and every network segment, server, application, etc. and ensure the appropriate safeguards have been deployed. These safeguards may include, badge readers, cypher locks, equipment cages, tinted windows, hardened facilities, etc. You should be evaluating your physical security as part of your external penetration testing activities.

- Total Security Advisor – 5 Physical Security Controls Your Business Needs https://totalsecurityadvisor.blr.com/facility-security/5-physical-security-controls-your-business-needs/
- SANS Institute - Physical Security and Why It is Important https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120

System Auditing

The MSP organization has made efforts to audit and monitor events across applications, systems, and devices in order to provide an early warning of a security incident.

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 any digital forensics or incident response activities.

Audit Policy

In developing an audit policy, (at a minimum) make certain that the following options have been configured within the in the Audit Policy section within the local policy on a Microsoft Windows host system. Set the audit values that match the policy and standards from your company. However, at a minimum, you should audit the following categories.

Operating System (OS) Events

- Start up and shut down events
- Start up and shut down service events
- Network connection events including failed connection attempts
- Changes or blocked attempts to change, system security settings and configurations

OS Audit Records

- Audit Account Logon Events (successful and failure)
- Change(s) performed after logged on (e.g., reading or updating critical file, software installation)
- Account modification(s) (e.g., account creation and deletion, account privilege assignment)
- Privileged account usage (success and failure)

Application Account Information

- Application authentication (success and failure)
- Application account changes (e.g., creation and deletion, change in privilege)
- Application privileged use

Application Operations

- Application startup and shutdown events
- Application failures (e.g., kernel panic)
- Major application configuration changes
- Application transactions, e.g.:
    - E-mail servers logging sender, recipients, subject name, and attachment names for each e-mail

  - Web servers logging each URL requested and the type of response provided by the server
  - Business applications logging financial records (where they were accessed and by whom)

Minimum Audit Logging Requirements

You need to ensure that there is adequate space in the audit logs for the events and alerts that will be generated. This is especially important if you will halt the system on audit failure. You should configure the system to handle your expected log capacity (you will have to test to see what that is) plus another 50 percent (50%) of capacity. Remember to set your rotation policy as well. This should be consistent with whatever policy you have.

At a minimum, log files should contain the following information.

- Timestamp, usually relative to the server or to the companies centralized NTP server
- Event, status, and any error codes
- Service, command captures and/or application name
- User or system account associated with an event
- Device used (e.g., source / destination IP address, terminal session ID, web browser associated cookie / session identifier, web browser details, etc.)

For addition information on logging events, please refer to the following resources:

- NIST SP 800-92 – Guide to Computer Security and Log Management https://csrc.nist.gov/publications/detail/sp/800-92/final
- Microsoft - Advanced Security Audit Policy Settings https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings
- Microsoft – Audit Policy Recommendations https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations
- Microsoft – Auditing Security Events https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/auditing-security-events

Hardening of Critical Systems

The MSP organization hardens critical systems with a baseline security configuration to limit the storage and exposure of sensitive data.

Practice to harden the security of critical systems in accordance with vendor or published hardening guidelines. This should include the least functionality requirements for both operating system and applications. Such hardening functions may include ports, services, and protocols that are not required for the intended use of the system within the 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, a standard harding practice 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.

For each service that exists on the system, you have a number of controlling options. You can disable the startup of options, so they do not run at all. The basic strategy is to run as few services as possible so hackers cannot exploit any bugs those services might have. Another strategy is to run services under less-privileged accounts. All default services run under the context of the Local System account, which has access to the entire system. If you install a defective program that runs under the Local System account, it could damage your system. Worse, a hacker might take advantage of the hole in the program to attack your system with full privileges of the Local System account. Many attacks in the UNIX environment took place under similar conditions.

For more information on hardening critical systems and endpoints, please refer to the following resources:

- Australian Cyber Security Center - Hardening Microsoft Windows 10 Workstations (v.1909)
  https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-1909-workstations

- Microsoft - Microsoft Security Baselines https://techcommunity.microsoft.com/t5/microsoft-security-baselines/bg-p/Microsoft-Security-Baselines

Disabling Microsoft Windows Services

One of the most difficult system hardening tasks is deciding to disable unused and unneeded services. This take involves aspects that are hard to get right. As a matter of principle, it is easier to define what should be enabled for the basic functionality that allows a Windows system to interact with the TCP/IP network stack.

For medium to high-security system, ensure the following services are the only ones running. The asterisks (*) indicate the minimal services required for the Windows host system to operate. All other services are optional and represent potential risk.

- DNS Client*
- EventLog*
- IPSec Policy Agent
- Logical Disk Manager*
- Network Connection Manager
- Plug and Play*
- Protected Storage*
- Remote Procedure Call
- Remote Registry Service
- RunAs Service
- Security Accounts Manager*
- Server
- Workstation

For a Microsoft Windows Domain Controller, one will also need to have the following services enabled and running:

- DNS Server
- File Replication Service
- Kerberos Key Distribution Center
- Net Logon
- NT LM Service Provider
- RPC Locator

- Windows Time

You can use the Services control panel to disable services that are running but are not needed. To start it up, open explorer and right click on This PC, then click on Manage. When Computer Management opens click on Services. If you right click on a service and then click on properties, you will get the details about the service. To disable the service, change the startup type to disabled.

Local Policies

For a Microsoft Windows system, make sure that the following options have been configured in the Password Policy section of your local policy. Set the values in accordance with your corporate policy.

• Enforce Password History	Enabled (recommended value 5)
• Maximum Password Age	Enabled (recommended value annual) also based on events
• Minimum Password Age	Enabled (recommended value is 5)
• Passwords Must Meet Complexity Requirements	Enabled
• Store Password Using Reversible Encryption	Disabled

Account Lockout Policies

For a Microsoft Windows system, ensure the following options have been configured in the Account Lockout Policy section of the Windows local policy. Set the values in accordance with the policy and standards the MSP organization has established.

• Account Lockout Threshold	Enabled (recommended value is 5)
• Account Lockout Duration	Enabled (recommended value is 30)
• Reset Account Lockout Threshold After	Enabled (recommended value is 30)

Perimeter Security Solutions

The MSP organization has deployed enhanced capabilities for perimeter security (e.g., next-gen firewalls and IPS).

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.

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.

Firewall

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

IPS

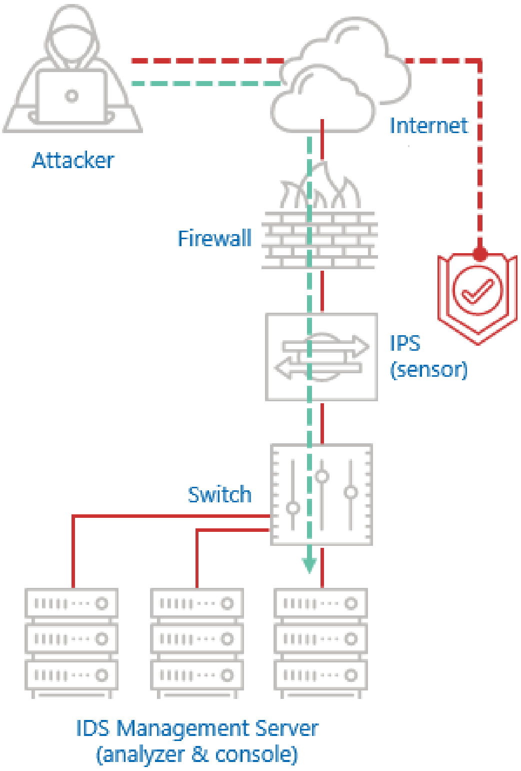
An IPS is designed to not only detect attacks, but also to prevent the intended hosts from being affected by the attacks. An IPS solution complements most firewall, antivirus, and antispyware tools by providing additional protection from new and emerging threats.

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.

An IPS solution has the major advantage of potentially blocking an attack when it occurs. Rather than simply sending an alert, an IPS actively attempts to block malicious and unwanted traffic.

The main components of a network based IPS 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.



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.

Endpoint Encryption

The MSP organization uses industry-accepted encryption technologies to protect sensitive data stored on portable devices or removable storage media.

Due to loss or theft, curious or malicious users may gain unauthorized physical or logical access to a device. Once accessed, the unauthorized entity may then transfer information from the device to another system or perform other actions that may potentially jeopardize the confidentiality of the information on a device. If strong encryption and security practices are not in place, the MSP organization may, not only be open to potential cyberattacks, but also be open to the loss of corporate and customer information as well as fines for non-compliance with laws including HIPAA and GDPR. Additional damages to MSP organization from the loss of data may result in direct financial damage from a tarnished public reputation resulting from the loss of customers and the inability to obtain new business.

As such, sensitive data stored on portable devices (such as laptops and smartphones) or removable and easily transported storage media (such as USB drives or CDs/DVDs) must use industry-accepted encryption technologies that use Advanced Encryption Standard (AES) 128-bit or 256-bit key lengths.

For encrypting data on the endpoints, there are an assortment of various vendor devices, utilities and tools that fall into the a few basic categories:

- **Self-Encrypting USB Drives**
  Portable USB drives that embed encryption algorithms within the chipset that controls the “hard drive” or storage chip. This eliminates the need to install any third-party full-disk or file encryption software. However, these drives are limited in their use for the secure protection of data as files are only encrypted when residing on the encrypted USB drive. Once files are copied from the encrypted USB drive, they may then be freely read and shared without any encrypted protection. Additionally, self-encrypting USB drives are often more expensive than non-encrypting USB drives.
- **Full-Disk Encryption Software**
  Used to encrypt unprotected storage media such as portable media (e.g. CDs, DVDs, USB drives) or mor commonly used to encrypt laptop hard drives. The flexibility of full-disk encryption software allows for data protection to be applied to most any type of storage media. However, like self-encrypting USB drives, a lack of control exists when files are copied from the encrypted drive, they may then be freely read and shared without any encrypted protection. There are several enterprise software solutions that will allow an organization to manage both full-disk and removable dive encryption from a centralized key management platform and management console.
- **File Encryption Software**
  Permits much greater flexibility by applying encryption to specific files that may contain sensitive data. When properly using file encryption software in conjunction with a data classification schema, the MSP organization can share encrypted files over email or cloud-based file sharing platforms while maintaining the protection of the file and its sensitive contents. As a good practice to share encrypted files, one must safeguard that passwords are shared securely over a different channel. For example, do not share the password with an encrypted file in that same email, or do not place a Post-It Note with the password attached to an external USB drive.

Take note that once a document, file or hard drive has been encrypted, it may not be opened without a proper key or password. Once encrypted it may be months or years before the file is accessed. If the key has been lost or the password has been forgotten, then encrypted file and the data it contains is rendered is useless. Have a process in place to make sure that that encryption keys and passwords are securely stored in a safe place (or service) before encrypting important information. Also, it is a best practice to have documented procedures in place that cites the location of the encryption keys and passwords with a means for the appropriate workforce personnel or staff to obtain or recover such keys and passwords.

Laptops & Portable Devices

Laptops and portable devices containing sensitive data are to be encrypted and protected by using industry-accepted encryption technologies.

Today, the process to encrypt laptop and portable hard drives is fully supported by the major operating system vendors. For example, Microsoft Windows provides a native encryption software option through BitLocker, and Apple offers built-in encryption for both the mobile IOS iPhone platform as well as the OS X desktop / laptop operating systems through FileVault (v.2). With modern hardware, any impact to device performance from the encrypted drive should go unnoticed.

Please refer to the following vendor documents for more information in preparing and managing your MSP assets for encryption:

- Microsoft - Preparing Your Organization for BitLocker: Planning and Policies
https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/prepare-your-organization-for-bitlocker-planning-and-policies
- Apple - Use FileVault to encrypt the startup disk on your Mac
https://support.apple.com/en-us/HT204837
- Apple - Secure device management overview
https://support.apple.com/guide/security/secure-device-management-overview-sec38eb8731b/web

Since a lost or stolen laptop can easily be booted from a USB drive containing an operating system allowing an attacker to access all the files on the computer, requiring full drive encryption on laptops and portable devices should be a standard for the MSP organization. Additionally, with laptop and portable device encryption, the MSP organization will need to have standards and procedures in place to perform regular backups of the full device or its data files for recovery.

Removable Storage Media

Removable and easily transported storage media (such as USB flash drives, USB hard drives or CDs/DVDs) containing sensitive data are to be encrypted and protected by using industry-accepted encryption technologies and every effort should be made to ensure that encrypted removable storage media is physically secured.

While providing an easy and convenient way to transfer or to backup digital files and data, removable storage media, specifically USB flash drive (thumb drives) can easily be lost or stolen. The use of encryption can help protect any sensitive data contained on a removable device if it happens to fall into the wrong hands of an unauthorized third-party.

Nowadays, most business laptops and desktop computers do not come with CD/DVD ROM drives but do come with an assortment of USB connections. As such, the control and encryption of USB-based storage devices will be a risk exposure to data loss that an MSP organization will need to address.

Endpoint Protection

The MSP organization employs an advanced endpoint protection solution that protects systems from file, fileless, script-based, and zero-day threats by using machine-learning or behavioral-based analysis.

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.

- 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, opened and when 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.

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.

Execute 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

Extended Detection & Response (XDR) - (Optional)

Extended Detection response (XDR) technology is currently being evaluated and adopted across the MSP organization.

Formerly known as Endpoint Detection and Response (EDR) or Managed Detection and Response (MDR), Extended Detection and Response (XDR) is an emerging platform designed to deliver visibility into usage data across internal networks, cloud SaaS, endpoints, and business applications all while applying advanced analytics and automation to better detect, analyze, seek and remediate known and emerging threats. Extended Detection and Response (XDR) is the next generation of security tools that stems from the marriage of its EDR and MDR platform predecessors. With XDR, the MSP organization can better monitor and respond to cyber-attacks and incidents across all connected endpoints, networks, SaaS applications, cloud infrastructure, email, and most any network-addressable resource – including managed client systems.

Where EDR was considered a vast improvement over older malware detection products that were based upon signatures and heuristics at the core of antivirus capabilities, XDR greatly extends the range of EDR to integrate with the deployed security solutions across the organization as well as extending into cloud services. With its broader capabilities, XDR incorporates the latest and most current technologies to provide the business much higher visibility into correlated threat information by employing analytics and automation to help identify threats and prevent attacks.

Some benefits of Extended Detection and Response (XDR) services and platforms include:

- XDR services improve overall security operations productivity with alert and incident correlation.
- XDR provides built-in automation for improved alerting and response.
- XDR can reduce the complexity of security configuration and incident response and offer a better security result.

For additional information and research on XDR solutions, review the following resources:

- Cisco – What is Extended Detection and Response (XDR)?
  https://www.cisco.com/c/en/us/products/security/what-is-xdr.html#~types-of-response

- Dark Reading – Why Threat Hunting with XDR matters https://www.darkreading.com/cloud/why-threat-hunting-with-xdr-matters/a/d-id/1337441
- Palo Alto Networks – Cortex XDR: Welcome to the Future of EDR https://www.paloaltonetworks.com/cortex/cortex-xdr
- Trend Micro – What is XDR? https://www.trendmicro.com/en_us/what-is/xdr.html

3-2-1 Backup and Recovery Solution

Advanced back-up and restore capabilities are implemented as a 3-2-1 backup and recovery solution.

As discussed in the IT Nation SECURE MSP+ Playbook: Fundamentals (Yellow Book), the adoption and implementation of a 3-2-1-tiered backup allows for the advanced management of backup and recovery protection capabilities across an MSP organization. In short, the 3-2-1 model indicates that the MSP organization should maintain three (3) copies of the data stored on two (2) different types of media with one (1) 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 and should have documented procedures followed by a competent administrator with experience. 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.

VLAN Segmentation

Adopt the use of a VLAN segmented design to help prevent an internal compromised host from attacking or corrupting additional hosts or client systems that reside on a different network.

The MSP organization should be well underway with a VLAN Segmentation design of their internal networks. Additionally, the support and maintenance of any hosted client systems or services should be VLAN separated from the normal MSP business operations network.

VLAN segmentation was introduced in the IT Nation SECURE MSP+ Playbook: Fundamentals (Yellow Book), for the Advanced (Green Book) certification, the MSP organization will have taken measures to migrate into a more segmented environment without disrupting normal business operations while enhancing overall network security. 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.

Evaluate the Current Environment

To start, have a look at your current environment to get an understanding of the network changes you may need to make and the impact they will have, if any, on the organization. Look at the risk associated with each department, office, application, or task. For departments, you may want to segment your technical staff from the finance and HR areas. That would reduce the potential for sensitive data leaks through your technical staff. Likewise, if Finance or HR personnel fall for a malware email, you can reduce the impact to your technical staff. Perhaps you have a workbench where your technical staff setup new equipment or clean up infected equipment. You might want to consider segmenting that specific area from the rest of your environment to prevent those systems from seeing systems owned by your organization.

Determine the Appropriate Segmentation

After evaluating your environment, make a plan to segment your environment that makes the most sense for your organization. Using the evaluation above, prioritize the segmentation from highest to least risk, while considering the impact on the organization at the same time. That may mean adjusting your plan to move your second most risky segment to be the first one to adjust for the impact on the first. Perhaps the first is finance and it is the end of quarter, so you move the executive team instead. Whichever you decide, make a plan, communicate that plan and be prepared to adjust. We caution against prolonging a move simply because there is never a good time. While that may appear to be true in the moment, the last thing the organization needs is an attack or a breach that could have been prevented or minimized and having to explain why something wasn't done sooner.

