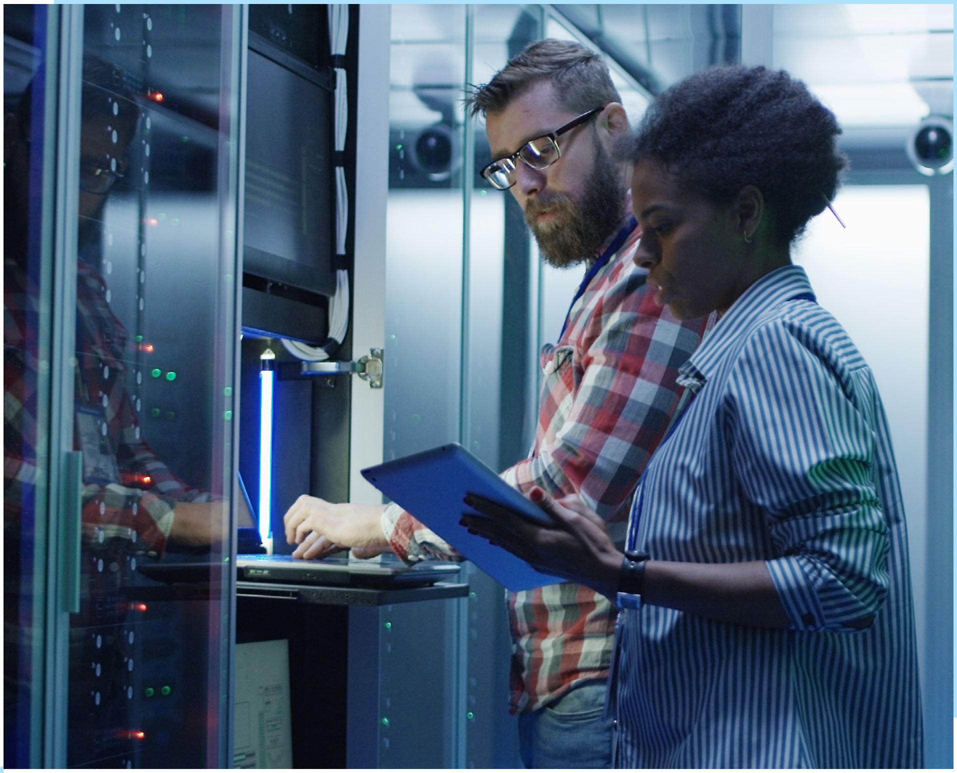
Cybersecurity Challenges Facing Today’s Small & Mid-Sized Businesses

The Value of a Managed Security Operations Center (SOC)

Contents

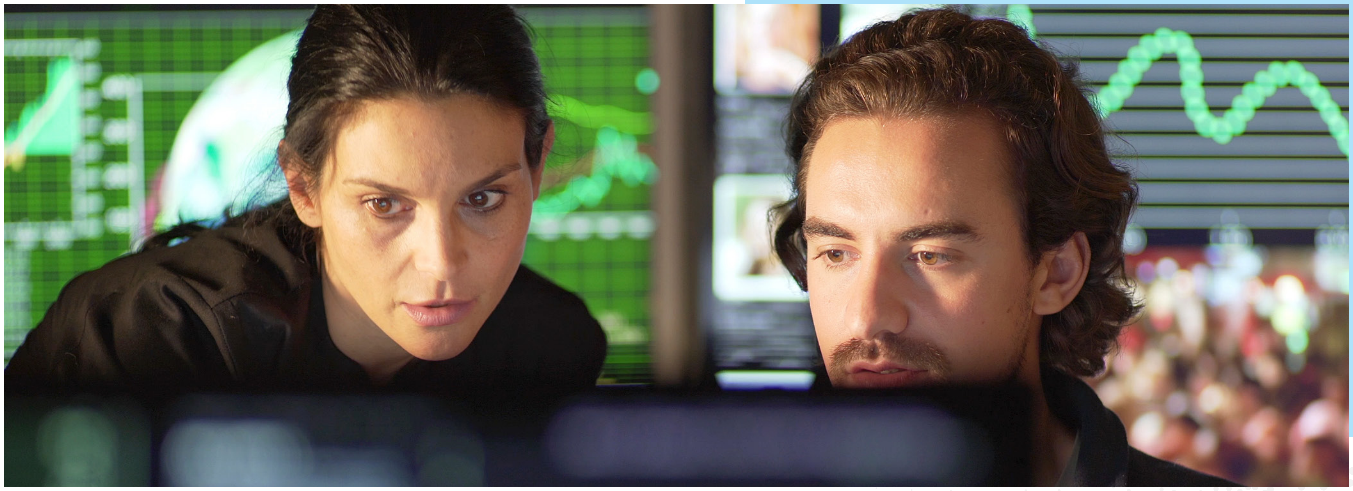
The Case for Managed Security Services

A strong defense against evolving cyber threats requires an always-on security mentality. But for many small and medium-sized organizations (SMBs) with limited resources, shifting to a more proactive approach to threat detection can be difficult. It's no surprise business owners are increasingly turning to managed service providers for cost-effective security skill sets and services.



Lack of Cyber Expertise in the Organization

Often, as organizations look to strengthen their cybersecurity defense, the first stumbling block is a lack of expertise. And invariably, when an IT professional is on staff, he or she is pulled in numerous directions, reactively addressing the need of the moment. Managed SOCs typically employ a team of specialists who are trained and certified in cybersecurity best practices, tools, and techniques. They understand the different types of cybersecurity attacks, compliance requirements, threat trends, and target vulnerabilities.



Alert Fatigue

Cybersecurity protection technology can generate hundreds to thousands of alerts every week. SMBs with limited or no experienced IT security staff can be quickly overwhelmed by the sheer volume of the alerts. With a narrow window to respond to alerts and a lack of experience prioritizing warnings, these warnings can soon become white noise. Now, critical alerts can potentially fall through the cracks and potential data breaches can go unnoticed. With a managed SOC on your side, you don't have to worry about monitoring and detection. Your SOC vets and prioritizes, and then works with you when steps to remediation are necessary.

145% It's estimated that the cybersecurity workforce needs to grow by 145% to meet increasing demand.[1]

IT Staff Supply and Demand

You may have an analyst or technician on staff now, but the security job market is ripe with opportunities. Due to a rising hiring demand, the global cybersecurity workforce skills gap stands at just over 4 million. The gap is nearly 500,000 in the United States alone.

Low supply coupled with high demand spells competition. Unfortunately, the more experienced your technician becomes, the more likely he or she may be to accept a higher salary elsewhere. The bottom line is it's tough to keep trained security staff. Be ready to adjust your IT budget to add the perpetual expense of hiring and training new people.

[1] "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)2 Cybersecurity Workforce Study, 2019" International Information System Security Certification Consortium, Inc. (ISC)2, 2019

Time and Energy Taken Away from Business

Working with a managed SOC built and staffed by a managed security services provider (MSSP) provides immediate security expertise, quick ramp-up and breathing room to proactively strategize the future of your IT security focus. Fortunately, the ideal managed SOC offers a variety of security solutions so you can choose your level of involvement. Options can range from security services done for you, with you or do-it-yourself. Let's explore the benefits of each option:

Do-It-for-You

You can partner with a managed SOC provider who monitors security events and provides remediation of malicious activity, working directly with you as an extension of your team. This allows you to enjoy top-notch cybersecurity protection for your business—and allows your team to focus on the needs of your employees, partners, and customers.

Do-It-with-You

Managed SOC resources can augment your IT security staff, allowing you to maintain fewer security personnel. Ramp-up is fast so you can immediately reduce your cybersecurity risk. In addition, by partnering your IT security staff with a managed SOC service, you're able to build internal skill sets through access to a team of experts.

Do-It-Yourself

If your internal IT staff can keep your organization safe from cyber risks, you may decide to develop your own SOC. You can still partner with a managed SOC provider for monitoring and protection, while you handle remediation. But keep in mind, this is a big job. We can guide you on steps to take to ensure success.

The Added Expense of Security

Managed SOC providers typically offer unlimited support at a pre-defined, fixed monthly fee. Your bill doesn't increase—even if the number of potential threats do. This approach allows you to easily manage and monetize security-as-a-service and spread the cost savings to other areas of your business.

The Managed SOC Difference

Built with SMBs in mind, the typical managed SOC team understands how you work and the challenges you face. For example, when managing an active attack, companies need to execute specific steps from investigation and response to remediation. A managed SOC team can provide clear documentation of the key processes, so you know your role and the role of your IT security staff. A managed SOC team will work in lockstep with you to ensure you're operating as one collaborative unit, strengthening your security so you can focus on your business. That's the managed SOC difference! Contact us to learn more.

mason
INFOTECH

Mason Infotech Ltd
01159408040
https://masoninfotech.co.uk

Nottingham, Nottinghamshire NG1 2AS