Secureworks

WHITE PAPER

Small Security Investments Can Lead to Big Rewards

Security professionals at most organizations often have a thankless job.

Typically challenged with a shortage of technologies, clearly defined processes, and supporting personnel and resources, they live in a reactive world handling the latest operational problem, patching the latest vulnerability, or responding to another compromise. Unfortunately, in this state, the organization is likely to see continued incidents and the associated degradation of its security posture.

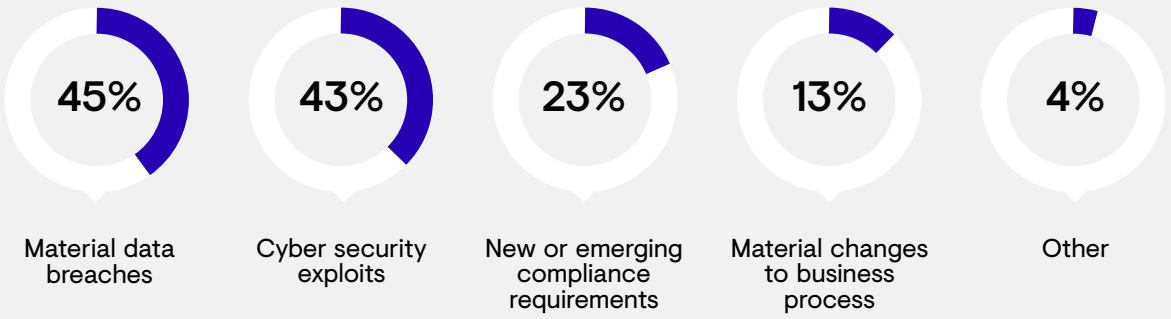
While most security professionals do not have the power to increase investments and make organizational changes that will help alleviate the aforementioned situation, they can, with the help of their leaders, drive key low-cost to high-reward investments that will improve their security posture. In this paper, we will explore those changes, including:

- Following sound risk management practices
- Prioritizing customization and tuning of technologies used to detect incidents
- Acquiring automated, intelligent and integrated security technologies
- Partnering with a managed security services provider (MSSP) to fill in capability gaps

Implementing these solutions often requires support from management because it may involve significant enterprise-wide changes, including the reallocation of budgetary and staffing resources. Before proposing any solutions, security staff should insure that they are working toward the same goals as the organization's management. A recent study by the Ponemon Institute indicated that security staff and management's priorities are often misaligned.[1]

Events that can cause security to be taken more seriously by the C-suite[2]

(More than one response allowed)



Secureworks

Every Organization Is Different

Each security team needs to create its own plan for improving day-to-day, tactical security because no two organizations face quite the same situation. That being said, some improvement actions are generally recommended for all organizations that have not already adopted them. These recommendations are described below.

Follow sound risk management practices.

Having risk management practices implemented throughout an organization and led by the security staff is critical to achieving the most "bang for the buck" in terms of security. According to 58 percent of respondents, IT security is a standalone function and not integrated with other business functions. As a consequence, most companies in this study do not have an IT security strategy that spans the entire enterprise.[3] Even those organizations that do such prioritization often choose security practices largely based on conventional wisdom and compliance requirements, not because they are formally determined to be the best feasible solutions for the organization as the result of a rigorous risk assessment.

When less-than-optimal security practices are adopted, the whole organization suffers. Additional incidents will unnecessarily occur, which will increase the damage to the organization and increase the amount of resources needed to respond to incidents. This is why it's so important for the security team to understand the fundamentals of risk management and to strive to make their decisions with risk management principles in mind. There is no "best" risk management methodology; rather, each organization should select the methodology or methodologies that best fits its resources and needs.

Prioritize customization and tuning of technologies used to detect incidents.

All too often a security team receives a major new security technology designed to detect incidents, but the team cannot take full advantage of this technology because the team members do not have enough time to monitor it periodically and make corresponding changes to the technology's configuration.

A classic example is security information and event management (SIEM). Deploying a SIEM involves extensive integration with other enterprise security controls, which may necessitate customizing the SIEM's configuration or even acquiring development support to code interfaces. Maintaining a SIEM over time not only involves taking upgrades, replacements and additions of the other enterprise security controls and monitored software into account, but it also necessitates tuning the SIEM to improve its detection accuracy, to better estimate the relative severity of each alert it generates, and to respond when necessary with containment measures, such as blocking communications that appear to be jeopardizing the organization's sensitive data.

Without performing customization and tuning actions on an ongoing basis, the security team will find the SIEM to be largely useless in terms of incident detection, other than perhaps helping to check a logging capability of a security compliance checklist. Just a relatively small investment in time can greatly improve detection and prevention capabilities, which in turn can significantly reduce the security team's workload and more than make up for the resources expended in doing the customization and tuning in the first place.

Acquire automated, intelligent, and integrated security technologies.

Many organizations still have security architectures that are largely based on a network perimeter-based approach to security. These architectures are increasingly ineffective because of three major trends: mobility; public clouds; and network traffic encryption. Perimeter-based network security controls are simply unable to analyze the security of an ever-growing percentage of the organization's data communications.