Make the Changes

For best results, consult with the switch vendor for the organization and cons**ider 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.
- 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.

Re-evaluate the Changes

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. Properly testing and VLAN changes for security configurations and access controls will help prevent a service outage due to an improper or unauthorized change.

Additionally, once the VLAN change has been implemented, be certain to add the new network to the list of hosts for vulnerability scanning.

Security Measurement Program

Measuring the effectiveness of your security policies and controls are critical to understanding your overall risk and security posture for the business. These measurements are used in multiple areas of your Security Program. We introduced the concept of measurements within the Fundamentals (Yellow Book), and we are asking your MSP organization to add a few more. These new measurements will look at your overall security capabilities, awareness training, and identification of any gaps within your security controls.

Developing a Program to Measure Security Capabilities

Efforts underway to develop a standards program designed to measure security capabilities across the MSP organization.

Measurements provide the organization a way to review risk trends and provide visibility into risk associated with people, process and technology. They also help enable accountability and effectiveness in the management of the risk throughout the organization. In addition, the measurements provide management with input for prioritizing resource allocation in budget and personnel. All of which contribute to an overall cost savings and increased management of risk for the organization in the short and long term.

The key steps in the measurement program are:

1. Selecting and documenting measurements
2. Collecting information for the measurements
3. Analyzing the data
4. Reporting of the results
5. Taking the appropriate action, when necessary

Defining the Key Steps – Selecting the Measurements

IT Nation SECURE has provided a list of basic measurements in the Fundamentals (Yellow Book), and we have included additional measurements below. The organization should determine whether or not these measurements are applicable to your organization. In addition, the organization should determine the input for each of the measurements to ensure collecting the data is available. Look for other measurements that might be applicable to your organization that we may not have listed here. Whichever measurements you choose to select and collect, they should be relevant to your business.

Defining the Key Steps – Collecting the Information

Once you have selected which measurements are relevant to your organization, you need to collect the information for the measurement formulas. Collecting information should be done from the same data sets identified in the measurements and at the same interval. If the measurement is monthly, then ensure the data is collected at the same time every month to give yourself enough time to calculate the measurement for the analysis phase which follows.

Defining the Key Steps – Analyzing the Information

You have selected the measurements and collected the information, now it is time to analyze. When analyzing the collected information, the organization should determine the following:

- Is this measurement providing accurate information, or do we need to adjust?
- If the information is accurate, are the measurements within our risk tolerance for the organization?
- If the risk is too great, what changes do we need to make that will lower the risk?
- Will this change impact our current priority list?
- If yes, what is the impact upon the business for making this change?

Analysis should be performed for all measurements and documented into a reporting format approved by the organization.

Defining the Key Steps – Reporting the Measurements

The organization should consider creating a dashboard for all of the measurement activities to include current state and graphical representation of trending. The reporting dashboard should be created and delivered on a monthly basis to individuals in the organization with a need to know. This should be considered a "company confidential" document since it contains sensitive information about the state of your security controls. This report should be used as the basis for a discussion around the plan of action and milestones (POAM) you have already started. Any new items discovered or identified during the measurement review should be added to the POAM and tracked accordingly.

Defining the Key Steps – Take Action!

As mentioned in the Reporting section, the next step is to formulate a plan and take action to improve the measurement objective to a range that meets the target. Evaluate when the measurement is not meeting the target objective:

- Is the formula not correct?
- Is the data received during the collection phase missing key inputs?
- Perhaps the target itself is not accurate?

Perhaps everything is set correctly and there is another reason for the missed target objective. You may need to take a look at your collection input:

- Do we need to change our processes or procedures?
- Are the security controls performing as expected?
- Do we need to re-evaluate our security controls?

The point here is following through to ensure everything is still performing as expected, whether that be your workforce personnel, technology, or application to ensure they are still meeting your business needs and not causing unnecessary risk for your organization. The measurements are in place to ensure your controls are effective.

Metrics for Security Awareness

Efforts are underway to develop a standards program for metrics and track security awareness across the MSP organization.

Measure the effectiveness of security awareness training, such as number malware infections, Phishing exercises, etc.

The measurement from the Fundamentals (Yellow Book) around awareness really focused on the actual security awareness training itself. In addition to the security awareness training measurement in the Fundamentals (Yellow Book) guide, the team has created a measurement set for your organization to judge the effectiveness of your training based upon the number of reported infections (malware) or phishing attempts. This measurement relies on the organization having a means by which phishing attempts through a phishing campaign managed by the organization can be measured. The malware component data should be accessible through your anti-virus console.

Identify Security Gaps

The MSP organization has policy, standards and procedures in place to identify gaps in security and compliance controls.

Most organizations perform vulnerability assessments against the technology stack to identify vulnerabilities within the operating system and any applications that may be on those systems. This is a good practice; however, it is only part of the risk management equation. There are three areas which need to be assessed to identify the risk in the organization:

1. People, Policy and Process (Human Element)
2. Technology (Vulnerability Assessment)
3. Penetration Test (Internal and External)

The last two are the easiest to perform with the caveat the penetration testing company has done it many times before and comes highly recommended by others. Technology is not your biggest risk, people are, and their actions or lack of action are the reason most organizations experience higher risk incidents. Organizations must assess their human element more today more than ever before. Threats like social engineering, phishing, ransomware, and malicious insiders are growing in popularity. Identifying the gaps within your people, process, and procedures is not an easy task. There are tools available to help identify the gap areas. The best way to get started is to align your organization to a security framework like the NIST Cybersecurity Framework (CSF).

The organization can use the CSF to evaluate and identify areas for improvement of the security controls for the entire organization, not just around the human element. Some of the human element measurements were introduced in the Fundamentals book.

Security Measurement Template

This template should be used to create additional measurements for the organization outside of the ones provided by the IT Nation SECURE Team.

Field	Data
Measure ID	State the unique identifier for measure tracking and sorting. The unique identifier can be from an organization-specific naming convention or can directly reference another source.
Goal	*Statement of strategic goal and/or information security goal.* For system-level security control measures, the goal would guide security control implementation for the that information system. For program-level measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal.
Measure	Statement of measurement. Use a numeric statement that begins with the word, "percentage", "number", "Frequency", "average", or a similar term. If applicable, list the NIST CSF security control(s) being measured. Security controls that provide supporting data should be stated in Implementation Evidence. If the measure is applicable to a specific FIPS 199 impact level (high, moderate, low), state this level within the measure.
Type	Statement of whether the measure is implementation, effectiveness/efficiency, or impact.
Formula	Calculation to be performed that results in a numeric expression of a measure. The information gathered through listing implementation evidence serves as an input into the formula for calculating the measure.
Target	Threshold for a satisfactory rating for the measure, such as milestone completion or a statistical measure. Target can be expressed in percentages, time, dollars, or other appropriate units of measure. Target may be tied to a required completion time frame. Select final and interim target to enable tracking of progress toward stated goal.
Implementation Evidence	Implementation evidence is used to compute the measure, validate that the activity is performed, and identify probable causes of unsatisfactory results for a specific measure. • For manual data collection, identify questions and data elements that would provide the data inputs necessary to calculate the measure's formula, qualify the measure for acceptance, and validate provided information. • For each question or query, state the security control number from NIST CSF that provides information, if applicable. • If the measure is applicable to a specific FIPS 199 impact level, questions should state the impact level. For automated data collection, identify data elements that would be required for the formula, qualify the measure for acceptance, and validate the information provided.
Frequency	Indication of how often the data is collected and analyzed, and how often the data is reported. Select the frequency of data collection based on a rate of change in a particular security control that is being evaluated. Select the frequency of data reporting based on external reporting requirements and internal customer preferences.
Responsible Parties	Indicate the following key stakeholders: • Information Owner: Identify organizational component and individual who owns required pieces of information; • Information Collector: Identify the organizational component and individual responsible for collecting the data. (Note: If possible, Information Collector should be a different individual or even a representative of a different organizational unit than the Information Owner, to avoid the possibility of conflict of interest and ensure separation of duties Similar organizations will need to determine whether it is feasible to separate these two responsibilities.); and • Information Customer: Identify the organizational component and individual who will receive the data.
Data Source	Location of the data to be used in calculating the measure. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information.

Reporting Format	Indication of how the measure will be reported, such as a pie chart, line chart, bar graph, or other format. State the type of format or provide a sample.

Measurement Objectives

The MSP organization should have matured to the point of being able to understand and implement the following objectives as part of a security journey.

These objectives are in addition to the objectives found within the Fundamentals book under the same section.

Security Budget Measurement

Field	Data
Measure ID	Security Budget Measure
Goal	*Statement of strategic goal and/or information security goal.* For system-level security control measures, the goal would guide security control implementation for the that information system. For program-level measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal.
Measure	Percentage (%) of the information security budget devoted to information security
Type	Impact
Formula	(Information Security Budget / Total Information Technology budget) * 100
Target	(Should be an organizationally defined target)
Implementation Evidence	What is the total information security budget for the entire organization? ________________ What is the total information technology budget for the entire organization? _______________
Frequency	Indication of how often the data is collected and analyzed, and how often the data is reported. Select the frequency of data collection based on a rate of change in a particular security control that is being evaluated. Select the frequency of data reporting based on external reporting requirements and internal customer preferences.
Responsible Parties	Indicate the following key stakeholders: • Information Owner: Identify organizational component and individual who owns required pieces of information; • Information Collector: Identify the organizational component and individual responsible for collecting the data. (Note: If possible, Information Collector should be a different individual or even a representative of a different organizational unit than the Information Owner, to avoid the possibility of conflict of interest and ensure separation of duties Similar organizations will need to determine whether it is feasible to separate these two responsibilities.); and • Information Customer: Identify the organizational component and individual who will receive the data.
Data Source	Location of the data to be used in calculating the measure. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information.
Reporting Format	Indication of how the measure will be reported, such as a pie chart, line chart, bar graph, or other format. State the type of format or provide a sample.

Contingency Planning

Field	Data
Measure ID	Contingency Planning Measure
Goal	*Statement of strategic goal and/or information security goal.* For system-level security control measures, the goal would guide security control implementation for the that information system. For program-level measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal.
Measure	Percentage (%) of information systems that have conducted annual contingency plan testing
Type	Effectiveness/Efficiency
Formula	(Number of information systems that have conducted annual contingency plan testing / number of information systems in the system inventory) * 100
Target	(Should be an organizationally defined target)
Implementation Evidence	1. How many information systems are in the system inventory? ________ 2. How many information systems have an approved contingency plan? ___________ 3. How many contingency plans were successfully tested within the past year? ________
Frequency	Collection Frequency: Annually Reporting Frequency: Annually
Responsible Parties	Indicate the following key stakeholders: • Information Owner: Identify organizational component and individual who owns required pieces of information; • Information Collector: Identify the organizational component and individual responsible for collecting the data. (Note: If possible, Information Collector should be a different individual or even a representative of a different organizational unit than the Information Owner, to avoid the possibility of conflict of interest and ensure separation of duties Similar organizations will need to determine whether it is feasible to separate these two responsibilities.); and • Information Customer: Identify the organizational component and individual who will receive the data.
Data Source	Contingency Plan testing results
Reporting Format	Pie chart comparing the percentage of systems that conducted annual contingency plan testing verses the percentage of systems that have not conducted annual testing

Incident Response

Field	Data
Measure ID	Incident Response Measure
Goal	*Statement of strategic goal and/or information security goal.* For system-level security control measures, the goal would guide security control implementation for the that information system. For program-level measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal.
Measure	Percentage (%) of incidents reported within required time frame per applicable incident category
Type	Effectiveness/Efficiency
Formula	For EACH incident category (number of incidents reported on time / total number of reported incidents) * 100
Target	(Should be an organizationally defined target)
Implementation Evidence	1. How many incidents were reported during the period? Category 1 – Unauthorized Access? ______ Category 2 – Denial of Service? ______ Category 3 – Malicious Code? ______ Category 4 – Improper Usage? ______ Category 5 – Scans/Probes/Attempted Access? ______ Category 6 – Investigation? ______ 2. How many incidents involving personally identifiable information (PII) were reported during the period? ______ 3. Of the incidents reported, how many were reported within the prescribed time frame for their category, according to the time frames established by the organization? Category 1 – Unauthorized Access? ______ Category 2 – Denial of Service? ______ Category 3 – Malicious Code? ______ Category 4 – Improper Usage? ______ Category 5 – Scans/Probes/Attempted Access? ______ Category 6 – Investigation? ______ 4. Of the PII incidents reported, how many were reported within the prescribed time frame for their category, according to the time frames established by the organization? ______
Frequency	Collection Frequency: Monthly Reporting Frequency: Monthly
Responsible Parties	Indicate the following key stakeholders: • Information Owner: Identify organizational component and individual who owns required pieces of information; • Information Collector: Identify the organizational component and individual responsible for collecting the data. (Note: If possible, Information Collector should be a different individual or even a representative of a different organizational unit than the Information Owner, to avoid the possibility of conflict of interest and ensure separation of duties Similar organizations will need to determine whether it is feasible to separate these two responsibilities.); and • Information Customer: Identify the organizational component and individual who will receive the data.
Data Source	Location of the data to be used in calculating the measure. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information.
Reporting Format	Indication of how the measure will be reported, such as a pie chart, line chart, bar graph, or other format. State the type of format or provide a sample.

Maintenance

Field	Data
Measure ID	Maintenance Measure
Goal	*Statement of strategic goal and/or information security goal.* For system-level security control measures, the goal would guide security control implementation for the that information system. For program-level measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal.
Measure	Percentage (%) of system components that undergo maintenance in accordance with formal maintenance schedules
Type	Effectiveness/Efficiency
Formula	(number of system components that undergo maintenance according to formal maintenance schedules / total number of system components) * 100
Target	(Should be an organizationally defined target)
Implementation Evidence	1. Does the system have a formal maintenance schedule? ☐ Yes ☐ No 2. How many components are contained within the system? ______ 3. How many components underwent maintenance in accordance with the formal maintenance schedule? ______
Frequency	Collection frequency: Quarterly Reporting frequency: Annually
Responsible Parties	Indicate the following key stakeholders: • Information Owner: Identify organizational component and individual who owns required pieces of information; • Information Collector: Identify the organizational component and individual responsible for collecting the data. (Note: If possible, Information Collector should be a different individual or even a representative of a different organizational unit than the Information Owner, to avoid the possibility of conflict of interest and ensure separation of duties Similar organizations will need to determine whether it is feasible to separate these two responsibilities.); and • Information Customer: Identify the organizational component and individual who will receive the data.
Data Source	Maintenance schedule, Maintenance logs
Reporting Format	Indication of how the measure will be reported, such as a pie chart, line chart, bar graph, or other format. State the type of format or provide a sample.

Physical and Environmental

Field	Data
Measure ID	Physical Security Incidents Measure
Goal	*Statement of strategic goal and/or information security goal.* For system-level security control measures, the goal would guide security control implementation for the that information system. For program-level measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal.
Measure	Percentage (%) of physical security incidents allowing unauthorized entry into facilities containing information systems
Type	Effectiveness / Efficiency
Formula	(number of physical security incidents allowing unauthorized entry into buildings containing information systems / total number of physical security incidents) * 100
Target	(Should be an organizationally defined target)
Implementation Evidence	1. How many physical security incidents occurred during the specified period? ______ 2. How many of the physical security incidents allowed unauthorized entry into facilities containing information systems? ______
Frequency	Collection frequency: Quarterly Reporting frequency: Quarterly
Responsible Parties	Indicate the following key stakeholders: • Information Owner: Identify organizational component and individual who owns required pieces of information; • Information Collector: Identify the organizational component and individual responsible for collecting the data. (Note: If possible, Information Collector should be a different individual or even a representative of a different organizational unit than the Information Owner, to avoid the possibility of conflict of interest and ensure separation of duties Similar organizations will need to determine whether it is feasible to separate these two responsibilities.); and • Information Customer: Identify the organizational component and individual who will receive the data.
Data Source	Physical security incident reports, physical access control logs
Reporting Format	Indication of how the measure will be reported, such as a pie chart, line chart, bar graph, or other format. State the type of format or provide a sample.

Security Awareness Training Effectiveness

Field	Data
Measure ID	Security Training Effectiveness
Goal	*Statement of strategic goal and/or information security goal.* For system-level security control measures, the goal would guide security control implementation for the that information system. For program-level measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal.
Measure	Percentage (%) of reported successful malware infections and the percentage of successful phishing attempts through campaign within the organization
Type	Effectiveness
Formula	Malware: (number of reported successful malware infections / total number of reported incidents) * 100 Phishing: (number of successful phishing attempts / total number of phishing attempts) * 100
Target	Zero (0)
Implementation Evidence	How many reported successful malware infections were reported over the period? ______ How many total incidents were reported over the period? ______ How many successful phishing attempts reported over the period? ______ How many phishing emails were sent through the exercise platform over the period? ______
Frequency	Malware: Monthly Collection and Reporting Phishing: Monthly Collection and Reporting
Responsible Parties	Indicate the following key stakeholders: • Information Owner: Identify organizational component and individual who owns required pieces of information; • Information Collector: Identify the organizational component and individual responsible for collecting the data. (Note: If possible, Information Collector should be a different individual or even a representative of a different organizational unit than the Information Owner, to avoid the possibility of conflict of interest and ensure separation of duties Similar organizations will need to determine whether it is feasible to separate these two responsibilities.); and • Information Customer: Identify the organizational component and individual who will receive the data.
Data Source	Malware: Ticket system, Anti-virus Console Phishing: Exercise Platform
Reporting Format	Indication of how the measure will be reported, such as a pie chart, line chart, bar graph, or other format. State the type of format or provide a sample.

