CONNECTWISE

CONNECTWISE WHITE PAPER

The Cybersecurity Talent Gap

CONTENTS

INTRODUCTION

Over an eight-year period tracked by Cybersecurity Ventures, the number of unfilled cybersecurity jobs grew by 350 percent, from one million positions in 2013 to 3.5 million in 2021. For the first time in a decade, the cybersecurity skills gap is leveling off. Looking ahead, Cybersecurity Ventures predicts the same number of openings in 2025 (3.5 million). This poses a challenge for MSPs, SMBs, and enterprise companies alike. Year by year, the cost of attracting and retaining cybersecurity talent rises. Many businesses are vying to attract people from the same, small talent pool in an increasingly competitive landscape.

As an MSP, you're dedicated to growing your cybersecurity services to make clients more secure, but you may be unsure how best to build your team. After all, we're already experiencing a talent shortage, and cybersecurity professionals are expensive resources to have on staff. A typical security operations center (SOC) is operated 24/7 by 10 to 13 people, making it a costly—and unattainable—proposition for many MSPs.

But all is not lost. We can help you scale your cybersecurity business without competing for coveted talent or breaking the bank.

3.5M

Unfilled cybersecurity positions by 2025

- **Difficult to attract and retain talent**
- **Number of successful cyberattacks continue to increase**

—Cybersecurity Ventures

CHAPTER 1: Develop Your Own Talent

Companies can seek creative alternatives to the traditional training approach focused on four-year computer science degrees to meet the demand for cybersecurity skills. By leveraging alternative training programs such as **ConnectWise certified training**, you can equip new and existing cybersecurity workforces with modern cybersecurity education and awareness.

Looking inward, your IT personnel could be capable of performing essential cybersecurity tasks. After all, cybersecurity professionals and IT professionals are cut from the same cloth in terms of education and training—they just have different responsibilities and manage different metrics.

At ConnectWise, we've made it our goal to help escalate, elevate, and empower your cybersecurity team by providing sophisticated training and certifications. To that end, ConnectWise offers **two certified fundamental classes for engineering and sales**. Our engineering course helps workers understand the technical side of cybersecurity, covering critical topics such as risk management, intrusion detection, and malware analysis. This course also demonstrates secure onboarding processes and discusses what an initial phase of an incident response program could look like. **Best of all, these classes are free for everyone.**

Another resource that you can leverage is the National Initiative for Cybersecurity Careers and Studies (NICCS). This expert organization has developed a **Cybersecurity Workforce Development Toolkit**. It includes resources for recruiting and retaining top cybersecurity talent and career path templates that help organizations understand their cybersecurity workforce and staffing needs, empowering you to protect yourself, your customers, and their networks.

Aside from implementing training efforts, many top MSPs are also doubling down on automation to maximize staff efficiency and available resources. Take professional services automation (PSA) and remote monitoring and management (RMM) software. In the past, many MSPs would hire additional headcount to handle the administrative processes of service delivery, onboarding, and invoicing. However, throwing more people at the problem isn't always an option, nor is it necessarily the right solution. Many MSPs are building automation and workflows into their existing tools and systems. When you invest in automation upfront, it makes your current staff more efficient and often eliminates the need to hire more staff.

In the same vein of efficiency, MSPs are doubling down on their efforts to standardize tools. This includes internal software and equipment as well as customer-supported systems. Standardization removes the need to train your teams on multiple tools, making them highly efficient in the systems they know and support. As an added benefit, standardizing tech stacks helps speed up resolution time, which increases customer satisfaction.

CHAPTER 2: When to Use a Cybersecurity Vendor

Training your teams to be cybersecurity specialists isn't always the best solution or most cost-effective. Rather than handling all cybersecurity work in-house, many MSPs seek the protection and monitoring of a reliable third-party vendor to take on many cybersecurity tasks. Here are a few key factors to consider:

Cost Efficiency

You might think that outsourcing a chunk of cybersecurity labor will cost more than doing it in-house. But when it comes to protecting important information within your network, leveraging teams (such as the SOC at ConnectWise) to support and deliver your cybersecurity support is the smartest approach. For example, if you build an in-house SOC, the cost can reach as high as $4 million per year. Instead of hiring a team of security analysts, implementing training, working through turnover, and installing numerous cybersecurity solutions, **you can turn to a reliable cybersecurity company** for couple thousand dollars per month.

Real-Time Monitoring and Instant Analysis

Speed reigns supreme in the world of cybersecurity. Equipped with quality software and expert analysts, cybersecurity companies can help your MSP detect potential network attacks as soon as they happen instead of days, weeks, or even months later.

Advanced Monitoring

It's important to know what different cybersecurity and remote monitoring software can do for your organization. **With services such as SIEM solutions**, you can customize your cybersecurity defense to monitor potential threats that target your organization's service domain specifically. With constant updates in servers, computers, and other electronics, a third-party SOC will monitor it all and prepare your network against threats. Best of all, they can pinpoint potential problems as soon as they happen, ensuring your organization will always be ahead of the curve for cybersecurity.

Time Efficiency

Using a SOC from a trusted third party ensures that your business's cybersecurity is diligently monitored around the clock, fixing issues before you or your clients are aware of any problems. Ultimately, you can reap the benefits of more productivity and peace of mind with a third-party SOC.

$2-4M

Cost of building your own SOC

CHAPTER 3: Partnering With ConnectWise

In today's rapidly changing cyber threat landscape, it can be difficult to build out a robust security program all by yourself. Consider leveraging ConnectWise to help you build, grow, and sustain a profitable cybersecurity practice.

ConnectWise SOC Services

Keeping pace with the grind of system alerts can burnout the best of staff. As the noise builds and response is stretched thin, the defense your clients depend on becomes vulnerable to failure.

As an extension of your team, **SOC** expert security analysts, combined with cutting-edge threat intelligence, will manage all your security monitoring—24/7.

ConnectWise Incident Response Service

Say hello to your cyber reinforcements The **ConnectWise Incident Response Service** provides real-time management, guidance, and analysis to help MSPs investigate, remediate, and recover from a severe security incident.

- 24/7/365 access to expert cybersecurity incident response analysts
- Real-time incident management coordinated within established processes and playbooks
- Formal analysis reports detailing observed and recommended tactical and strategic improvements
- 30 days post-incident monitoring of the environment for re-infections

ConnectWise Cybersecurity Center

Navigating the ever-changing cybersecurity landscape can feel overwhelming. You're managing cybersecurity best practices and customer safety, but you're also wondering if your product vendors are secure. You're not alone.

Our priority is to help you protect your customers and business, and we do this in two ways. First, we commit to keeping our products secure, and second, we provide information, education, and solutions to help MSPs build their own cybersecurity services.

The **ConnectWise Cybersecurity Center** exists to help you clearly see cybersecurity intelligence, resources, and best practices specific to MSP businesses. We continually research and access cybersecurity experts to build resilient and flexible programs, solutions, and services that help you meet your cybersecurity and service offering goals.