Secureworks®

WHITE PAPER

Prioritizing Limited Resources on the Most Important Strategic Security Concerns

Many of today's security teams are challenged with moving from reactive to proactive approaches for handling risk.

While security budgets remain flat or, in some cases, are declining, organizations must mature their security posture through changes to people, process, and technology, and, at the same time, gain security buy-in throughout the organization. An organization attempting to advance along this reactive-proactive spectrum must make key strategic changes.

This paper examines the underlying challenges that need to be addressed by organizations, as well as guidance on low-resource methods for improving security strategy such as developing a security roadmap, leveraging multiple operational models and making security everyone's responsibility. By initiating these key strategies, an organization can make fundamental improvements to its entire security program.

Today's Strategic Security Concerns

The leaders responsible for overseeing and directing information security programs are already aware of the wide variety of constantly changing day-to-day security concerns that their organizations are facing. For them, it seems like there is always a new emergency for the staff to address, and a new headline in the news raising questions from upper management. All too often, this causes security leaders' efforts to be so consumed by tactical issues that they and their staff operate in a reactive mode instead of proactively addressing strategic concerns to achieve long-term improvements.

Therefore, it is critically important for leaders to identify and implement strategic security initiatives that help shift security risk handling from a reactive, tactical approach to a proactive approach. Tactical issues should not be ignored, but ensuring that strategic initiatives are still pursued will help alleviate tactical resource constraints over time. With a reactive approach, security is looked at as filling the tactical gaps, and spending resources accordingly. However, with a fully thought out strategic approach, achieving compliance and other security initiatives becomes much easier. A more strategic approach also reduces the need for quick tactical shifts to fill holes.

Although the root causes of less-than-optimal security are somewhat different for each organization, a few causes are common to most organizations. Carefully consider each of the following as potential opportunities for strengthening your organization's security posture.

Resource Utilization

It should come as no surprise that most organizations are understaffed when it comes to security professionals. Besides the obvious budgetary limitations and the general shortage of qualified people, there are also serious issues with roles and responsibilities. Because so many security team members are dedicated to handling daily operational issues, there are few resources, if any, available to perform security planning services, such as consulting with the organization's data and application owners and their support staff to ensure that new projects have appropriate security controls built in. An increase in upfront strategic security planning would help bring about a decrease in future security team resource utilization.

Alignment with Risk Management

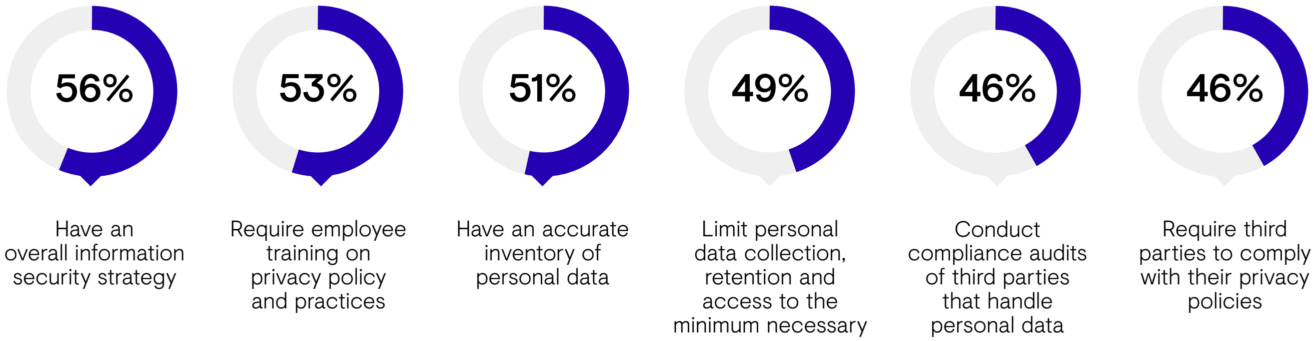
An organization's security capabilities, such as its management, operational, and technical security controls, should be the embodiment of the organization's risk management practices. Unfortunately, as a recent PWC report[1] indicated, one in ten respondents had not performed any risk assessments at all over the past two years and fewer than a third said their company performed risk assessments in the critical areas of anti-bribery and corruption, anti-money laundering, or sanctions and export controls. As a result, security capabilities are often not in alignment with the organization's risk management goals, which makes the security capabilities less effective and unnecessarily costly. Note, however, that not every organization needs to have the same security capabilities or the same level of security maturity; for more information on this, see the National Institute of Standards and Technology (NIST) Cybersecurity Framework[2] or the Capability Maturity Model Integration (CMMI) Institute[3].