Security Lifecycle

When implementing information security services, an MSP organization will consider factors such as service provider qualifications, operational requirements, the type of service, and the ability to deliver adequate protection across the business. The adoption of a Security Lifecycle allows for the development of processes and procedures designed to enable the business to implement or develop services and solutions in a manner that limits security risks, addresses security vulnerabilities, and reduces overall expenses.

As discussed in the IT Nation SECURE Fundamentals (Yellow Book), a Security-Lifecycle allows an MSP organization to adopt a framework that allows for the selection, implementation, and management of the information security and service. The following requirements are adopted from the NIST SP 800-35 and are discussed at length within the IT Nation SECURE MSP+ Fundamentals (Yellow Book):

- **Phase 1: Initiation**
  The MSP 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 MSP organization determines the security posture of the current environment using metrics and identifies the requirements and viable solutions.
- **Phase 3: Solution**
  Decision makers within the MSP 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 MSP organization selects and engages the service provider, develops a service arrangement, and implements the solution.
- **Phase 5: Operations**
  The MSP 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 MSP organization ensures a smooth transition as the service ends or is discontinued.

Objectives and Baselines

Efforts are currently underway to establish security and risk management objectives and environment baselines.

Given the modern business ecosystem of connected and interdependent onsite devices, cloud services and third-party platforms, the most reliable way for an MSP organization to ensure the stability and security systems and services is to regularly perform assessments and proactive maintenance. Most every hardware and software vendor and manufacturer regularly provide firmware updates and security patches for the supported life of their products. These patches or hotfixes may bring additional features or functionality to this solution, but, for the most part, these releases address known vulnerabilities, fix bugs, and may resolve other underlying issues of performance within the product. Without an effective way to properly identify, patch, and manage IT systems or digital assets throughout their life-cycle, an MSP organization may find it nearly impossible to address the ever-evolving cybersecurity threats and challenges that may impact business operations and services provided to existing and potential customers.

The first step for an MSP organization to adopt an effective cybersecurity program with supporting security life-cycle practices is to understand what exactly the business is trying to protect. Time, talent, and funding will need to be invested by the MSP organization in order to identify and document business critical systems and sensitive data in order to establish baseline security objectives and controls to help reduce the risk of cybersecurity incidents and potential data breaches. In short, the security life-cycle objectives and baseline controls serve to advise and guide the MSP organization on how to make the most effective use of the cybersecurity investments made to support business operations and customer services.

In addition, objectives and baselines discussed within the IT Nation SECURE Fundamentals (Yellow Book), an MSP Organization should determine what technology, systems and data are in scope for the implementation of baseline security controls. Identified assets should be listed as either in scope for baseline controls or tagged as an excluded asset. All assets excluded from baseline security controls must have a documented rationale along with management acceptance and approval for the risk.

Once information technology, services and data systems have been identified, the MSP organization must assess the value and criticality of each asset along with its worth to the business. It may take some time, but the business must thoroughly map out all hosts and services that reside or connect to the company network. For each asset, identify all key components of individual servers, document the networking infrastructure that connects those servers, take and inventory of the software running on each server, and what type of data is stored on each server. Systems housing sensitive customer data as well as any systems containing proprietary or confidential company data should be flagged as the highest priority for security controls.

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 assess the level of damage or impact that may result from a cybersecurity incident or data breach.

- **Confidentiality**
  Damages relate to the unauthorized disclosure of sensitive information (e.g. if someone disclosed sensitive information publicly or to a competitor). Confidentiality of data may be addressed through physical or logical access controls, user identity and access management, and encryption.
- **Integrity**
  Damages arise from the unauthorized modification of information (e.g. if someone modified sensitive information to be incorrect). At a minimum, integrity involves monitoring the modification or deletion of files. Additionally, there are a variety of software tools and utilities available for file and system integrity checking that compare hashed values and / or generate log entries and alerts upon the modification or deletion of files.
- **Availability**
  Impact occurs when information was either temporarily unavailable for use or was permanently lost (e.g. if someone took down an organization’s website, deleted sensitive information, or fell victim to a ransomware attack). 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 or ransomware attacks.

Additionally, templates and baselines are commonly used in Microsoft Active Directory network environments. The use of templates to load groups of policies with a single operations procedure is a key benefit to standardizing on the Microsoft platform. It is a best practice for an MSP organization to assess and adopt a Microsoft security policy 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.

- Microsoft - Windows Security Baselines
  https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines
- Microsoft - Group Policy Settings Reference Guide for Windows & Widows Server
  https://www.microsoft.com/en-us/download/details.aspx?id=25250
- Microsoft - Reference guide for managing and deploying Microsoft Windows 10
  https://docs.microsoft.com/en-us/windows/deployment/deploy-whats-new

Life-Cycle Policies

Security and risk management life-cycle policies serve as the foundation of a strategic program allowing the MSP organization to keep pace with a dynamic and evolving threat landscape.

The successful adoption of a cybersecurity policy across the MSP organization depends in large part upon the business approaches the tasks of policy development, publication, adoption, and review. As management and workforce personnel responsibilities associated with security policy life-cycle processes are distributed throughout the business, having the organization take a structured approach will offer the best chance to minimize risk with standardized cybersecurity policies and best practices.

Establish a policy and standard where an inventory of all IT assets which store, process, transmit, or otherwise have access to restricted or sensitive data are identified, documented, and stored in a centralized information repository. The scope should apply to all employees, workforce personnel, contractors and third parties who handle IT assets and data on behalf of the MSP organization. For example, IT assets may include the following elements:

Hardware

- Endpoint Devices: desktops / laptops / servers / tablets / kiosks
- Network Devices: routers / Wi-Fi / switches / firewalls / network appliances
- Voice Devices: PBX technology / IP phones / video
- Mobile Devices (company issued): Android / iPhone / tablets
- Office Support Devices: printers / fax machines / scanners / copiers / digital whiteboards

Software

- Operating System: License: Microsoft Windows / Mac OSX / UNIX / LINUX
- Database System License: Microsoft SQL / Oracle / open source
- Cloud Services (SaaS): Microsoft Office 365 / Azure / Google G Suite / AWS / Oracle
- Business Application: Microsoft Office / QuickBooks / Adobe / ConnectWise

Information Assets

- Company policy and guidelines
- Company standards and procedures
- Company data: security / passwords / network maps / contacts / support tickets / etc.
- Company employee / workforce personnel training and security awareness training
- Company onboarding Information for employee / workforce personnel
- Customer onboarding information
- Customer data: security / passwords / network maps / contacts / support tickets / etc.

For each information asset, the MSP organization will designate an Information Asset Owner as the individual responsible for identifying, classifying, and protecting information assets in accordance with the standards and guidelines expressed within the Information Security Policy of the MSP organization.

Risk Awareness

The MSP Organization fosters an awareness of existing security risk and is working to understand how risks impact the business, operations and services provided to customers.

Risk awareness is not the same as understanding risk. The MSP organization must implement a risk assessment process included within the security life-cycle management policy, standards, and procedures. As a best practice, an annual assessment of IT assets and services should be performed in order to identify security risks and implement risk-based security controls to better protect systems and services. Management and key stakeholders of the MSP must work to evaluate security threats and the potential business impact to the organization as well as any threats that may impact software and services offered to customers.

Additionally, any identified risk must have an appropriate risk treatment or mitigation plan that defines how the MSP organization works to address the risk, the approval process for the identified risk, and details as to how the risk will be tacked and monitored. As part of the defined risk treatment, management and key stakeholders of the MSP organization may decide to accept the security risk, transfer the risk, mitigate the risk, or avoid the risk. Whatever the decision and method, appropriate justification for each action must be documented as part an overall risk management program.

Implementing Security Procedures

Implementing security procedures with adequate workforce and resources to accomplish Security Life-Cycle goals and objectives across the MSP organization.

As a best practice, and MSP should strive to meet the following.

- **Ownership of the Project or Service**
  Ensure there is an implementation owner with executive support, and that those implementing the project or service have a stake and responsibility in the security plan and supporting procedures that are in line with business operations.
- **Over Communicate**
  The security plan and procedures should be communicated to all key stakeholders. Management and supporting workforce personnel should each understand their roles and responsibilities.
- **Establish Long Term-Goals**
  Consumed by daily business operations, owners and managers may lose sight of long-term security goals. Make it a point to regularly review and update the security procedures.

- **Have a Meaningful Plan**
  The vision, mission, value statements, and steps should be concise and supported by management and workforce personnel responsible for the nurture and success secure operating procedures.
- **Talk Strategy**
  Keep security strategy, plans and procedures a part of regular messaging throughout the MSP organization.
- **Provide Progress Reports**
  Initiate a method to track progress of the security plan and other business processes that are important to the MSP organization. Make certain that management and invested workforce personnel can recognize progress and momentum within the security lifecycle.
- **Drive Accountability**
  Each measure, objective, data source, and initiative must have an owner as accountability and high visibility help drive changes towards security plans and procedures across the MSP organization.
- **Empower Teams**
  As accountability may provide strong motivation for improving individual and overall performance, management and workforce personnel must also have the authority, responsibility, and tools necessary to impact relevant plans and security measures. Without proper support and funding, lack of involvement and ownership may occur.
- **Monitor and Measure**
  Over time, the established products or services may evolve and mature to address any number of events or adapt to market changes. As such, established metrics for monitoring and measuring the MSP organization allows stakeholders to evaluate performance and identify the ways and means for improvement.

Risk Management Program

Risk is part of everyday life. Each of us deal with risk on a daily basis in multiple arenas; individually, as a family, employee and business owner. The risks for each of those areas do share some commonality, however as a business owner of a managed service provider, you have other risk to concern yourself with daily. Risk for the MSP business owner is not simply limited to information technology within your own organization. You are responsible for the information technology and, more importantly, your client's business as well. If your client has a breach, compromise, or incident they will hold you accountable. The more clients you have, the more risk you assume. That is a lot of risk. Let us not stop there. You also have employees and potentially contractors who do work on your behalf. Without the proper safeguards in place, monitoring of those safeguards, and measurement of those safeguards to ensure effectiveness, you have just compounded your risk. Now you are completely overwhelmed and unable to sleep at night wondering if you are the next breach, compromise, or incident. The bad news is no matter how hard you try you will never eliminate risk. The good news is you can plan for that risk and minimize the impact for you, your business, and your clients. This section is focused on how to make that happen for you.

Developing a Risk Management Plan is the best way for your organization to survive in the likely event of an incident occurring. As you look back through Fundamentals and this Advanced book, you will see we have been preparing you for this moment. As part of the SECURE MSP+ Certification, we want your organization to become fully aware of all of the risk with your business, be able to report on that risk, and make adjustments to your risk posture to minimize your exposure to risk.

Like anything within information technology, a framework is needed to provide guidance and direction along with context for the organization to understand, identify, and develop a plan to mitigate risk. While there is no dedicated risk framework for managed service providers today, the IT Nation SECURE team is recommending you start with NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and NIST SP 800-39, *Managing Information Security Risk*. If you are an ISO shop, you should have a look at ISO/IEC 31000, *Risk management – Principles and guidelines*, ISO/IEC 31010, *Risk management – Risk assessment techniques*, ISO/IEC 27001, *Information technology – Security techniques – Information security management systems*, and ISO/IEC 27005, *Information technology – Security techniques – Information security risk management systems*. Please note there is no requirement in the MSP+ Certification path for your organization to be certified as ISO 27001 or 27005 compliant. The information contained within this book is a good starting point should you wish to pursue obtaining that compliance and would also be useful if pursuing SOC 2 compliance. This book section is not a guarantee of SOC 2 compliance. There are more tasks and objectives the organization must complete including an audit by a certified SOC 2 auditor.

Strategy and Objectives

The MSP organization has efforts underway to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level of acceptance and/or compliance in line with management objectives.

To establish your risk objectives, the organization must define the strategy for risk. This is really about creating your organizational risk frame. To create the frame requires involvement from the entire organization. We are not saying every individual, but rather senior leaders/executives, mid-level planners, and the individuals performing the day to day work. This frame will establish the context for your risk-based decisions. The framing component will lead to your risk strategy that addresses how your organization intends to assess risk, respond to risk, and monitor risk. This includes:

- Risk Assumptions (about the threats, vulnerabilities, consequences/impact and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time)
- Risk Constraints (on the risk assessment, response, and monitoring alternatives under consideration)
- Risk Tolerance (levels of risk, types of risk and degree of risk uncertainty that are acceptable for your organization)
- Priorities and Tradeoffs (the relative importance of your business functions, trade-offs among different types of risk that you face, time frames in which your organization must address risk, and any factors of uncertainty the organization needs to consider in the risk response)
- Uncertainty (do not know what it is, but it might be important)

This leads to establishing your foundation for a Risk Management Program and delineates the boundaries for risk-based decisions. There are three components to the program; assess, respond and monitor. In the assess component of the risk frame, the organization will identify the threats to your organization (operational, assets, or individuals) or against your clients, vulnerabilities (both internal and external), harm (consequences or impact from the threats or vulnerabilities), and likelihood the harm will occur. The end result will be your determination of risk. Support for your risk assessment comes from identifying the tools, techniques, and methodologies your organization will use to assess risk, the assumptions related to the risk assessments, the constraints that may affect the assessments, defined roles and responsibilities, how the assessment information is collected, processed, and communicated throughout the organization, how the assessment is conducted within your organization or with your clients, the frequency of the assessments (recommended quarterly to start), and how the threat information is obtained (RSS feeds, ISAO/ISAC, other trusted source).

Once that area is completed, you can move on to how the organization responds to results of the assessment. Your response should provide a consistent, organization-wide response to the risk in accordance with your risk frame. This is done by developing alternative courses of action for responding to risk, evaluating those alternative courses, determining the appropriate course of action consistent with your risk tolerance (see risk frame) and implementing the risk response based upon your selected course of action. You will need support for this component as well; describe the type of risk responses that can be implemented (accepting, avoiding, mitigating, or transferring). You may see references to sharing of risk and that is never a good idea. It only leads to confusion since there is no clear owner of the risk. Therefore, you should avoid the risk of sharing risk. Responding to risk may require you identify tools, techniques and methodologies to develop your courses of action, how your courses of action are evaluated, and how risk responses are communicated across your organization, your client's and any external entities like your supply chain partners.

The last component of risk management addresses how the organization monitors the risk over time. The purpose of monitoring is to verify your planned response measures are implemented and the information security requirements implemented are satisfied, you are able to determine the effectiveness of the response measurements following their implementation, leading you to identify any risk-impacting changes to your organization systems or environments in which they operate. To support the monitoring component, your management plan should describe how compliance is verified and how the ongoing effectiveness of risk responses is determined. Again, you may need tools, techniques, or methodologies to assist with mitigation are implemented correctly, operating as intended and producing the desired results to reduce the risk to the MSP organization, its business operations and services provided.

Risk Management Policies

The MSP organization has adopted policies and standards for risk management.

The Governance program started in the Fundamentals and added to here in the Advanced book are setting the stage for an effective risk management program. As stated in Fundamentals, the foundation for your information security starts with your policies. Those same policies are at play here as part of your risk management. The sample policies provided in the University were created around ISO 27001 to meet a risk-based approach. The link for the policies in the ConnectWise University is here:
https://docs.connectwise.com/ConnectWise_Business_Knowledge/Information_Security_Policies

Understanding of Business and Security Risks

The MSP organization has efforts underway to better identify and understand business and security risks.

With your newly gained knowledge of determining your risk as part of the risk frame above, you should have a better understanding of the risk for your organization. This understanding should be communicated across your entire organization and employees made aware of the risks associated with the business, their impact on the risk, how to respond to risk, and their role in monitoring the risk in their areas. Every role within the organization plays a part in your risk management; be transparent, be open, and be honest. Make sure the response is defined clearly in your risk management plan. You may need to have another look at your incident response and business continuity/disaster response plans as well to ensure they all align. Once you have a handle on your own risk, it will be much easier to communicate with how you can help clients to minimize their risk. A solid risk management program will lead to trust not only within your organization, but with your clients and third-party vendors as well.

Understanding of Threat Environment

The MSP organization understands the existing threat environment to business operations and clients.

As part of your risk frame, you were asked to identify the threats and threat information on a regular cadence. There are many avenues for your organization to stay on top of threats specific to your industry or those of your clients. One way is to become an active participant in the technical service provider-information sharing and analysis organization (TSP-ISAO). This is a non-profit organization currently led by CompTIA. There are other information sharing and analysis communities (ISAC)s as well. Gathering threat information for your client industries may also prove useful. You can visit https://www.isao.org and search for the various organizations and communities available today to gather threat intelligence or provide intelligence.

- ISAO Standards Organization
  https://www.isao.org/

Addressing Critical Systems

The MSP organization has an Initial security strategy program underway to address critical systems/services.

Start your risk management on your critical systems, services and processes. You may also wish to include your critical customers; ones that have compliance or regulatory requirements. Once you have gone through the three components: Assess, Respond, Monitor, you can then focus on the next set of systems until you have all of your systems, clients and their systems covered under your risk management program. Ensure you are constantly and consistently reviewing your risk measurements, monitoring your security controls and making adjustments based upon the daily threat landscape.

Implementing Risk Management

The MSP organization has efforts underway to implement risk management procedures with adequate resources and personnel.

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. 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 as we pointed out in the Fundamentals. This section is designed to take your organization to the next level and develop a formal program. Implementing the above items will take time, a lot of effort, energy and a lot of patience. Planning is key as you have learned through this book. With that in mind, please refer to NIST Special Publication 800-39, pages 34 through 48. Those pages specifically outline the steps and tasks for Risk Framing, Risk Assessment, Risk Response and Risk Monitoring. They will take you all the way through implementing risk management within your organization. If you get stuck or have questions, please send an email to the IT Nation SECURE team. We are here to help. ITN_Secure_Cert@connectwise.com

Vulnerability Management / Assessment Program

As a fundamental practice, the MSP organization should have taken the time to understand all the software and services used within their environment. The primary focus of 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 identified and researched to determine if there are any know vulnerabilities, a course of action for prioritizing systems for patching or mitigating vulnerabilities of operating systems and business software.

Documented Procedures

The MSP organization will have documented standards and procedures for the identification, remediation, prevention, and management of system vulnerabilities in order to protect networked hosts, services, and data.

Many MSPs organizations are unable to distinguish between the activities included in varying forms of assessments: Network Assessment, Security Assessment, Vulnerability Assessment, and Penetration Testing. Understanding the business problems that each type of assessment solves for and building use-case scenarios is important to considering what type of assessment best meets the strategies within a vulnerability management program.

To begin the process, the MSP 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, the business can develop a program plan. This includes documentation surrounding the following aspects:

- 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 Assessment

In short, a vulnerability assessment or vulnerability analysis is the process of identifying the security vulnerabilities within networks, systems, and hardware and then taking steps to fix those security vulnerabilities.

Internal Scans:

- Check and/or validate existing patch levels and host system baseline security configurations.
- Test the security and anti-malware solutions (e.g., to ensure that systems are resistant to malicious inbound emailed attachments and web-downloadable binaries and executables).
- Performed on-site by workforce personnel or third-party contractor who is qualified to conduct the testing.
- Assessment scans completed with authentication (having access credentials and user privileges) in order to properly assess patches and vulnerabilities.

External Scans:

- Test the patch levels and host system baseline configurations, but from the public / internet facing services and infrastructure.
- Performed off-site / remotely by workforce personnel or third-party contractor who is qualified to perform the testing.
- Assessment scans completed unauthenticated (without authentication credentials or user privileges) in order to properly assess patches and vulnerabilities.

Upon completion of the vulnerability scanning tests, a report of the findings must be produced stating the outcomes and explaining what actions, if any, should be taken in order to eliminate or mitigate any identified risks or vulnerabilities. Such vulnerability assessment reports are designed to provide the MSP organization and key business stakeholders meaningful information about risks to business operations and services provided.

Vulnerability Management

Vulnerability management is a key component in understanding business risk across the MSP organization. To feed and nurture a successful vulnerability management program, the business needs to understand how vulnerabilities impact the overall weaknesses within the networked environment. A best practice is to use a risk-based approach in order to make appropriate decisions on how and when to mitigate identified vulnerabilities within a prioritized manner that first addresses the most critical systems along with the most critical issues. For clarification, vulnerabilities may encompass more than just regular, simple system and application patching. Flaws within the design (hardware, software, and architecture), the code (operating systems, applications, firmware), and business process (missed steps, insecure procedures) may all contribute to areas where the busines is vulnerable to threats and risk. A successful vulnerability management program integrated within business planning and operations, will provide many returns from its investment.

Attackers constantly seek new exploits and vulnerabilities to exploit, however, they always find an easy path in taking advantage of older, known vulnerabilities that remain unpatched. For an

MSP organization, having a vulnerability management framework in place where regular, ongoing assessments are conducted to check for new vulnerabilities remains crucial for preventing cybersecurity breaches. Without a proper program oversight and an operational practice involving vulnerability testing and patch management, security gaps may be left open within the MSP business networks for an extended period of time. This opening may allow cyber attackers the opportunity to exploit vulnerabilities and carry out an intrusion and compromise the confidentiality, integrity and availability of business operations and services.

When building an internal vulnerability management program, there are several factors that an MSP organization will need to consider:

- **Inventory Management**
  What systems and assets are on the network? Having an inventory of all IT assets which store, process, transmit, or otherwise have access to restricted or sensitive data is crucial for verifying that the organization has addressed all vulnerabilities across the business networks. If an unknown asset or host has been found on the network, then the odds are that it will likely have unpatched vulnerabilities and may open the business up to additional risk.

- **Patch Management**
  How will security patches be delivered to IT and networked assets across the MSP organization? When, and how often will patches be applied? Will regular business service be disrupted, or will systems experience any downtime to apply patches that address major vulnerabilities? Requirements and best practices for developing and implementing a patch management program across the MSP organization will be discussed in the following section.

- **Vulnerability Scanning Solutions**
  How will the MSP organization check for vulnerabilities? It is important to have workforce personnel who are trained and have experience in working with a comprehensive collection of vulnerability scanning tools to use for detecting issues and documenting them for patching or remediation. Checking external network assets (such as vendor networks, cloud-based applications, and externally hosted servers) with vulnerability scanners is also crucial for modern vulnerability testing.

- **Risk Assessment**
  What are the biggest security risks revealed while performing vulnerability scans and penetration testing? When allocating money, time and workforce resources to patch management, it is important for the business to prioritize addressing the simplest vulnerabilities that have the greatest impact on improving network and host security across the MSP organization.

Threat Intelligence

Efforts underway to adopt the use of threat intelligence to be better informed of cybersecurity vulnerabilities and issues that may impact the MSP organization.

The primary method for identifying new threats as they arise will be through vendor and security-specific internet mailing lists, feeds, and notification services. Many publicly available sources of system security alerts and advisories are available to most anyone with an internet connection. For example, the U.S. Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories (free to the public) to maintain situational awareness across the federal government and in the public. Additionally, many software vendors, subscription services, and relevant industry information sharing and analysis centers (ISACs) also provide security alerts and advisories. Some examples of such communications include notifying relevant external organizations, external mission/business partners, supply chain partners, external service providers, and peer or supporting organizations.

Although not complete, the following is a recommended list to which the MSP organization should subscribe. Additionally, there may be other vendors that are applicable to a specific line of business with specific software packages and systems. A more detailed list for sources of cybersecurity and vulnerability alerts and advisories can be found in **Appendix B: Security Alert & Advisory Resources** at the end of this document.

- Computer Emergency Readiness Team Coordination Center (CERT/CC)
https://www.kb.cert.org/vuls/
- NIST National Vulnerability Database (NVD)
https://nvd.nist.gov/
- US-CERT National Cyber Awareness System
https://www.us-cert.gov/ncas
- European Union CERT (CERT-EU)
https://cert.europa.eu/cert/filteredition/en/CERTNewsFilter.html
- Multi-State Information Sharing & Analysis Center (MS-ISAC)
https://www.cisecurity.org/ms-isac/
- SANS Internet Storm Center (ISC)
https://isc.sans.edu/
- U.S. Department of Homeland Security, Automated Indicator Sharing
https://www.us-cert.gov/ais

Alignment with Business

Efforts underway to ensure business operations and goals are aligned to reflect measures required for protection from any newly discovered vulnerability, threat, or risk to the MSP organization.

Having secure configurations and creating the core capability of a vulnerability management program starts by having dedicated subject matter experts. 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 such tests across the business. This helps to manage (track, report on, correct) security vulnerabilities, threats, and risks as part of the overall vulnerability management program.

As vulnerabilities are tied to business applications and services, responsible workforce personnel and key stakeholders can quickly assess potential options and scheduling of remediation efforts based upon the total impact on business productivity and services. By presenting vulnerabilities within the understood context of business processes and by involving all relevant workforce personnel and stakeholders will allow the MSP organization to align security culture and practices with the business strategy.

Aligning a vulnerability management program with the business allows vulnerability management into a respected, strategic business asset.

Assessment of Critical Systems

Efforts underway to regularly conduct a thorough assessment of potential risks and vulnerabilities that may impact the confidentiality, integrity, and availability of critical systems and important data.

To ensure the comprehensive protection of business-critical systems, an MSP organization should identify and document what critical systems, services, and data must ultimately be protected. The security of critical systems should be designed to meet the immediate business and maintain a certain flexibility to address potential emerging threats. Additionally, the MSP business operations and services must be flexible enough to meet any future needs as the organization grows and changes. Having the MSP organization adopting best practices surrounding the protection and security of their own business systems and data will help to avoid a potential downstream impact to their client IT systems and their data environments.

Patch Management Program

A regular part of the security routine must involve the planning, testing, implementing, and auditing of patches through an automated patch management solution. At a minimum, an MSP organization should ensure that server and host operating systems, as well as the individual business software programs on the client's computer, are inventoried and patched on a regular schedule. Additionally, the MSP organization must 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 impacted customers.

Patching Schedule

The MSP organization performs regular patching of IT systems and applications.

Product vendors will normally provide fixes for vulnerabilities identified in products that they still support and have not yet reached their end of support life. These files come in the form of software updates known as patches. These patches may be made available to customers immediately or on a regular release schedule (perhaps monthly).

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 system upgrades and maintenance support
- Patch vulnerabilities regularly

The MSP organization may also want to adopt a patching schedule similar to the following standard best practices:

- All security patches are evaluated for applicability and impact within 5 calendar days of their release.
- Critical, high, and/or important patches are implemented within 5 calendar days of release.
- Medium/moderate patches within 14 calendar days of release.
- Low priority patches within 60 calendar days of release.

Security Configuration Management

Efforts underway to establish and enforce baseline security configuration settings and patch levels for IT assets employed across the MSP organization.

The secure management and control of baseline configurations for a server or application is designed to enhance security and lessen the risk to the business. At a program level, configuration management involves most every aspect of IT infrastructure including both physical and digital assets e.g., hardware, software, firmware, and documentation.

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.

Attackers are looking for legacy or unpatched systems with default settings that allow them to be immediately vulnerable. Once an attacker exploits a system, they start making changes to files in order to ensure their access, encrypt the host with ransomware, or use the compromised system as a launchpad for additional attacks. The use of security configuration management and monitoring tools can be a helpful utility for the MSP organization to use in order to identify misconfigurations or to detect any unusual changes to critical files or registry keys on a host system.

Baseline configuration management and security hardening tasks should include:

- Removing unnecessary services from bother servers and endpoint systems
- Installing the latest operating systems and vendor service packs
- Updating to the latest point release of an application and applying vendor service packs
- Renaming default accounts on servers, endpoints, network devices, and software applications
- Changing default account access
- Enabling security configurations and baseline security policies
- Enable auditing and logging of key system and security events
- Use internal firewalls, access control lists (ACLs), or configure network VLAN segmentation to help protect networked systems
- Configure automatic updates or have the means to centrally manage updates
- Implement practical physical security measures – e.g., laptop locks, locked racks in the server room, cameras for sensitive areas, clean desks, locked screen when unattended, etc.

Documented Practices

The MSP organization has documented and adopted patch management standards and procedures as part of an overall change management process.

For an MSP organization, a well-defined patch management procedure should fit within an overall change management program and should include documented procedures involving each of the following steps as a process flow:

- Change request submittal
- Risk / impact assessment
- Approve / reject change
- Testing
- Scheduling / user notification / training
- Implementation
- Validation checking
- Documentation centrally stored and accessible by authorized users

Admittedly, there are times and emergency situations where changes may need to be made without following the change management process established by the MSP organization. Such cases should prove to be rare and then only performed by keep workforce personnel that are authorized to make an emergency change to production systems. Once implemented, an emergency change should be documented and passed through the "official" change management process to benefit from the additional validation and documentation protocols that are required through the change control process.

Change Management

The MSP organization is following an established change management process for patching identified vulnerabilities across all IT systems and applications.

Change is the one constant for most any organization and managing changes in the configuration of IT assets and services remains an essential element of IT security and oversight. Though similar, change management is sometimes confused with configuration management. Change management is only a part of a much broader configuration management process to ensure stability of business systems and services and to avoid potential unapproved or undocumented changes.

Since the configuration of an information system and its components has a direct impact on the security posture of the system. As such, how those system configurations are implemented and maintained requires a unified approach in order to provide acceptable security.

For an MSP organization, a change management program should account for the following:

- Scope and administrative controls incorporated into organizational change control policy
- Formal review process of all proposed changes
- Only approved changes are implemented

- Periodic re-assessment and vulnerability scanning of the environment to evaluate the need for upgrades or modifications to established security baseline configurations.

Patch Testing

The MSP organization has established set of planned tests to validate system configuration changes and assess patch implementation across IT systems and applications.

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.

A set of planned and documented (or scripted) tests are developed to verify that a patch change accomplished its intent and does not adversely affect other system components or functionality. This plan may be specific to each change, but it should follow similar established standards for testing and deployment of patches to hardware, firmware, operating systems, and applications.

Prior to introduction into the production network or systems, it is a best practice for all changes to first be tested on a test platform isolated from the production business environment and services. Never test on production systems.

A documented test plan must be followed to ensure no adverse effects on the network, systems, or applications. Any discrepancies should be documented, and a new change request should be generated for the new process once all issues have been resolved.

Disaster Recovery/Business Continuity Plan (DR/BCP)

A business disruption can cost money, impact the availably to provide services, and place strain customer relationships. An additional approach to addressing or mitigating risk stems from establishing best practices and operating procedures within a business continuity management program. The MSP organization should design and execute effective disaster recovery (DR) and business continuity plans (BCP). Good DR/BCP programs take time to develop and include many aspects and management oversights from risk assessments, disaster tracking, human resources, facilities management, emergency management, as well as the technology utilized for data backup and recovery actions.

Plan Development

A formal Disaster Recovery (DR) & Business Continuity Plan (BCP) is documented and scheduled to undergo an annual review with plans for testing procedures to measure recovery capabilities and adapt to business needs.

It is recommended that the MSP organization develop and create a documented playbook to address the most likely disaster / crisis scenarios and along with the planned responses from the business. Plans are to include the assignment of specific, individual owners to required action and activities. Such documented ownership of response and recovery actions will help the MSP organization reduce confusion and save time when the DR/BCP plan needs to go live during a response or recovery exercise. It is also vital that recovery procedures are periodically tested to realize any gaps within the program prior to a disruptive incident.

Details of the documented Disaster Recovery (DR) & Business Continuity Plan (BCP) being developed by the MSP organization should include the following aspects:

- Recovery priorities of critical business systems and services
- Acceptable recovery time frames:
- Recovery Point Objective (RPO) - the max interval of data loss since the last backup that the business can sustain (e.g., how many hours/days/weeks of work or data can the business afford to lose and still resume with minimal disruption?)
- Recovery Time Objective (RTO) - how long can IT processes and services be down before affecting the business (e.g., how many hours/days/weeks can the business survive an internet service outage?)
- Plans based upon a Business Impact Analysis (BIA)
- Roles and responsibilities of key team members
- Recovery strategy to alternate worksites or remote workforce / work from home
- Allow for both temporary operating measures and the full recovery / resumption of normal business operations

For the MSP organization, he DR/DCP is part of an overall program designed and structured to respond to disruptive events, restore critical business functions, and resume normal business operations. As a result, the contents of the DR/BCP should focus on the worst-case scenario, recovery of the steady/current state operations, and defining the critical restoration/resumption steps. Since event-specific characteristics and operational impacts will drive the MSP management decision-making and actions, The DR/BCP does not need to prescribe a specific set of technical details for system recovery steps, as those specific details may be contained within another document that can be referenced within the DR/BCP. This allows the system owners and administrators to update their documentation without having to run through the full review process of the overarching DR/BCP and security program.

For ease of use, the DR/BCP can be broken down into a few primary, event-driven categories:

- **Pre-Disaster**
  Defines the advanced, pre-planning business continuity activities to be executed to minimize and reduce risk to the organization.
- **Disaster Response**
  Defines the post-disaster chain of events and business continuity activities required to respond to an event, as well as the more detailed steps need to restore and resume operational business function.
- **Restore Operations**
  Defines the detailed actions that need to be taken in order to stabilize critical business operations (survival-mode) and restore the business operations in the order of their criticality.
- **Resume Operations**
  Defines the chain of events, critical tasks and detailed steps that need to be taken to resume business function processes back to normal given appropriate resources, including alternate site locations.
- **Evaluate DR/BCP Performance**
  Assesses and measures the recovery efforts of the business in meeting DR/BCP objectives and performs a review of lessons learned to incorporate into future recovery efforts.

As part of each category, it would be wise for the MSP organization to document and include a high-level process diagram as well as a critical task checklist of supporting action items with steps and/or details that need to be performed. For the MSP, it will be a good practice to develop separate checklists – one to address internal business operations and one to address services provided to customers.

For more information on DR/BCP development, please visit the following resources:

- Department of Homeland Security: Ready Business - Business Continuity Plan
  https://www.ready.gov/business-continuity-plan

- National Fire Protection Association (NFPA) 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs
https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600
- DRI International - Professional Practices for Business Continuity Professionals
https://www.drii.org/certification/professionalprac.php
- Federal Emergency Management Agency (FEMA), CGC 1 - Continuity Guidance for Non-Federal Entities
https://www.ready.gov/sites/default/files/2020-03/continuity_guidance_circular.pdf
- Institute for Business & Home Safety - Open for Business® Toolkit
https://disastersafety.org/business-protection/ofb-ez/

Safeguard Measures

Efforts underway to ensure measures are in place to safeguard vital resources, facilities, and data as part of DR/BCP management program.