Adjusting a security architecture to take mobility, public clouds and encryption into account is rarely as simple as repositioning a few network-based security controls. Besides deploying virtual private networking (VPN) technologies that are configured to force all of the organization's network traffic through key monitoring points, which is only somewhat effective in improving the situation, security controls often need to be heavily modified or even completely replaced. A common example is intrusion prevention systems (IPSs); it may be necessary to deploy many more network-based IPS sensors to monitor traffic while it is unencrypted, or even to reduce or eliminate use of network-based IPS in favor of host-based IPS that can monitor activity on individual hosts, including unencrypted network traffic being sent and received.

Few organizations, if any, can afford to suddenly build a completely new security infrastructure that addresses trends in mobility, cloud and encryption, as well as other ongoing changes in security. Therefore, security infrastructure changes tend to be gradual, replacing or upgrading one security technology at a time as budget and staffing allow. What is critically important is for security teams to be selecting and recommending acquisition of security technologies with the following three particular traits.

As threats continue to advance, having security technologies with these capabilities will become increasingly important, and eventually an absolute necessity, because they all improve security operations and reduce the frequency and impact of security incidents while also reducing the workload on the security team.

Key traits governing acquisition of security technologies:

- Automation, such as IPSs that can make sound decisions regarding attacks and block associated attack activity through automated means, such as terminating connections and disabling compromised accounts.
- Intelligence, such as SIEMs that can ingest threat intelligence feeds from well-qualified service providers to facilitate faster and more accurate detection of attacks.
- Integration, with the ultimate goal of enabling use of a single interface for managing all of the organization's security infrastructure technologies.

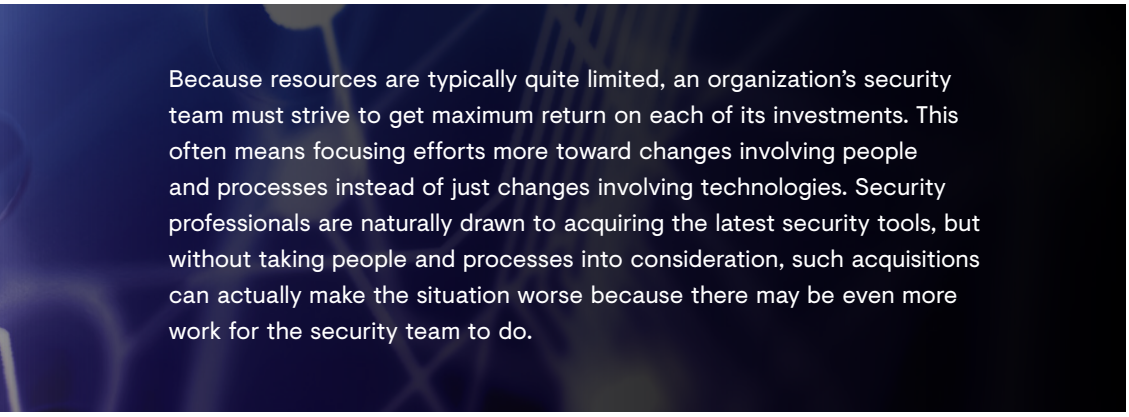
Partner with an MSSP to fill in the gaps.

Do not let pride get in the way of filling gaps in your security posture. In almost all cases, an organization's security team cannot possibly keep up with all of its designated responsibilities. Monitoring logs and IPSs, managing SIEM tools, performing incident response planning and keeping up with the latest threat intelligence, just to name a few, create an overwhelming amount of responsibilities that one organization does not have the expertise to handle. If security team members are willing to give up some of their duties and degree of control over security to an MSSP, they can be rewarded by a less chaotic and stressful environment where they can focus on designing and managing the core security infrastructure, providing security consulting services to users and departments and keeping current with the latest advances in security technologies. The use of an MSSP can help alleviate those day-to-day issues that consume so many resources. While you may be saying to yourself, it would cost money to use an MSSP, think of the internal resources freed up to focus on the strategic and operational issues that will lead to long-term improvements in your security posture.

Conclusion

Security professionals are under more pressure than ever to safeguard their organizations' sensitive data. They are given an incredible range of responsibilities with a limited amount of technologies, processes, staffing and support from upper management to successfully fulfill these responsibilities.

With limited resources at their disposal, security professionals need to be willing to make major changes to their responsibilities in order to be able to focus more of their time on strengthening the organization's overall security posture. Much of this improvement will be gradual, such as increasing the effectiveness of the organization's security technologies and incident response capabilities, as well as adopting and utilizing sound risk management practices, while some improvements may be achievable relatively quickly, including establishing relationships with MSSPs to fill capability gaps. Ultimately, all of these changes should lead to large reductions in data breaches and other compromises for the organization.



Because resources are typically quite limited, an organization's security team must strive to get maximum return on each of its investments. This often means focusing efforts more toward changes involving people and processes instead of just changes involving technologies. Security professionals are naturally drawn to acquiring the latest security tools, but without taking people and processes into consideration, such acquisitions can actually make the situation worse because there may be even more work for the security team to do.

Sources:

[1] PwC, *The Global State of Information Security®* Survey 2018.

[2] Ponemon Institute, *The Evolving Role of CISOs and Their Importance to the Business*, August 2017.

[3] Ponemon Institute, *The Evolving Role of CISOs and Their Importance to the Business*, August 2017.

Secureworks®

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp