ARMOR™

Too Many Hats, Not Enough Heads

SOLVING SECURITY TALENT PROBLEMS WITH A SECURITY PROVIDER

Summary

Overworked and occasionally under-trained in cyber security, IT professionals are struggling to maintain their companies' security postures on top of other daily tasks. When staff members are forced to wear too many hats, they become a weak link in the systems and processes that defend critical data. Companies struggle to focus on security when it isn't their core competency and often see being secure as a distraction to their main goals of generating revenue within their industries.

Due to this issue, organizations have shifted focus from preventing attacks to simply dealing with them when they happen. To power out of the distraction rut, companies can look outside their organizations to find the answer to their security needs. Companies that choose to work with a security provider gain access to the best security professionals and technologies and relieve the stress on their already weary IT departments while keeping focus on their core business.

This white paper details why you should not and, most importantly, do not need to handle security on your own. Learn how to select the right security provider and close the gap towards mitigating attacks.

Table of Contents

Your Overloaded IT Department

As the prevalence of cyber attacks rises so does the pressure on business and technology professionals. Burnout is a well-known problem in the world of cyber security, as evidenced by research studies, blog discussions and happy hour lamentations.

According to one study,[1] 56 percent of information security professionals say their organization is short-staffed. IT departments are being asked to do more with the same tools and are not permitted to correct legacy security gaps due to funding, but tech workers complain they are so busy that they can't make blocks of time long enough to work on complicated problems or even find a moment to clear off their desks. If this is true for your organization, can you really expect the attention to detail, mental agility and up-to-date education that is necessary to defend your assets from threats?

Building an effective security problem doesn't happen by accident; it requires specialized knowledge of each piece of security technology and software in use. This ensures proper integration into an organization's infrastructure, enabling them to fully leverage automation and stay ahead of threats.

Yet executives who task their IT departments with securing the company's systems are often unaware that information technology and security, while related, are not the same thing, and that even the most talented specialists aren't likely to be knowledgeable about the fundamentals of security. This leaves businesses struggling to fully understand security practices and tools.

The rise of the cloud has also added to this challenge. Many IT professionals are not security experts or know how to design effective overlapping controls essential for cloud security and compliance. Technology executives may not be aware of how a move to the cloud complicates things, but IT managers certainly are.

56%

OF INFORMATION SECURITY PROFESSIONALS

Say Their Organization Is Short-Staffed. [1]

LEARN MORE

ARMOR™

The Unintended Consequences of Overworked IT

IT departments are stretched thinner all the time when trying to simply “keep the lights on” while adding new tasks and tools to keep their businesses competitive. Is adding more people the answer? No, but finding real cybersecurity expertise is a challenge in itself. Businesses need to focus on the original “roots” of IT and pursue additional automation. When handling security issues, perhaps a better approach would be to develop skills internally. However, true cyber security expertise is developed over years of detecting, analyzing and defeating actual cyber attacks.

Only 17 percent of IT workers have even a basic security certification, and only 29 percent of organizations have anyone with a security certification on staff.[2] This is a frightening statistic when you consider that security is a full-time job.

Threat monitoring needs to be real-time and responses need to be set in motion as soon as a threat is identified to mitigate it before an attacker can compromise systems. One or two people can’t do this job—a skilled team needs to be in place to provide the level of protection and expertise that is necessary to keep assets out of the hands of threat actors.

Compliance adds another layer of complexity to the problem at hand but should be seen as the foundation of being secure. Regulatory and audit authorities state time and time again that their regulations are “basic data security standards”. An IT department that is not fully versed in answering regulatory requirements will simply work in checklists, but the assessor who follows behind them will see the failings of that approach. Most compliance isn’t prescriptive and is point-in-time; education and planning are required, and experience in those areas is crucial to meeting requirements.

17%

OF IT WORKERS

have even the most basic security certification. [2]

29%

OF ORGANIZATIONS

have anyone with a security certification on staff. [2]

LEARN MORE

The Unintended Consequences of Overworked IT (cont.)

Threat actors continually evaluate environments for vulnerabilities, meaning security can't lapse. Target was PCI-DSS compliant when it was breached. Weak credential management and a failure to monitor controls provided an opening for hackers to steal nearly 70 million private records.

If that can happen to Target, which was heavily invested in its security posture, companies with lesser resources are wise to worry about their own exposure.

Remaining compliant is just one facet of starting to protect information assets. Intellectual property, company secrets and research and development results also need to be defended by skilled, focused personnel. Trusting an overworked IT department to secure these valuable properties alongside their regular workload places a company's operations, reputation and bottom line at risk.

70M

Target was PCI-DSS compliant when it was breached. Weak credential management and a failure to monitor controls provided an opening for hackers to steal nearly **70 million private records.**

Is DIY Defense Desirable?

Security-conscious organizations tend to believe a greater investment in security talent, techniques and technology will yield better results. They try to reduce their risk by buying more security tools and "throwing bodies" at their security problems.

However, the best defense against a threat today isn't necessarily the best defense against a threat tomorrow; hackers are adaptable, their techniques, tactics and procedures are always changing.

Security tools themselves don't provide infallible security. If they did, then vendors would guarantee outcomes—but even though there are more than 500 vendors[3] offering security tools, none of them back up their products with a solid promise that their product will prevent breaches.

There's a good reason for that. Even the best tool from the most trusted vendor is only as good as the security team supporting it. If that team is skilled at monitoring, identifying and resolving network anomalies, the tool will be satisfactory—and if they're not, it won't.