Backups serve as the core component to most every recovery effort. As a good practice, the MSP organization should have plenty of redundant backup processes and storage procedures in place (e.g., 3-2-1 backups). If any physical or digital records need to be physically transferred to a new work location, proper care due diligence must be taken to preserve their integrity and security during transport or shipping.

Additionally, the restoration of physical or digital files, forms and supplies from a primary site to a recovery site will need to be handled with similar care and due diligence to preserve their integrity and security. Such handling and restoration should only be conducted by authorized individuals who are familiar with the data and properly trained to perform restoration and recovery actions.

As a good practice, digital data backups may be stored offsite and in multiple locations for recover, However, physical data can be destroyed if not immediately moved from the afflicted building or office location. Such physical data may include any mail or packages (received or unopened), paper files stored in desks and with file cabinets, external hard drives/USB drives, and any potential work that may be in progress. If needed, the DR/BCP should consider such items and include the necessary storage and transport procedures where necessary.

Access Measures

Efforts underway to ensure availability and access to vital resources, facilities, and data as part of DR/BCP management program.

Access to technology, digital communications and network resources are required for the productivity and quality of business operations and the management of customer support and services provided by the MSP organization. As such, each workstation, laptop, server, service, and business resource (fax machines, printers, copiers, scanners, cash registers, etc.) may be needed while working through a crisis or emergency that involves the evacuation and/or relocation of IT resources and workforce personnel. The ability for an MSP organization to run both office productivity and enterprise software is critical to ongoing business operations and the support of customers. Therefore, the DR/BCP requires specific recovery strategies for the information technology solutions used by the organization. Recovery plans should be developed so access to technology can be restored in time to meet the needs of the business and maintain customer services levels. Where possible, manual workarounds and supplemental resources may be identified and be included as part of the IT recovery plan so business can continue while access to computer systems are being restored.

Workforce Personnel

Workforce personnel identified for roles and responsibilities required to implement DR/BCP management program.

More often than not, it is poor communications, lack of leadership, and lack of board oversight that 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 DR/BCP and incident response programs should elevate the importance across the entire MSP organization.

By properly organizing DR/BCP roles so that key team members and supporting workforce personnel will not be unnecessary overwhelmed by the multiple activities that require their ongoing attention to details. Having identified and documented the key stakeholders and what key roles within the MSP organization are involved in a response and recovery effort or addressing a security incident is vital to ensure ongoing business operations. The responsible stakeholders and roles may change depending on the type of incident and the resources of the organization.

Stakeholders likely include department managers, senior management, key workforce personnel, partners, customers, and legal. With the involvement of diverse responsibilities, roles, and individual personalities, additional business politics, resistance, negotiation, and ignorance may blend into the overall response and recover actions. Therefore, have an established management plan with defined roles assigned to key individual, will provide a strong pathway for the business to recover.

Having a fully functioning DR/BCP management program may involve the following roles from within an MSP organization:

- **Human Resources Leader**
  Responsible for all activities related to people affected by the event (workforce, visitors, contractors, and other people). The HR Leader and their team should prepare for the evacuation of workforce personnel, organize the delivery of first aid to the injured, and

establish and maintain contact with emergency services and the families of workforce personnel.

- **Business Leader**
  Responsible for all activities that involve coordination with external third-party infrastructure and services. Ensures products and services are resumed, and serves as the primary contact with those responsible for the recovery of internal services and infrastructure.
- **Infrastructure Leader**
  Responsible for activities related to internal infrastructure recovery. Depending upon the size of the MSP organization, this leadership role may be subdivided to address multiple teams with a designated leadership role in place for each service or department within the business.
- **Communications Leader**
  Team member who is the primary (if not the only) point of contact with the media and any public entity. Having a single point of contact for outside communications will help avoid any misunderstandings due to the release of conflicting messages.

Backup and Restore

The MSP organization has implemented advanced 3-2-1 backup solutions for critical systems and data and has successfully performed recovery testing.

As discussed in the IT Nation SECURE Fundamentals (Yellow Book) and within the Security procedures allow for the advanced management of backup and recovery protection capabilities across the MSP organization. In short, the 3-2-1 backup model indicates that the MSP organization must maintain three (3) copies of the data stored on two (2) different types of media with one (1) copy stored offline.

Consider the following best practice requirements for managing and conducting backups across the MSP 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 / good).
- 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 a chance to recover at later date.

Third-Party / Vendor Risk Program

Vendor management describes many different activities, including researching and sourcing vendors, obtaining quotes, researching capabilities, quality of work issues, negotiating contracts, turnaround times, managing relationships, evaluating performance, and ensuring payments are made. In short, working with vendors and partners requires a lot of varied skills, resources, and time.

Following are some key points to consider when focusing upon the details involved when assessing the risk management of vendors.

Involvement of Business

The MSP organization conducts third-party / vendor risk assessments as part of standard business practices.

The third-party / vendor governance and organizational structure questions, along with the security controls and technology questions laid out in the IT Nation SECURE MSP+ Fundamentals Playbook (Yellow Book), provide a good starting point for an MSP organization to implement a Third-party / Vendor Risk Program. The skills resources and time spent on vendor management at this point can be a strain on time and workforce resources. This is a best practice that needs to be established, and many MSP organizations are now starting to realize how this effort makes their business more secure. It is most likely a shared responsibility between senior leaders in sales, finance, and security.

Vendor Assessment Methodology

The MSP organization employs a standard vendor risk management questionnaire designed to help identify potential weaknesses among third-party vendors and partners.

As a business, the MSP organization may be asking all the right questions but may need help in knowing and understating all the right answers. It is time to begin to establish a standard that third-party vendors will need to meet in order to engage in a secure business relationship. Developing a methodology and a routine process for assessing business partners and vendors, and defining levels of acceptable risk, will allow business operations to t build a repeatable standard that can be used to measure and monitor the vendor provided services and software.

Review Criteria

The MSP organization has established a vendor risk management decision process based upon criteria from best practices in security and risk governance, technology and business operations.

Focusing on governance and controls around security and technology, can provide a good picture of how a third-party vendor meets acceptable level of risk as defined by the MSP organization. As the business continues to build on its program, the acceptable level of risk should be less tolerable. As the MSP organization begins to expand a collection of security reviews of vendors and partners, the more knowledge the MSP business will become in identifying the levels of risk to business operations and services. As the MSP organization matures in its security practices, the vendors and partners engaged should also grow and mature their security capabilities. The more that is known about a vendor and the risk they bring to the MSP organization, the more one should expect from them regarding their security practices. Ideally, a vendor’s security posture and practice should exceed your expectations of them and their products and/or services.

Oversight of Vendor Risks and Assessments

The MSP organization is making efforts to consolidate the processing of third-party / vendor risk assessments into a unified program.

It is possible that as the MSP organization builds out its third-party vendor management program that there will be some duplication of business efforts in evaluation. Depending upon the product or service the business is looking to purchase, the vendor assessment process might begin from within different departments of the organization. For example, the finance team might be evaluating a new payroll product and performing their due diligence and assessment on the third-party company. The finance team completes their assessment of the product, negotiates pricing, and wants to move forward with a pilot. The finance team then requests the IT team to create a secure connection in order to allow access the software during the pilot. Since this will likely be the first time that the IT team hears of the project, they may also require their own security assessment of the product and the third-party vendor before allowing and connection for the pilot.

As the MSP organization matures its third-party / vendor management program, the business teams across the company will become more in sync with each other in organizing the process of third-party vendor security assessment and overall vendor management. Such initiatives take time and resources but may ultimately require a dynamic leader to take ownership and champion the program and processes needed to mature the program.

Incident Management Program

The objective of an incident management program is to adequately respond to electronic incidents that take place within the organization's purview. An incident response plan is communicated and provides workforce personnel with the knowledge and training to identify and deal with a security incident. The security incident may be at the same time a business catastrophe, as addressed by the business continuity plan. However, a security event, might be less catastrophic than a fire or meteor strike, but a breach of security, such as a hacker attack or a case of internal fraud can also greatly impact the business. An incident could be a single event, a series of events, or an ongoing problem.

A plan usually has several phases that include planning, triage, and running the incident. Additionally, it is best practice to add a process phase to perform a review that is conducted after the situation is under control and abated. The review process of the incident can lead to improvement in how the business responds to similar events in the future.

Capabilities for Incident Management

The MSP organization develops, documents, and communicates an incident response policy with standards and procedures that addresses coordination among business lines and regulatory compliance.

Definitions

Standards need to be developed to define exactly what an incident is. The answer is contingent upon your organization's goals and priorities. A good place to start is by understanding your organization's current policies, the International Standards Organization (ISO) accreditation, and applicable legislation, regulations, guidance, and generally accepted best practices.

Another item that requires definition is the role of the computer emergency response team (CERT). The CERT should be built internally using your most skilled and highest available members. Members of the team will need to represent expertise within the various information systems belonging to an organization, be on call 24 hours a day, and be capable of responding within a nominal amount of time. There should also be a backup available for when members are out of town or on vacation (succession planning).

The IT nation SECURE Team has provided a sample incident response checklist used by the ConnectWise SOC for MSP's in **Appendix C: Sample Incident Response Checklist** at the end of this document. The checklist will prove to be a great resource to start with as you build out your program.

Incident Classification

To be effective in managing the incident response process, your organization should create an event classification system. This system will be used to filter out the background noise from the serious problems that come up. An effective approach to this is to assign events a degree of urgency and then give the highly urgency issues a priority ranking. Incidents categorized as low and medium urgency classes may just be logged; however, medium events may be examined later by a system administrator. High urgency events should expect immediate triage and investigation. In some cases, the response activities may require the attention of other relevant departments and groups within the organization.

An escalation list with designated roles and responsibilities should be used for all incidents. Actions may need to be escalated and communicated as the degree of urgency increases as the incident progresses. As an event increases in urgency and priority, an appropriate individuals and leadership further up the escalation list is contacted. Ultimately, incidents of the highest urgency and priority may involve the activation of a designated computer emergency response team (CERT) or managed by a well-trained security operation center (SOC).

As an incident escalates, it is likely that other business departments other than security administration will need to become involved. Executive management will need to understand their role and act carefully to not hamper the ability of the CERT or SOC to properly respond and perform its job, e.g., by assigning unreasonable or time-consuming activities. Human resources, legal, and public relations personnel may also need to be involved. Finally, the situation produces evidence that shows possible criminal activity was involved, executive leadership should be prepared to contact law enforcement.

Make sure to include any third-party vendors or partners on the escalation list. Relevant vendors who provide services to your MSP organization should provide a 24-hour on-call contact or have a staffed helpdesk with personnel familiar with the services provided to your business. It is also recommended that some type of information security and/or service level agreement be included in any contract between your MSP organization and the third-party vendor or partner.

Reporting

Before, during, and after a cyber incident, various kinds of data will be collected. In addition to typical intrusion detection and server audit log files, when an incident is being managed a significant amount of data (e.g., collected evidence, additional log data and documentation of the incident) will be generated. After the incident has passed, new information may be calculated relating to what the incident may have cost the organization, as well as what resources may need to be recovered or replaced. It is important for the incident response policy and standards list the type of reports that will need to be generated. It will also be helpful to outline what the incident reports will contain, and to whom the incident reports will be made available.

A well-written investigative incident response report tells a story in which one must answer various questions such as who, when, where, why, and how. While one is answering these questions, any supporting materials such as figures, tables, data, and equations that may be required to help the incident timeline and events unfold in an effective, easy to follow narrative that can be easily understood and readily communicated.

The supporting material for an incident report can be referred to directly from within the text and integrated in the writing format to identify and clarify its impact. It is a good practice to number any figures and tables in the same order as they are introduced within the incident report. For example, tables can be numbered as Table 1, Table 2, Table 3, etc. Similarly, figures can be labeled as Figure 1, Figure 2, Figure 3, etc. As with any technical writing, numbering the materials helps to avoid confusion and makes the narrative easier to understand what transpired and actions taken during investigation of the incident. For the incident report, it may be more practical to reduce narration and to emphasize important facts by placing larger tables, schedules, figures and images to the rear of the report in appendices.

Executive / Board / Owner Oversight

Executive leadership provides effective ownership and oversight of an incident response program within the MSP organization.

IT leads an incident response team with strong executive support & inter-departmental participation. When it comes to cybersecurity incident response, IT should be leading the incident response effort, with executive representation from each major business unit, especially when it comes to Legal and HR. Please refer to the Fundamentals geode (Yellow Book) for more information about setting up your incident management program.

Defined Roles and Responsibilities

The MSP organization has defined roles and responsibilities for an incident response program.

Typically, incident response is managed by a group of people who together comprise an "Incident Response Team," of which the Chief Information Security Officer may be a member or the leader. In some organizations, the leader of the team is afforded the title "Information Security Incident Response Coordinator," "Information-Security Incident Response Leader," or something of the sort. This title is, of course, in addition to any other titles the leader may have as part of his to her job. For the MSP organization to properly staff a security incident management program, consider the following roles and responsibilities:

- **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 life-cycle

- **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 ISPs, SaaS providers, cloud service providers, hosting providers, 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

Consult the IT Nation SECURE Fundamentals Playbook (Yellow Book) for additional information to help establish an incident response program.

Incident Response Training

The MSP organization provides specialized training to workforce personnel responsible for incident response and recovery.

Internal incident response training must be linked to the assigned roles and responsibilities of your workforce personnel, CERT team, or SOC to ensure that real-world content is covered with a level of detail to make sure that skills are maintained across business operations and services. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

At a minimum:

- Regular users may only need training to know who to call or how to recognize an incident.
- System administrators may require more advanced training on how to handle and remediate incidents.
- Incident responders may receive more specific training for the specialized skills needed for threat hunting, digital forensics, reporting, system recovery, and restoration.

At a minimum, the MSP 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

Communication Plan

The MSP organization has a communications plan as part of an incident response program.

Communications within the organization and to all impacted external parties are key to a successful incident response program. It is important to ensure that you have properly thought out a communications plan so that the right people will be involved when an incident occurs.

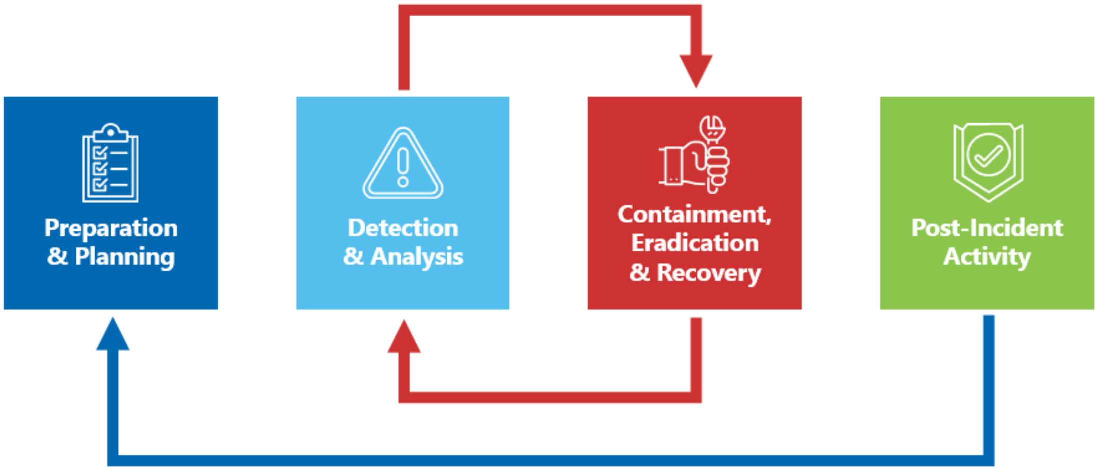
Consult the IT Nation SECURE Fundamentals Playbook (Yellow Book) for additional information to help establish an incident response program.

Incident Response Life-Cycle

The MSP organization has an incident response program with a life-cycle of preparation, detection, analysis, post-incident activity and reporting.

Having a flexible incident response program with documented and well-practiced plans should allow the MSP organization to address most any suspected cyber incident throughout a logical series of life-cycle phases.

The IT Nation SECURE Fundamentals Playbook (Yellow Book) clearly outlines the Incident Response Life-Cycle, according to NIST. Please use the Yellow Book as a reference.



Incident Response Lifecycle (NIST)

To meet the minimum requirements this lifecycle, the incident response plan needs to be formally documented in policies and standards to include preparation, detection, analysis, containment, eradication, recovery, and post-incident activities. All of these activities must be documented and tracked for reports and audits.

Security Architecture

Introduced within the IT Nation SECURE Fundamentals (Yellow Book), 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 for an MSP organization not only considers security risks and mitigations, but also includes the blending of people, process, and technology.

Beyond the fundamentals, an MSP organization must have made advanced efforts in order to mature their security architecture and have developed the following aspects:

- Basic understanding of best practice with several objectives, strategy and tools in place.
- Security architecture is defined at critical layers and is reasonably effective.
- Security architecture is defined and a need for monitoring and measurement has been identified but may yet be fully realized across all business operations.

Reference Architecture

The MSP organization has adopted risk-based policy and standards approach in delivering security architecture and controls that align with business requirements and objectives.

In the IT Nation SECURE MSP+ Fundamentals Playbook (Yellow Book), the concept and principles of Zero Trust were introduced. 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.

Zero Trust

Within the concept of Zero Trust, there is no ”one-size-fits-all” approach to security as each control and design element feeds into an overall security architecture based upon business operational needs as well as the and the specific needs of the MSP customers. In short, a Zero Trust architecture is guided by 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.

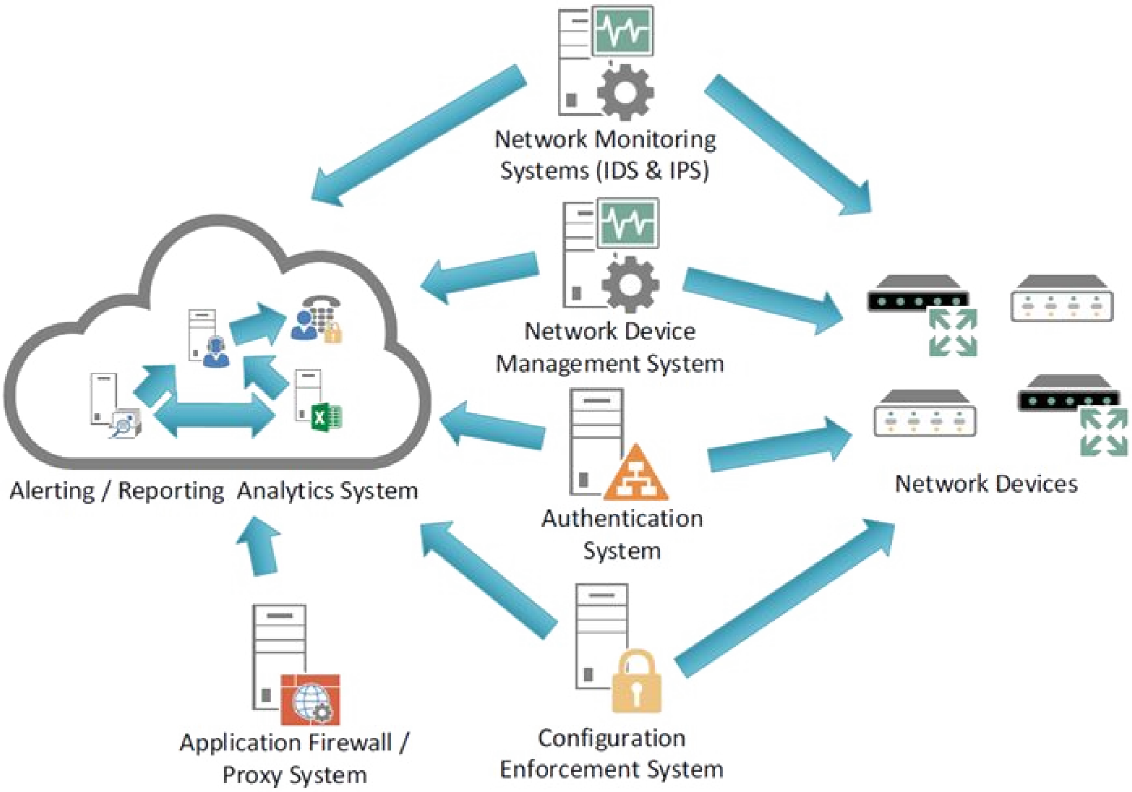
- **Authenticate and Authorize Prior to Access**
  Systems and services, both internal and external to your organization, may be available for access directly over the internet, so the authentication of user requests requires a much stronger mechanism as opposed to the use of a simple username and password 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

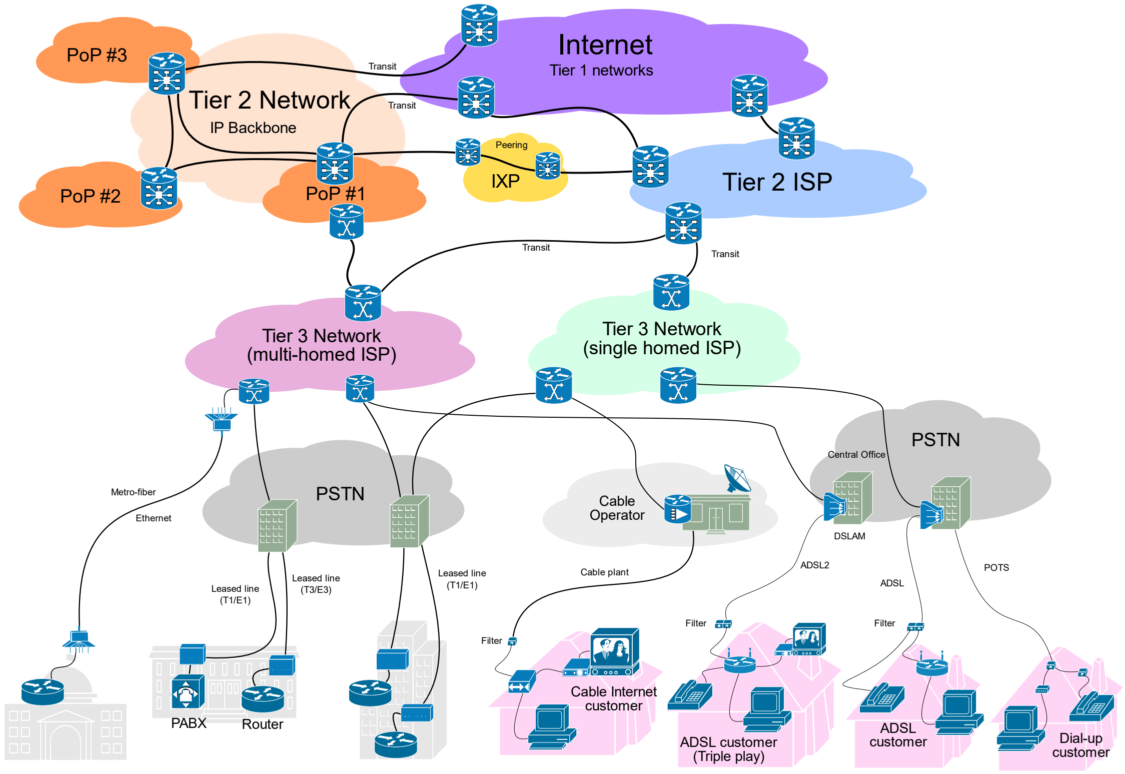
identify rogue devices and malicious activity. The collected data and analytics can serve to help you improve security policy creation and enforcement.

Certain types of data fall under different classifications and have data privacy requirements that relegate control and use of such data (e.g. HIPAA, GDPR, PCI, etc.). In addition to understanding what data needs to be protected, an MSP organization must also to understand and document how and where data is being protected. Such documentation should be developed the represents a visual presentation of the protective safeguards and controls that have been implemented as part of the MSP's security architecture. Producing a network diagram as a visual representation of network architecture will allow the business to make design concepts easier for users to understand how IT assets and data flows are related and connected. The following network boundary diagram serves as an example.


Network Monitoring Systems (IDS & IPS)
Network Device Management System
Alerting / Reporting Analytics System
Authentication System
Network Devices
Application Firewall / Proxy System
Configuration Enforcement System

Network Boundary of DMZ with High-Level Data Flow

Additionally, following is a sample of a physical network topology diagram that shows multiple networks connected via the internet. From this diagram, it would be easy to document what ports, protocols and types of data are used as part of business operations.



Sample Diagram of Physical Network Topology

Image By User:Ludovic.ferre - Internet_ConnectivityOverview.svg, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=10029345

The adoption of security architecture policy and standards framework and strategy will require the assigning of roles and responsibilities, creating organizational structure, and defining measurements, the involvement top-level management (e.g., the board of directors, owners, or executive leadership) must be required in order to drive the culture and change across the MSP organization. Management must be seen to actively support security initiatives and drive enterprise architecture standards across the entire MSP busines operations and services provided to customers.

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

Product Security

The MSP organization has adopted a software development life cycle (SDLC) that is aligned with security requirements and objectives.

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 the MSP 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 an adopted SDLC in alignment with security policies, standards, and practices allows the business to produce more security solutions and services, both internal and external to the organization.

The MSP must confirm that that workforce personnel understand 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. The use of documentation, formalized training courses and hands-on experience are multiple ways the organization can help foster the growth and maturity of product development and service offerings.

Product Compliance

The MSP organization must follow a well-defined purchasing practice based upon security policies and standards designed to meet business needs.

The purchase of new systems, hardware, or services must be made in accordance with established policies as well as technical standards. Purchase request should be based upon requirements documentation and consider the long-term strategy and roadmap of business requirements and initiatives.

Any significant purchases (products or services) should be evaluated through a structured process for authorization and approval that includes the development of a detailed Request for Proposal (RFP) document and vendor questionnaire that identifies any necessary security controls and feature requirements.

It is a good practice for new hardware installations, or the onboarding new services are formally planned and communicated to key stakeholders and impacted parties ahead of the proposed date of implementation or cut over. Additionally, the operational and security requirements will need to be shared for comment from key stakeholders and interested parties, well in advance of installation.

Purchased products or services must undergo comprehensive testing and assessment against elements within the RFP and will need to be formally accepted by key stakeholders and users prior to adoption as a production system or service that supports critical business functions.

People and Process

The MSP organization has defined roles and responsibilities for the onboarding and development of cybersecurity professionals.

A healthy security architecture is built on three pillars—people, processes, and technology. Since technology and process elements have been addressed within the above sections, the multiple roles of people and their responsibilities throughout the MSP organization will need to be identified.

Workforce Personnel

To support the MSP organization business and service offerings, specific security roles and responsibilities will need to be defined. These roles can be used in accordance with user rights, and privileges, and account groups for controlling access to systems and data. Within the MSP organization, consider the following roles and the level of access each requires in order to perform their job 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-Party Service Providers

Cybersecurity Professionals

In addition to the above, the MSP organization must consider designated roles and responsibilities for cybersecurity professionals, engineers, and analysts to be in line with existing security initiatives and business strategy. These roles may be developed from existing internal workforce personnel or be hired from outside. No matter the case, the job function of the cybersecurity professionals within the organization should be clearly defined with duties and responsibilities and any desired skills knowledge or abilities.

There are hundreds of job descriptions that can be located on the internet, but is would server the MSP organization well if the cyber security role were specifically tailored to the immediate business needs and strategy. If the organization is able to hire or develop the right people with a positive attitude, the relevant experience, the necessary job qualifications and equip them with the specific operational and cybersecurity training needed to be successful, the security culture of the MSP organization will mature and be better able to meet emerging threats and risks to the business.

The operational risks posed by workforce personnel and human error will always remain one of the greatest threats to cybersecurity and protected data. However, having an experienced workforce knowledgeable about business operations and vested in the culture of security across the organization can also be a great benefit. The users of are the first line of defense to protect against malicious cyberattacks and fraudulent activities that may impact security or compliance. Train them well and keep them happy.

Senior Leadership

When senior management and executives commit to developing a positive culture around cybersecurity and invest in training for the roles and responsibilities of workforce personnel, the alignment with process and technology will blend to better protect the organization. Having a top-down approach that drives the cybersecurity culture may allow the MSP organization to retain and rely upon those employees with the institutional knowledge and experience necessary to maintain the security of operations, services and data.

Security Awareness Training

The MSP organization must provide annual training to workforce personnel on a variety of security risks and safe computing practices specific to individual job roles.

Regular security awareness training can serve as the foundation to help create a strong culture of cybersecurity across the MSP organization. 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.

If the MSP organization has yet to implement this type of security and awareness training initiatives, now is the time to do so. There are many resources and vendors available to help develop a security awareness training program. Though they may be designed with onboarding in mind, the security and compliance training modules will also need to be a part of an annual curriculum offering to be completed by all workforce personnel in order to meet certain regulatory requirements. Required topics for security awareness, training, and education include:

- Phishing
- Social Engineering
- Mobile Devices
- Malware
- Browsing Safely
- Social Networks

- Passwords
- Data Security
- Insider threat
- Cloud Services
- Physical Security
- Working Remotely
- Encryption

Specific, customized cybersecurity and compliance training for certain roles must be developed and provided within the MSP organization, such courses and training are as follows:

- Specialized Training for Privileged Users and Administrators
- Specialized Training for Helpdesk
- Specialized Training for Engineers
- Specialized Training for Sales
- Specialized Training for Executive / Senior Leadership

The completion of security awareness training is documented and centrally collected in order to monitor and measure the effectiveness. Such data may include exam scores and well as results from phishing exercises. The MSP organization will use the results to create key performance indicators (KPIs) that will be used for the measure various aspects of the security awareness training program.

Identity and Access Management (IAM)

The MSP organization will maintain identity and access management policies and standards to avoid compromise of services and data.

The MSP organization will have a defined process for the onboarding, modification and change of users and service accounts through an identity and access management process. New user accounts and user IDs must be created based on a standard documented request approval process. Appropriateness of the requested access must be verified prior to granting access to new users or the modification of existing user accounts. By policy and practice, the use of generic and shared IDs should not be permitted.

Establishing the standard of creating accounts that are linked to individuals allows the MSP organization to enable granular access controls and create specific roles for each user (internal, customer, partner) from within a single directory. This practice will help the MSP organization:

- Adopt products and capabilities while minimizing the overall impact to the business and existing services
- Reduce the risk of malicious attackers or untrained personnel gaining unauthorized access and interfering with critical business operations and services
- allow for quick provisioning and de-provisioning of access to services and data
- Monitor and audit access requests and authorization security controls are functioning as intended
- Enhance the productivity and compliance of workforce personnel

SSO & MFA

Even today, usernames and passwords remain at the core of Identity and access management practices, however they no longer provide enough security to properly prevent account compromise or the exposure of sensitive data. As modern, evolving cyber threats become more complex, many organizations are adopting solutions surrounding single sign-on (SSO) and multi-factor authentication (MFA). These solutions can strengthen the cybersecurity posture of the business without hindering the overall user experience.

Single-Sign On (SSO) is a login and authentication method in which users have a single set of credentials (user ID & password) to access multiple applications. Enabling an SSO is the one of the approaches to allow users access to multiple services or devices without having to enter in a separate set of credentials. For the end user, there are not as many passwords to manage which enhances the overall user experience. For systems administration, an SSO solution make it easier to manage user accounts and monitor their access across multiple platforms and services. It is this ease of use that allows for all encompassing access through a single-entry point that many cyber attackers love to find to take advantage. It is the very reason that SSO should be deployed with MFA.

Multi-factor authentication (MFA) solutions are implemented in order to require users to enter two or more identification elements in order to gain access a service or application. These data elements of information are designed to be unique to the individual user and extremely difficult for an imposter top attacker to guess or emulate. With an MFA solution in place, it becomes more difficult for malicious threat actors gain access to critical systems and sensitive data. Modern MFA solutions will often make use of smartphones with soft token apps and SMS codes as part of the user authentication process. However, many vendors and security professionals will drop MFA credentials into three categories:

- Something You Know: passwords, security questions, and pin numbers
- Something You Have: device or object, like a smartphone, security badges, verification apps, or security tokens
- Something You Are: biometrics e.g., fingerprints, facial and voice recognition

Auditing and Compliance

With the unification of Identity and access management capabilities integrated with SSO and MFA, the MSP organization will have some degree of integration for auditing and compliance at the system level across the business. As such, the MSP organization must set audit policies for events to monitor across all workstations and servers. This may be accomplished by any myriad of means, but first, audit logs will need to be enabled and collecting the right events to monitor. Following are some useful guides from Microsoft to help with the configuration of audit events:

- Microsoft - Monitoring Active Directory for Signs of Compromise https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise
- Microsoft - Audit Policy Recommendations https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

Security Operations (SOC)

The MSP must establish as SOC as the centralized hub of its detection and response capabilities as part of an overall cybersecurity program.

Having a centralized business function staffed by security professionals as part of a Security Operations Center (SOC) with the 24/7/365 services to continuously watch the IT systems environment and rapidly respond to potential risks, ensures ongoing protection across the MSP organization. However, for the SOC team members to remain current with the most recent security insights and guidance available, they will require specialized training and the tools and resources necessary to monitor network traffic and receive alerts and to act when malicious activity or anomalous traffic is detected. Whether outsourced or staffed in house, SOC personnel should have training in the following:

- Ethical Hacking
- Cyber Forensics
- Reverse Engineering
- Malware Analysis
- Intrusion Prevention Systems

The SOC may employ the use of a SIEM and log management capabilities with other essential security tools as part of their service to provide centralized security monitoring of cloud, on-premises, and hybrid environments while assessing and defending everything from websites and databases to networks and endpoints searching for gaps in security controls.

The SOC should be working to simplify compliance management with correlation tools that all ow the organization to keep sensitive data aligned to regulations, policies, and obligations that are applicable to business operations. Additionally, the SOC must work with clearly defined, formal processes within their assigned responsibilities for monitoring and alerting as well as orchestrating incident response.

For mor information for best practices for establishing a Security Operations Center, refer to the following resources:

- AT&T Security - Benefits of a security operations center (SOC) https://cybersecurity.att.com/blogs/security-essentials/benefits-of-a-security-operations-center-soc
- SANS Institute - Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf
- SPLUNK - What Is a Security Operations Center (SOC)? https://www.splunk.com/en_us/data-insider/what-is-a-security-operations-center.html

Case Studies

Following are a few examples of cases from the field that highlight some of the good, bad and ugly examples of business disruption and a success story that may occur within an MSP organization in dealing with cyber security and compliance controls while dealing with people, processes and technology.

