Closing the Cybersecurity Talent Gap

Contents

Introduction

Cybersecurity Ventures predicts there will be 3.5 million unfilled cybersecurity positions worldwide in the next couple years. Be it health care, retail, or manufacturing, this poses a challenge for organizations of all sizes, across all vertical market segments. Year by year, the cost of attracting and retaining cybersecurity talent rises. Many businesses struggle to attract people from the same, small cyber talent pool in an increasingly competitive landscape. Retaining talent adds another angle to the mix.

As a growing business, you're dedicated to serving your customers and delivering the greatest value you can. But in an everevolving cyber threat landscape, how confident are you in your ability to keep your business operations running smoothly, and your most critical assets secure from today's threat actors? If you're like many others, your IT team is already stretched thin and making sense of the complexities of cyber defense is a frustrating challenge to solve. Talent availability shortages aside, cybersecurity professionals are expensive resources to have on staff. In an environment where systems, endpoint, and user access should be monitored 24/7, building out solid security coverage is costly—and an often unattainable proposition for many operators.

But all is not lost, and cyber criminals can be kept at bay. Here are two possibilities to help you scale your cybersecurity defense without competing for coveted talent or breaking the bank.

3.5M

Unfilled cybersecurity positions in the next couple of years

- **Costly to attract and hire security talent**
- **Difficult to retain IT security personnel**
- **Challenging to protect the business as the number of attack vectors continue to expand**

— Cybersecurity Ventures

Develop Your Own Talent

Companies can seek creative alternatives to the traditional approach focused on finding and hiring staff with specialty degrees in cybersecurity. Looking inward, your IT personnel are 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.

By leveraging alternative training programs such CISSP certifications (Certified Information Systems Security Professional), you can equip new and existing IT staff with modern cybersecurity education and awareness. As the world's premier cybersecurity certification program, CISSP will empower your staff to effectively design, implement and manage a best-in-class cybersecurity program—ensuring your business is looking at your defense-in-depth in a holistic, 24/7/365, and strategic-based approach.

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 operators understand their cybersecurity workforce and staffing needs, empowering you to protect yourself, your customers, and their networks.

Further, good security requires all employees be guardians of the business. In addition to having cyber-smart IT staff, it's also important to have cyber-smart employees. Elevating the security awareness of your employees about current cyber threats, company security policies, and the personal role each plays in keeping your business safe is an often overlooked component.

A user-focused cybersecurity awareness program will help arm your frontline workers with important understanding of the risks of attacks that target unsuspecting users. Good basics include education on:

- **Phishing and social engineering**
- **Passwords and network access**
- **Device security**
- **Physical security**

There are many ways to implement this type of training along with resources available to help inform first steps.

Working with a Cybersecurity Partner

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 operators opt for security services and 24/7 monitoring from a reliable managed service provider 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 mission critical information within your environment, leveraging 24/7 monitoring and response services delivered by experts within a security operations center (SOC) can be a cost smart approach—and a force multiplier to your cyber

defense! For example, depending on the size of your organization and the number of systems and endpoints to be monitored, the cost of building an in-house SOC can be untenable. Instead of hiring a team of security analysts, implementing training, working through turnover, and installing numerous and complex cybersecurity monitoring solutions, you can turn to a proven cybersecurity partner for turn-key services at a fixed and predictable monthly fee.

REAL-TIME MONITORING and ANALYSIS

Speed reigns supreme in the world of cybersecurity. Equipped with quality software and expert analysts, a cybersecurity partner can help your business detect potential network attacks as soon as they happen instead of days, weeks, or even months later. Businesses should assume they will eventually be attacked. The question becomes, when that happens, will you know before it's too late? With enterprise-grade solutions managed by expert analysts, you'll gain a new level of control and visibility of your environment. The result? Detection of malicious activity that may indicate an attack in motion and resolution before it does damage.

ADVANCED MONITORING

It's important to know what different cybersecurity and remote monitoring software can do for your organization. With services such as security information and event management (SIEM) solutions, you can customize your cybersecurity defense to monitor for potential threats that target your organization's most critical assets. With constant monitoring of system and user events, backed by a 24/7 SOC for analysis and response, you'll be best prepared to identify and stop threats to your business. Best of all, such services can help you pinpoint potential problems and advise on remediation measures to close security gaps and enhance your defense-in-depth.

TIME EFFICIENCY

Using managed services from a cybersecurity partner ensures that your business is diligently monitored around the clock and fixing issues before you are aware of any problems. Ultimately, you reap the benefits of more productivity, stronger defense, and the peace of mind that comes with knowing that expert security staff are looking after your defense so you can focus on what's most important to you—looking after your business!

Conclusion

As cyber threats become more sophisticated, the need for an advanced intrusion detection system and skilled professionals to protect your valuable data and alleviate risks has never been more pressing. How you build, manage and train your cyber security team is critical. It requires careful planning and ongoing investment in talent development. In-house staff must continuously adapt to evolving threats to maintain strong security. You must have enough staff for around the clock diligence, and will need to provide them with regular training and professional development opportunities to keep pace with the ever-changing threat landscape.

Alternatively, partnering with a trusted and reliable cybersecurity partner offers many advantages and strategic benefits over building it all yourself. A security partner can provide the security systems and software needed to protect your network, and a pool of highly skilled and experienced professionals who are dedicated to cybersecurity. This way you can avoid the capital expenses associated with acquiring the needed equipment and software, and the operational costs that would go towards training and maintaining a full-time cybersecurity staff. It also allows you to focus on your core competencies while leaving cybersecurity to professionals who possess the up-to-date knowledge and expertise needed to counter rapidly evolving vulnerabilities and exploits.

Whether in-house or with a partner, by prioritizing your cybersecurity efforts, you can significantly enhance your defense against cyber threats. Investing in the right cybersecurity systems and talent will establish robust defenses against potential cyber attacks, which will safeguard your mission-critical systems and sensitive data, and maintain the trust of your subscribers.

ZCorum provides a comprehensive and fully managed cybersecurity solution. For more information on how we can quickly protect your network, with minimum expense and manpower on your part, see our website.

ZCorum™

800-909-9441

ZCorum provides a suite of broadband diagnostics and managed services to cable companies, telephone companies, utilities, and municipalities. As broadband providers face greater complexity and competition, ZCorum continues to help operators increase operational efficiency and reduce costs, while improving subscriber experience. This is achieved through ZCorum's diagnostics solutions for DOCSIS, DSL and Fiber networks, plus managed services that include data and VoIP provisioning, residential and commercial VoIP service, branded email and Web hosting, along with 24x7 support for end-users. ZCorum is headquartered in Alpharetta, GA. For more information, please visit **ZCorum.com.**