Additionally, security teams need to focus on the operational "care and feeding" of their security infrastructure. Threat intelligence needs to be applied to these technologies to ensure that they are reporting useful information and is required to enable a proactive security approach.

That reality pushes some companies to consider two options: hiring their own teams of security professionals or building an in-house security operations center (SOC), a facility staffed by specialized security professionals whom monitor and defend an organization's enterprise information systems.

> 500

VENDORS OFFERING SECURITY TOOLS

LEARN MORE

Is DIY Defense Desirable? (cont.)

These are certainly possible if the budget and business acutance are there, but the cost of building and staffing a SOC will outweigh the benefits for most organizations as well as distract organizations from their core business.

Some companies underestimate the cost of setting up a SOC because they're only thinking of log analysis. Hiring three shifts of log analysts who can actively work alerts when anomalies are discovered is a viable endeavor; however, the next step is incident response, and that's where the costs add up. When an incident occurs, the SOC needs to be staffed with high-level (and therefore high-dollar) experts who can take a triaged incident, investigate, conduct forensics, and remediate the issue. This requires at least two tiers of analysts staffed around the clock. They need real-time feeds from active threat intelligence with clear focus on quality threats, redundant systems and time off their primary duties to train for new certifications.

A strong focus on vulnerability and threat management needs to be in place to quantify current security state, measurable risk, as well as develop and maintain hardening standards for the overall environment. An average SOC costs millions and takes months to become operational.

Another responsibility assigned to the security team is the delivery of security awareness training. While companies know they need to conduct security awareness training, both for their own benefit and to meet regulatory requirements, finding security personnel with the people skills and willingness to conduct such training is difficult; not everyone is a natural trainer and even analysts that are good at presenting are not always willing or able to take time away from interesting work to present basic training to non-technical staff. In addition, removing an analyst from his or her

Is DIY Defense Desirable? (cont.)

primary duties to conduct simple training is a poor use of resources from a strategic point of view.

Lack of career advancement for security analysts in non-security industry companies is another hurdle to attracting and retaining SOC-level talent. Like all people, security professionals want to advance their careers. In a company where security is not a revenue-producer, there isn't room for a security analyst to move up to an executive position. Today's skilled security experts are in high demand and retaining this level of talent is becoming even more difficult. For these reasons, security professionals tend to gravitate toward jobs at security service providers and security brands.

Security analysts are in such high demand that they can write their own tickets, and tend to job-hop frequently for reasons that include not only better pay but a chance to work with for companies that take security seriously, have buy-in from the Board of Directors and middle management as well as the chance to work with a more skilled security team with good techniques and better technology.

Security professionals know that training and reading can only teach them so much; they need to work alongside more skilled and experienced team members on the job and field new challenges in a live environment in order to better their skills and, therefore, their careers.

Security leaders that can actively mentor those around them are critical to this need. These are additional reasons security professionals tend to prefer employment at security service providers and security brands, where they can learn the most, handle the widest range of challenges, and potentially move into the ranks of leadership.

Companies that recognize the difficulties and expense of setting up a SOC may consider the use of a public cloud provider as a more practical option. They assume their cloud provider will have the tools, techniques and expertise to keep their customers' data secure, but that is a misconception. Many public clouds only secure their own infrastructure. This means securing your data is still your responsibility, and so you still need to keep your own security staff on the payroll and purchase and manage your own security tools. The burden is lightened, but not eliminated.

So if your security shouldn't be managed by your IT department, an in-house SOC is too expensive and your public cloud provider won't provide a complete solution, what can your organization do to help your IT department reduce risk and protect assets?

Support Your IT Department with a Security Service Provider

A good security provider is an extension of your team. Instead of relying solely on your IT department, whose staff doesn't have the necessary skills or bandwidth to handle security, they will have a full bench of experts with deep expertise in your particular environment, working around the clock to monitor and respond to events on your network.

Acting as an extension of your team, they can aid in building partnerships with your internal staff and coordinating efforts towards preventing and detecting attacks, limiting the overall risk of attacks and allowing you to focus on core industry functions.

There are many types of incidents that can occur, and few analysts will have experience in responding to all them. When an incident occurs, your security providers can dedicate top-tier specialists to monitor and address the situation until it is resolved. This flexibility ensures that you have the right resource at the right time and are not continuously paying the salary of an expert who is only needed sporadically.

Shift Complexities Offsite

Your IT department is the heart and soul of your organization. It keeps your network and business-critical systems running, ensures that desktops and devices are functioning, and supports your users. All those responsibilities keep your IT professionals operating at full capacity, and asking them to take on the additional burden of managing 24/7 security will create security gaps that expose your entire organization to breaches and take critical resources away from aiding to generate revenue.

By sharing the burden of security with a provider, your IT department is free to fulfill its core functions while your assets are guarded by dedicated experts who have the tools, experience, and resources to fend off malicious actors.

This is a necessity for businesses that wish to operate safely in a threat landscape that is constantly evolving in complexity and volume.

References

1. Kelley, D. (2014, May 9). Why Overworked Employees Are Security Risks.

   Retrieved from Security Intelligence: https://securityintelligence.com/security-risk-staffing-it-teams-overworked-employees/

2. Spadafora, A. (2016, July). Most organizations don't have an IT security expert.

   Retrieved from Betanews: http://betanews.com/2016/07/02/it-security-expert/

3. Manjon, M. (2015, June 4). A framework to help make sense of cybersecurity tools.

   Retrieved from Network World: http://www.networkworld.com/article/2931576/security0/a-frame work-to-help-make-sense-of-cybersecurity-tools.html

US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167

ARMOR™