Case Study: Network Segmentation

Background

Flat networks are easy to manage for an organization, however that ease also makes a bad actor's job easy as well. They are able to freely discover and move around the organizational network the same as your team. Network segmentation reduces the attack surface making it more difficult for the bad actors to move laterally within your environment, and that is a good thing. In the example that follows, you will see why segmentation is so important not only to prevent the lateral movement, but also to lower the exposure risk of key areas that might be in your business, like a workbench or your remote monitoring and management (RMM) tool. In addition, you will find network segmentation will bring you one step closer to a "zero trust" configuration discussed in the Security Architecture section to again help lower your risk impact in the event of a security incident.

Tackling Technical Debt

If you are like most service providers, you have been running around taking care of your clients and not focusing your own housekeeping, opting to put it off for billable work. That decision has led to a lot of clean up within your own technology stack and now is the time to address it. Firewall policies have gotten out of control, subnets might actually be one subnet with no differentiator of even a net mask and they probably lack context. Our sample MSP is in the same boat.

The MSP owner, lead tech, and a few other stakeholders sat down to review the environment and layout the systems, applications, IPs, ports, etc. within the business. The team's goal was to discover all of the devices, applications, and who needed access to what and what needed access to who.

The Importance of Network Discovery

During the discovery process, they uncovered the workbench area was still connected to the operational side of the business. Meaning, the technicians who were working on client computers, potentially infected with viruses, had the ability to reach out and "see" the production systems throughout the organization. In addition, they discovered their sensitive backend finance system could be accessed by the technicians. Thus, providing a potential risk to the business owner.

A Strategy to Solve the Problem with Network Segmentation

The team developed a strategy to logically and physically segment the network based on applications, users, content, and business function. Not only did they separate and isolate the departmental users, they also identified user types, placed users into groups, and then wrote specific security policies for their next-generation firewall platform to only allow traffic and communications to specific systems.

Think about Zero Trust
Do you trust every aspect of the company network and connected assets? Do you trust the users, devices, and applications? By applying proper security and access controls between these segments you can protect and trust your network security architecture and the services it provides. Adopting the practice of network segmentation provides a good starting point for the "Zero Trust" method which the MSP organization should consider moving towards as part of an overall security strategy.

The team also invested the time to segment out the remaining flat networks from their environment. The company had a corporate wireless network and a guest wireless network which were both on the same network subnet and only separated by a VLAN. However, both networks presented a security issue where they could each route to the other on the back end – resulting ins guests potentially accessing production systems and data. To correct the issue, they had to separate out those areas and create a specific set of network security policies for the users that requires the specific access to systems for their job role and required duties. In short, they created actual network segmentation and reduced the overall risk from their Wi-Fi networks.

Benefits of Network Segmentation
With the adoption of network segmentation, an MSP organization will place their business in a much better place to continue to expand services and implement new security technologies as they become available. In the case study, the business owner was very pleased to reduce the risk to an acceptable level that previously with exposure with the service workbench to his financial system, and through the guest wireless solution. The segmentation also afforded them to limit their NAT down to 120. Now, instead of having a largely reactionary security posture, the company improved their overall ability to be more proactive and grow in maturity from an cybersecurity and information security standpoint.

Network segmentation also helped the company reduce their compliance burden, generate effective insights from their reporting and analysis, improve their focus on threat hunting, and reduce their overall business risk.

Case Study: SOC Deployment & Business Integration

Following is a summary of an MSP organization that has specialized in the service of customers within the Healthcare industry.

Background

The MSP organization had made efforts to informally monitor security controls, alert on certain log events, performed ad hoc assessments and several incident response investigations. However, a SOC did not exist and the organization was struggling to mature their own capabilities and the security services provided to their customers.

Challenges

With their currently deployed tools and staffing, the MSP organization had a limited view into their environment which resulted in several undetected security incidents that could have potentially compromised the MSP organization as well as their downstream customers. Such issues could be financial, compliance related, or have a negative impact on their reputation.

Moving Forward

The MSP organization went on a talent search and onboarded several dynamic security professionals who had the qualification and experience necessary to help lead the initiative to design and deploy a SOC. The executive leadership at the MSP organization realized that an investment in establishing a strong foundation with the right people, standards-based process, and updated technology was necessary to propel the future growth and advanced service capability of the business.

- **People**
  With the new management and workforce personnel, the MSP organization set to work to define the governance oversight and standards-based operating model for the SOC. A mission charter with clearly defined with immediate opportunities for integration across existing IT security functions as well as integration plans across all other business units (e.g. HR, legal, IT compliance, risk management, incident response, and DR/BCP). Since people serve as the core asset of the SOC, clearly defined roles and responsibilities were established when staffing the SOC which easily allowed for the onboarding new staff and the integration of SOC operations across the different business units.
- **Processes**
  The MSP organization worked to develop and document SOC processes and procedures to formalize consistent practices and response actions. The SOC personnel worked with the different business units to create process documentation for the following:
  - Event Monitoring and Detection
  - Threat Monitoring
  - Vulnerability Management
  - Incident Response
  - Reporting and Risk tracking

  With the investment in time, talent and leadership, the newly established SOC was able to mature and standardize processes through practice and adjusting to meet the needs of the MSP organization and supported customers.

- **Technology**
  The SOC did not just magically appear overnight, the MSP organization has to work and develop a technology road map of products, services and personnel that would be required over the next few years in order to enhance the capabilities of their SOC. Technology platforms on the roadmap included the deployment and integration of the following solutions:
  - Firewall Log / Reporting Platform
  - Network Traffic Analysis (NTA)
  - Intrusion Detection / Prevention System (IDS/IPS)
  - Next-Generation Antivirus (NGAV)
  - Endpoint Detection and Response (EDR)
  - Security Information and Event Management (SIEM)
  - Vulnerability Management and Assessment

  Additional technology enhancements and upgrades were performed to allow the existing asset inventory management system to integrate into the new SOC functions. Having the IT asset inventory integrated with the SOC allowed the business to assess and mor accurately pinpoint incidents as well as the ability to identify security gaps that that may impact the business or services provided to customers more accurately.

Overall Benefits
By having a vison and focusing on the fundamentals, the MSP organization was able to effectively organize and deploy a SOC that delivered value to both the business and its customers. The SOC was able the help the MSP organization bring value by providing:

- Governance: consistency, accountability, and proper integration with relevant business
- Processes and Procedures: tested, efficient, repeatable outcomes
- Integration: technology platforms with information to support decisions and response

Case Study: Phishing Compromise and the HHS Wall of Shame

An insurance and financial services company had to report to HHS and notify over 100,000 people that their data had been breached. They are now on the Wall of Shame.

Background
In 2009, the U.S. Department of Health and Human Services (HHS) released a portal from the Office of Civil Rights (OCR) as part of the HITECH Act to publicly post breaches of unsecured protected health information. HIPAA requires covered entities to report any breach of over 500 individuals to HHS and the HHS secretary is required to post these breaches. Today, the companies reporting a breach can be searched on what many have named the “Wall of Shame”.

According to the *2020 State of Password and Authentication Security Behaviors Report* by Yubico and Ponemon Institute, 51% of IT Security respondents say their organizations have experienced a phishing attack, with another 12% stating their organizations experienced credential theft.

Why should I care?
I do not have protected health information in my systems.

You should care because while you may not have PHI you do have sensitive and confidential data and probably personably identifiable information (PII) in yours and/or your customer's systems. The circumstances surrounding the breach could happen to your company.

The Incident
In October, the company discovered that a hacker gained access to several employee's email accounts through various phishing attacks. A third-party forensics team was hired by the company to assist with the investigation. They determined that the initial successful attack happened four months earlier in June. The forensic team also found that additional email accounts were compromised during the four-month period of the attack. Upon discovery the company immediately secured the compromised accounts to prevent further remote access by the hacker. The investigation found the compromised member data included names, Social Security numbers, bank account numbers, insurance premium payment information, dates of birth, and addresses.

Addressing the Incident
So, what happened next and how did they fix the problem. They immediately reviewed their email security controls and updated them to better protect against phishing attacks. Additionally, two-factor authentication was implemented for email and other systems containing sensitive or confidential data. They also implemented additional training around phishing awareness which is repeated on an on-going basis.

Security leaders would tell you the best way to detect unauthorized access is through access management and network monitoring. They also recommend taking away risky decisions from email users within your company. As threats continue to become more sophisticated, shoring up email applications and user authentication will be critical.

Conclusions
Even though you may not end of on the "Wall of Shame", the lesson here is the same. Phishing attacks are becoming more and more sophisticated and securing your systems using multi-factor authentication should be a priority for your company. Add in network monitoring and access management and you put yourself further down the path towards preventing a data breach and having to report it to law enforcement and your customers.

Additional Reading

- U.S. Department of Health and Human Services (HHS) - Office for Civil Rights (OCR), Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health

Information
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

- Yubico – The 2020 State of Password and Authentication Security Report
  https://www.yubico.com/authentication-report-2020/

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.

As described within the following sections, 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 IT Nation SECURE MSP+ Fundamentals Playbook (Yellow 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
- 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

Additionally, The MSP vendor community has many free webcasts and resources found on their websites, newsletters, etc.

Next Steps
Once the MSP+ Cybersecurity Framework Fundamentals are understood and beginning to be adopted, 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.

ConnectWise Certify for Engineers

For an MSP organization to qualify for the IT Nation SECURE MSP+ Certification:

- **Technical staff must have completed the ConnectWise Certify Fundamentals for Engineers with a 100% pass rate.**
- **All new hires will complete Fundamentals training within 90 days.**
- **Technical staff must have completed the ConnectWise Certify Advanced for Engineers with a 50% pass rate or greater.**

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:

- Secure onboarding processes
- 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.

Fundamental Learning Objectives: **ConnectWise Certify for Engineers**

- **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 10**1 – 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 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.
- **Security 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.

Next Steps for Engineers

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

ConnectWise Certify for Sales

For an MSP organization to qualify for the IT Nation SECURE MSP+ Certification:

- **Sales personnel must have completed the ConnectWise Certify Fundamentals for Sales with a 100% pass rate or greater.**
- **All new hires will complete Fundamental training within 90 days.**
- **Sales personnel must have completed the ConnectWise Certify Advanced for Sales with a 50% pass rate or greater.**

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.

Fundamental Learning Objectives: ConnectWise certify for Sales

- **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.

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 are as follows:

- **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

MSP+ Certification

The MSP+ Certification Program has two parts; MSP+ Certification and MSP+ Accredited Partner. The differences between the two will be noted within their respective paragraphs below.

MSP+ Fundamentals (Yellow Book)

While there is no certification here, this is the foundational elements required for the MSP to move into the Advanced book and ultimately obtain the MSP+ Certification through self-attestation.

SECURE MSP+ Certification - Advanced (Green Book)

For an organization to achieve this level of certification they must have completed all of the items within the Fundamentals book and the bolded items in the Advanced book (this book) along with the Education requirements:

- 100% pass rate for all technicians and sales staff of Certify Fundamentals
- 50% pass rate for technicians and sales of Certify Advanced

The organization will send an email to ITN_SECURE_CERT@connectwise.com requesting the MSP+ Certification. The IT Nation SECURE team will then assign the certification assessment plan in ConnectWise Identify. The team will then respond to the ticket generated from your email to share your login instructions and the required information to complete the assessment. Once the organization completes the assessment, the IT Nation SECURE team will perform a review and spot check the requested evidence. If anything needs to be addressed, the IT Nation SECURE team will again reply to the ticket requesting the items be resolved. Upon a successful review, your organization will be awarded the MSP+ Certification logo. This certification will be valid for a period of one year from date of issue. The organization will be required to maintain this certification through a renewal process, if they so choose. The organization will also have the opportunity to advance their certification to that of the MSP+ Accredited Partner. Additional benefits will be made available to Partners who have successfully completed all of the requirements and received the logo.

MSP+ Accredited Partner - Master (Blue Book)

This is the pinnacle certification for managed services partners. This certification will involve the partner completing all of the requirements within the Master book along with the Educational requirements for the Master level.

The process will be the same as the MSP+ Certification (Advanced), except a thorough review of all the required evidence will be performed by the IT Nation Secure team. Upon a successful review, the organization will be awarded the MSP+ Accredited Partner logo. This certification will be valid for a period of one year from date of issue. The organization will be required to maintain this certification through a renewal process if they so choose. Additional benefits will be made available to Partners who have successfully completed all of the requirements and received the logo.

FAQs of the 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.

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.

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.

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.

What is a Governance 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.

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.

What is a governance 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.

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.

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.

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.

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.

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.

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.

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.

Appendix A: Informative References

Apple. Secure Device Management Overview
https://support.apple.com/guide/security/secure-device-management-overview-sec38eb8731b/web

Apple. Use FileVault to Encrypt the Startup Disk on Your Mac
https://support.apple.com/en-us/HT204837

AT&T Security. Benefits of a security operations center (SOC)
https://cybersecurity.att.com/blogs/security-essentials/benefits-of-a-security-operations-center-soc

Australian Cyber Security Center (ACSC). Hardening Microsoft Windows 10 Workstations (v.1909)
https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-1909-workstations

Cisco. What is Extended Detection and Response (XDR)?
https://www.cisco.com/c/en/us/products/security/what-is-xdr.html#~types-of-response

ConnectWise University. Information Security Policies
https://docs.connectwise.com/ConnectWise_Business_Knowledge/Information_Security_Policies.

Dark Reading. Why Threat Hunting with XDR Matters
https://www.darkreading.com/cloud/why-threat-hunting-with-xdr-matters/a/d-id/1337441

Department of Health and Human Services (HHS) - Office for Civil Rights (OCR). Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Department of Homeland Security (DHS): Ready Business. Business Continuity Plan
https://www.ready.gov/business-continuity-plan

DRI International. Professional Practices for Business Continuity Professionals
https://www.drii.org/certification/professionalprac.php

Federal Emergency Management Agency (FEMA), CGC-1. Continuity Guidance for Non-Federal Entities
https://www.ready.gov/sites/default/files/2020-03/continuity_guidance_circular.pdf

Institute for Business & Home Safety. Open for Business® Toolkit
https://disastersafety.org/business-protection/ofb-ez/

ISAO Standards Organization
https://www.isao.org/

Microsoft. Advanced Security Audit Policy Settings
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings

Microsoft, Audit Policy Recommendations
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

Microsoft. Auditing Security Events
https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/auditing-security-events

Microsoft. Group Policy Settings Reference Guide for Windows 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. Microsoft Security Baselines
https://techcommunity.microsoft.com/t5/microsoft-security-baselines/bg-p/Microsoft-Security-Baselines

Microsoft. Monitoring Active Directory for Signs of Compromise
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise

Microsoft. Preparing Your Organization for BitLocker: Planning and Policies:
https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/prepare-your-organization-for-bitlocker-planning-and-policies

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

Mintz Matrix. State Data Security Breach Notification Laws
https://www.mintz.com/mintz-matrix

National Cyber Security Centre (UK). Cyber Essentials
https://www.ncsc.gov.uk/cyberessentials/overview

National Fire Protection Association (NFPA) 1600. Standard on Disaster/Emergency Management and Business Continuity Programs
https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600

Netwrix Blog. Four Tips for Building a Strong Security Culture in Your Organization
https://blog.netwrix.com/2018/06/28/four-tips-for-building-a-strong-security-culture-in-your-organization/

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 800-171 Rev.2. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Palo Alto Networks. Cortex XDR: Welcome to the Future of EDR
https://www.paloaltonetworks.com/cortex/cortex-xdr

SANS Institute. Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey
https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf

SANS Institute. Physical Security and Why It is Important
https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120

SPLUNK. What Is a Security Operations Center (SOC)?
https://www.splunk.com/en_us/data-insider/what-is-a-security-operations-center.html

Tech Beacon. 6 ways to develop a security culture from top to bottom
https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom

Trend Micro. What is XDR?
https://www.trendmicro.com/en_us/what-is/xdr.html

Total Security Advisor. 5 Physical Security Controls Your Business Needs
https://totalsecurityadvisor.blr.com/facility-security/5-physical-security-controls-your-business-needs/

Yubico. The 2020 State of Password and Authentication Security Report
https://www.yubico.com/authentication-report-2020/

Appendix B: Security Alert & Advisory Resources

Vulnerability Alerts & Advisories

- Computer Emergency Readiness Team Coordination Center (CERT/CC)
  https://www.kb.cert.org/vuls/
  The CERT/CC Vulnerability Notes Database is run by the CERT Division, which is part of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. The Vulnerability Notes Database provides information about software vulnerabilities. Vulnerability notes include summaries, technical details, remediation information, and lists of affected vendors.

- NIST National Vulnerability Database (NVD)
  https://nvd.nist.gov/
  The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

- CVE Details
  https://www.cvedetails.com/vulnerability-feeds-form.php
  CVE Details provides an easy to use web interface to CVE vulnerability data. One can browse for vendors, products and versions and view CVE entries, vulnerabilities, related to them. Once can also view statistics about vendors, products and versions of products. CVE vulnerability data are taken from National Vulnerability Database (NVD) xml feeds provided by National Institute of Standards and Technology (NIST).

- US-CERT National Cyber Awareness System
  https://www.us-cert.gov/ncas
  US-CERT is housed under the Department of Homeland Security. Its mission is to provide cybersecurity leadership. Your institution can sign up for US-CERT alerts, bulletins, and tips. Using US-CERT resources ensures that one will have access to up-to-date cybersecurity topics and threats. A subscription to any of the National Cyber Awareness System products ensures access to timely information about security topics and threats.

- Federal Financial Institutions Examination Council (FFIEC)
  https://www.fsisac.com/
  The Federal Financial Institutions Examination Council (FFIEC) recommends all financial institutions take part in the FS-ISAC. Per Presidential Directive 63, public and private sectors are required to share information about physical and cybersecurity threats. Institutions should keep well informed about emerging threats and share information. FS-ISAC provides access to Cyber and Physical Security Alerts, as well as other services,

from many sources. Sources include the government, private vendors, and cross-sector members.

- Multi-State Information Sharing & Analysis Center (MS-ISAC)
  https://www.cisecurity.org/ms-isac/
  The Multi-State Information Sharing & Analysis Center (MS-ISAC) is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. MS-ISAC provides real-time network monitoring, early cyber threat warnings, and other advisories. Institutions are advised to access the advisories and cyber threat alert levels reported by MS-ISAC.

- Industrial Control Systems CERT (ICS-CERT)
  https://ics-cert.us-cert.gov/advisories
  IES-CERT advisories provide timely information about current security issues, vulnerabilities, and exploits that impact industry control systems.
  Also, ICS-CERT offers Alerts by Vendor: https://www.us-cert.gov/ics/alerts-by-vendor?page=0

- Full Disclosure at Seclists.org
  https://seclists.org/fulldisclosure/
  A public, vendor-neutral forum for detailed discussion of vulnerabilities and exploitation techniques, as well as tools, papers, news, and events of interest to the community.

- Bugtraq at Seclists.org
  https://seclists.org/bugtraq/
  The premier general security mailing list. Vulnerabilities are often announced here first. It is recommended to check this frequently.

Security Threat Intelligence

- SANS Internet Storm Center (ISC)
  https://isc.sans.edu/
  The Internet Storm Center (ISC) is a free service to the Internet community and relies on an all-volunteer effort to detect problems, analyze the threat, and disseminate both technical as well as procedural information to the general public. The ISC gathers millions of intrusion detection log entries every day, from sensors covering over 500,000 IP addresses in over 50 countries. It is rapidly expanding in a quest to do a better job of finding new storms faster, identifying the sites that are used for attacks, and providing authoritative data on the types of attacks that are being mounted against computers in various industries and regions around the globe.

- European Union CERT (CERT-EU)
  https://cert.europa.eu/cert/filteredition/en/CERTNewsFilter.html
  CERT-EU hosts a dynamic feed that covers all the important security news. It is not

information from CERT-EU itself, but rather an aggregation of other news feeds. They also produce big screen maps that track the latest news and cyber threats.

- U.S. Department of Homeland Security, Automated Indicator Sharing
  https://www.us-cert.gov/ais
  The Department of Homeland Security's (DHS) free Automated Indicator Sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing email (although they can also be much more complicated).

- FBI InfraGard Portal
  https://www.infragard.org/Application/Account/Login
  InfraGard is a partnership between the FBI and members of the private sector. The InfraGard program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure.

- National Council of Information Sharing and Analysis Centers
  https://www.nationalisacs.org/member-isacs
  Each critical infrastructure sector has its own organization that monitors and ferrets out threat information specific to the industry vertical. Search for your industry to lean more.

- The Spamhaus Project
  https://www.spamhaus.org/organization/
  Spamhaus is a European non-profit that tracks cyber threats and provides real-time threat intelligence. Spamhaus has developed comprehensive block-lists for known spammers and malware distributors, which they provide to ISPs, email service providers, and individual organizations.

Cyber Security News Feeds / Blogs

- Dark Reading
  http://www.darkreading.com/
  One of the most widely-read cyber security news sites on the Web, Dark Reading.com encompasses 13 communities, each of which drills deeper into the enterprise security challenge: Analytics, Attacks & Breaches, Application Security, Careers and People, Cloud Security, Endpoint, IoT, Mobile, Operations, Perimeter, Risk, Threat Intelligence, and Vulnerabilities and Threats. Each community is led by editors and subject matter experts who collaborate with security researchers, technology specialists, industry analysts and other Dark Reading members to provide timely, accurate and informative articles that lead to spirited discussions.

- The Hacker News
  https://thehackernews.com/
  The Hacker News (THN) is a leading, trusted, widely-acknowledged dedicated cybersecurity news platform, attracting over 8 million monthly readers including IT professionals, researchers, hackers, technologists, and enthusiasts. The Hacker News features latest cyber security news and in-depth coverage of current as well as future trends in Infosec and how they are shaping the cyber world.

- Naked Security by Sophos
  https://nakedsecurity.sophos.com/
  Naked Security is Sophos's award-winning threat news room, giving you news, opinion, advice and research on computer security issues and the latest internet threats. Sign up to receive a daily email update from us. The newsletter includes the headlines from the last 24 hours so you can choose which stories interest you at a glance.

- Google – Project Zero
  https://googleprojectzero.blogspot.com/
  Project Zero members spend most of their time doing vulnerability research and exploit development. Most members of Project Zero have a history of publicly reporting vulnerabilities in widely used software or participating in projects related to vulnerability research.

- The State of Security by Tripwire
  https://www.tripwire.com/state-of-security/
  The State of Security is an award-winning blog featuring the latest news, trends and insights on current information security issues, including risk, compliance, incident detection and vulnerability research. Apart from our own frequent contributors, we welcome dozens of industry professionals as guest authors to share with our readers their security expertise.

- Veracode Blog
  https://www.veracode.com/blog
  Application security (AppSec) firm Veracode's blog has grown into one of the leading sources for AppSec news and insights. With regular contributions from security experts, the blog offers informed commentary on the latest security issues. Favorite topics include application security testing, software vulnerabilities, hacking, mobile security, and more.

- Krebs on Security
  https://krebsonsecurity.com/
  Brian Krebs is an award-winning author of a daily blog, KrebsOnSecurity.com, covering computer security and cybercrime. From 1995 to 2009, Krebs was a reporter for The Washington Post and covered tech policy, privacy and computer security as well as

authoring the Security Fix blog. He is also known for interviewing hackers and provides very informative and investigative articles.

- Schneier on Security
https://www.schneier.com/
Bruce Schneier is an internationally renowned security technologist. He is the author of over one dozen books, as well as hundreds of articles, essays, and academic papers. His influential newsletter "Crypto-Gram" and his blog "Schneier on Security" are read by over 250,000 people. He has testified before Congress, is a frequent guest on television and radio, has served on several government committees, and is regularly quoted in the press.

Vendor Security Blogs

- Adobe – Security Bulletins and Advisories
https://helpx.adobe.com/security.html

- Alien Vault – Security Blogs
https://www.alienvault.com/blogs

- Amazon Web Services (AWS) – Security Blog
https://aws.amazon.com/blogs/security/

- Apple – Security Updates
https://support.apple.com/en-us/HT201222

- Cisco - Threat Research Blog
https://blogs.cisco.com/talos

- CrowdStrike - Research & Threat Intel Blog
https://www.crowdstrike.com/blog/category/threat-intel-research/

- FireEye - Threat Research Blog
https://www.fireeye.com/blog/threat-research.html

- Hewlett Packard Enterprise (HPE) - Product Security & Vulnerability Alerts
https://www.hpe.com/us/en/services/security-vulnerability.html

- Juniper Networks - Security Intelligence Center
https://www.juniper.net/us/en/security/report-vulnerability/

- Microsoft Security Blog
https://www.microsoft.com/security/blog/

- Oracle - Critical Patch Updates, Security Alerts and Bulletins
https://www.oracle.com/security-alerts/

- Palo Alto Networks – Unit 42
  https://unit42.paloaltonetworks.com/
- Recorded Future
  https://www.recordedfuture.com/blog/
- Red Hat – Notifications and Advisories
  https://access.redhat.com/security/updates/advisory
- Ubuntu – Security Notices
  https://usn.ubuntu.com/

Appendix C: Sample Incident Response Checklist

Following a cyber attack or security incident, IT providers must take the right steps to protect the confidentiality, integrity and availability of business data at the impacted organization. This checklist is designed as a reference guide to help MSPs and MSSPs respond quickly and appropriately to a cyber attack or related situation. Please note that these are recommendations only, and that ConnectWise accepts no legal liability under any circumstances as to how you choose to implement your specific incident response policies and plans.

ConnectWise | 4110 George Rd #200, Tampa, FL 33634 | 1-866-223-7394 | © 2020 All Rights Reserved | Updated

INCIDENT RESPONSE Checklist for MSPs

ConnectWise®

1 Incident Process Ownership and General Guidelines

- The ConnectWise SOC and the responding SOC team member should be the main point of contact in an incident scenario to ensure all actions recommended from ConnectWise are from a security minded standpoint and all potential risks can be analyzed before moving forward. The partner reserves the right to refuse SOC direction and/or follow the direction of their insurance advisor or law enforcement.

- The SOC team can assist with information gathering, analysis, remediation and restores dependent on deployed ConnectWise toolset (*NOC*, *BDR*, *RMM*) and related products. SOC level of involvement is at the sole discretion of the SOC team based upon ConnectWise products and the risk and potential impact involved as determined by SOC, as aligned with contract requirements and Scope of Service.

- Primary responsibility of a security incident is the **sole responsibility of the partner**. SOC will provide recommendations and assistance with the aforementioned items but partners are the primary process and action owners. Additionally, it is important this document is followed thoroughly and, in its entirety, when possible to ensure the incident is remediated fully.

2 What to Do Immediately Following a Cyber Attack

- **Partner:** Call the impacted organization's insurance company. They will explain their requirements and outline any steps that may need to be taken to protect forensic data or evidence. You want to support—not hinder— your customer's ability to collect an insurance claim. **Be certain to entirely review and discuss Insurance stipulations before proceeding as those will dictate how and if you can proceed further.**

  The SOC team should be contacted immediately following an incident so our investigation can start, and we can verify if any wide-reaching measures are necessary immediately. (Such as mass network disconnects or suspending RMM services and other related organization impacting items)

- **Partner/SOC Advisory:** Review the impacted organization's business continuity or disaster recovery plan, as there may be specific requirements and action items mandated by certain policies or the business owner(s).

- **Partn**er: If possible, have the client acknowledge (in writing) that the infection or attack occurred prior to your arrival onsite and that you were not the cause of this infection to prevent liability.

- **Partn**er: Remind the business owner to communicate or reiterate the company's rules of disclosure to its employees, and to address what should or should not be communicated via public channels like social media, the press, as well as with clients. A standard recommendation is that nothing is permitted to be disclosed until the company releases a formal statement (generally after the facts of the event have been gathered and properly analyzed).

- **Partner/SOC Advisory:** Perform a separate isolated back up of everything—even encrypted or infected computers—to create a recovery path if the containment or remediation steps destroy data (or in the event that decryption fails and a recovery key is discovered after the event has occurred). **Do not overwrite any existing clean backups.** There are cases where the threat actor releases the decryption key months after an attack has stopped paying dividends.

3 Identification

- **Partner:** During the identification phase of the incident your team in conjunction with the SOC need to work to thoroughly investigate and record all possible details related to the security incident as it unfolds. The SOC team will be assisting in recording all details for analyzing and post-incident review.

  Below are items to be recorded if available and any information should be passed along to the SOC team to assist with the incident response and progressing analysis.

  - Who discovered or reported 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?

4 Containment

- **Partner/SOC:** During the containment phase the Partner and SOC will be working in tandem to stop any active threats and contain the breach to prevent further spread and damage to the affected business.

  Work together with the SOC to verify the attack vector utilized. This will vary widely depending on the scope of the attack.

  - If it's a single site/client location with an unconfirmed vector a port scan can be utilized to potentially reveal accessible network ports or services which shouldn't be openly accessible such as RDP, vulnerable services or RMM tools. This can be facilitated through Nmap, Zenmap, Nessus, or RapidFire Tools.

  - If it's across multiple sites the above can still apply but we also need to verify and audit RMM tools and accounts and other remote access methods used by the partner or vendors as there is a high chance this can point to our attack vector. This can be confirmed through log gathering and will be where containment needs to immediately be focused.

  - In addition to the above, ensure 2FA or multi factor is immediately enabled on any remote access tools.

- **Partner/SOC:** Work to ensure infected and compromised systems are isolated from non-affected systems.

- **Partner:** Deny all international traffic in the firewall and only allow what is necessary. Additionally, close access to any unneeded ports or services as previously determined through the perimeter firewall.

- **Partner/SOC Advisory:** Deny all inbound traffic across RDP or other remote access tools to the client sites. If necessary, enable VPN access first, the utilize RDP through the VPN-protected connection.

  If determined necessary as a last resort of containment, unplug your Internet connection at the router until you have regained control of the network. You can also disconnect all power to switches on the network to help avoid lateral movement of the threat and isolate network segments as you work towards containment.

- Partner: Audit all local and domain administrative accounts for recent changes or additions. Rapidfire Tools can be used to automate this step. Remove old and unexpected new accounts and immediately expire and reset all domain and local administrative accounts, including service accounts as this may assist in further containment if compromised credentials are in use.

- **Partner/SOC:** Check all security and system logs for unusual activity, this can include firewall logs as well if applicable.

- **Partner:** Test your backups, and if possible, create a manual set and store them off the network.

- **Partner/SOC:** If applicable, verify through ConnectWise Fortify for Assessment/Dark Web Monitoring for any stolen credentials on your client's domain.

- **Partner/SOC:** If not in place, consider adding Webroot for DNS protection to further prevent command and control calls to infected websites and C2 servers.

- **Partner/SOC:** Leverage ConnectWise Fortify for Endpoint (powered by Sentinel One) to help hunt for and isolate the threat, provide additional visibility, and further spread of the attack. Additionally, leverage Fortify for Network (powered by EventTracker) to analyze and provide additional visibility into the firewall and active directory on endpoints.

- **Partner:** Receive authorization in writing, email or text from the client or insurance provider before moving to the Remediation Phase.

5 Remediation

- **Partner/SOC:** Once the incident has been contained, we need to find and work to eliminate the root cause of the breach. It is vital to ensure all previous and successive steps are followed to minimize or eliminate the chance of potential reinfection.

  Be sure when working through these steps machines are properly isolated following previous steps to prevent further spread of the infection when working devices.

- **Partner/SOC Advisory:** If necessary clean a domain controller, preferably in safe mode, of the infection.

- **Partner:** Disable Autorun on all systems on the network using a group policy object (GPO) in Windows. Visit goo.gl/yBCNeg to read: How to disable the Autorun functionality in Windows. Note: It is strongly recommended to disable the Autorun feature using GPO from the Domain Controller.

- **Partner/SOC:** While also possible to disable Windows Task Scheduler in the same manner via GPO, it is suggested on more current systems (post-Windows XP/2003) to manually check items such as Task Scheduler, Appdata directories and Temp directories on affected systems for unknown, suspicious, or potentially malicious items.

  Work with the SOC based on current analysis for suggestions on known directories and registry entries where malicious files may be contained with the potential to auto-execute or re-infect.

- **Partner:** Reset all user passwords to a default password, then share that new password verbally around the office so users can reset their passwords. Do not email it out and be sure to force users to change from the new temporary password you set. If you only force password changes, then there is a chance the threat actor will reset their compromised account and still have access to the network.

- **Partner:** Reset all device passwords, including switches, routers, firewalls, VPNs, IDS devices, etc.
- **Partner:** Bring up one server at a time, clean it, and if it's not a required server shut it down until you have completed cleanup of the network.
- **Partner:** Bring up one workstation at a time (off the network) and clean as needed. Reboot several times looking for a return of the infection.
- **Partner/SOC:** As a final step in remediation with machines still in isolation, reboot the devices and check with Sentinel One or other third-party AV solution for any new alerts that may indicate a recurring infection that was not properly remediated. This step needs to be done before bringing devices back onto the production network.
- **Partner:** Check your backups again. You can never have enough good backups.

6 Recovery

- **Partner/SOC Advisory:** This phase is for restoring and returning affected systems back to the production environment. Some items to keep in mind during this process are as follows:
    - Have systems been patched, hardened and tested before restoring to the business environment?
    - When necessary can affected systems be restored from trusted back-ups?
    - What tools moving forward will ensure similar attacks will not reoccur?
- **Partner:** Restore from clean backups where needed. If clean backups do not exist, ConnectWise does not advise as to whether MSPs or their clients should pay a ransom. That decision is entirely up to the insurance company and the data owners.

  Note: If necessary, Shadow Explorer can be utilized to recover important files manually via VSS snapshots if available and in the case full clean backups do not exist. (https://www.shadowexplorer.com/)
- **Partner/SOC:** Scan the network one more time with relevant tools (e.g. SentinelOne, HitMan Pro, or other updated security scanning engines).
- **Partner:** Once the network is back online, run a new backup job and backup all critical data before allowing users back onto the network. In certain cases, this may be a time-consuming effort, but is well worth it vs. running the risk of a second or repeat infection occurring.

7 Debrief

- **Partner/SOC:** Once the incident is fully isolated, remediated and recovered hold an after-action meeting with the SOC team to discuss findings and what has been learned from the breach. Some questions to be answered during this phase are as follows:
  - What changes can be made to the client's security to prevent future occurrences?
  - What employee training awareness should be addressed?
- **Partner/SOC:** Review and document the entire incident and perform post incident analysis.
- **Partner:** Debrief with the client fully, and work to design and implement a security plan designed for their budget that will help defend against this type of attack in the future.