Security Goal Definition

Many organizations do not formally define their goals for their information security efforts, and even those few organizations that do have formally defined goals may lack quantitative metrics for measuring their progress toward those goals. Without clear, quantifiable goals, different teams within the organization will each have their own definition of what success is when it comes to security. For example, the sales department might consider availability to be the most important attribute, and the financial office might look for less security-related spending, while the marketing department might be squarely focused on having no client data compromises. According to the 2018 Global State of Information Security Survey, even standard security goals are often not met. For instance, only about half of respondents have put key security measures in place, as reflected in the figure below.[4]

Many businesses are still beginners at data-use governance[5]

Only about half of respondents have put key measures in place

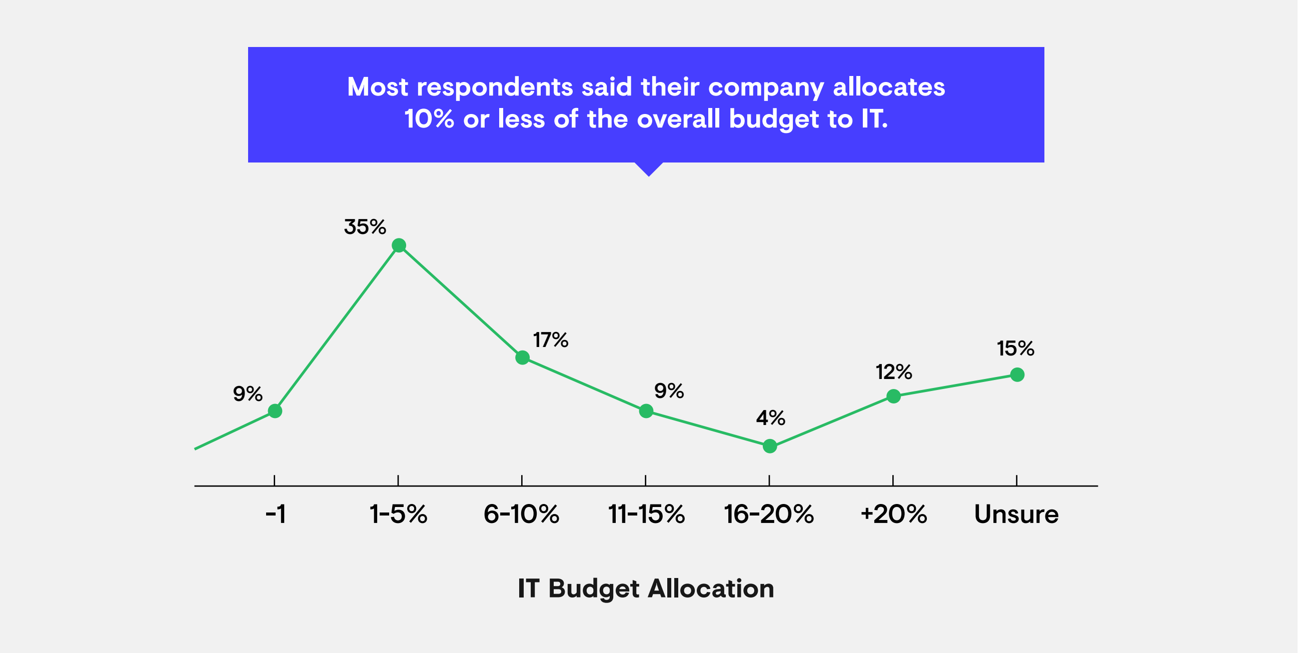


Security Responsibilities

Security has become the entire organization's responsibility, not just the responsibility of the security team. Without proper communication of security responsibilities for each part of the business and buy-in throughout an organization, the board of directors and executive teams will not allocate sufficient resources, and users, groups, and departments will not understand and follow their roles in organization-wide security responsibility. For most organizations, lack of buy-in to security responsibilities at all levels of the organization is the underlying cause of most or all of the organization's security issues. Perhaps even more alarming is that just 53 percent of organizations require employee training on privacy policy and procedures, as shown in the graphic above.

Recommendations for Addressing Strategic Security Concerns with Limited Resources

Identifying an organization's strategic security issues is one thing; determining how to best address those concerns is quite another. Every organization has limited resources for security, but often these resources are so limited that it seems as if it is simply impossible to achieve a reasonable security posture. As the figure below[6] indicates, most companies allocate less than 10 percent or less of their overall budget on IT. Nevertheless, every organization can take steps toward improving its security strategy to some degree regardless of budgetary constraints.



The key to addressing an organization's strategic security concerns with limited resources begins with clearly defining the organization's security goals. The subsequent program built to accomplish these goals must consider both risk management principles and compliance requirements. The program must also ensure that all people in the organization understand their security responsibilities and the reasoning behind them, because this can lead to a significant reduction in successful social engineering attacks against the organization, as well as incidents caused by common user violations of the organization's security policies.

It is important to set realistic expectations for addressing the organization's strategic security concerns. Some aspects of a fundamental all-in approach can be implemented fairly quickly, but most will take time. Phased approaches are often best so that there is time to optimize and there are not too many changes happening at any one time.

The following strategic approaches are highly recommended for most organizations that need to improve their security posture. These suggestions should consume relatively few resources, yet can generate large returns on investment by leading to significant improvements of an organization's security posture.

Develop a Security Roadmap

This roadmap is to be used for documenting the current state of the organization's security capabilities, and then planning how to mature those capabilities and how to enable measurement of the effectiveness of each capability. It is important to take an all-encompassing view of security capabilities; although many think of them as being synonymous with technologies, they also include people and processes. Simply implementing the latest and greatest technologies without the supporting people and processes in place will not help an organization, and, in fact, may harm it because of the resources it wastes. As stated in the recent Ponemon 2018 Study on Global Megatrends in Cybersecurity[7], 58 percent believe the problem of not having an expert cyber staff will worsen and 46 percent believe artificial intelligence will not reduce the need for experts in cybersecurity. So, when designing this roadmap, consider it from a people, process and technology standpoint and how they should work together to achieve those goals.

Leverage Multiple Operational Models as Appropriate

Organizations are often reluctant to entrust security operational functions to anyone other than their own security staff, but the limited scalability of such a centralized model is driving organizations to seek alternate operational models. For example, external entities, such as managed security service providers (MSSPs), can often operate particular security technologies on behalf of the organization, especially those that require continuous staffing. By establishing partnerships with external entities, an organization can significantly reduce its own costs, fill operational gaps and improve its security posture.

Make Security Everyone's Responsibility

As already mentioned, having a centralized model for security staffing is no longer sufficiently scalable for most organizations. Many people have already responded to the rather constricting nature of IT departments by acquiring and using their own IT solutions, forming what is known as shadow IT. Shadow IT has facilitated rapid innovation throughout organizations, but at the cost of security becoming an afterthought, if it's thought of at all. Centralized security teams are losing control of the organization's security. Organizations can respond to this in one of two ways: eradicate all shadow IT and force all major IT acquisitions to pass through the security team, or accept the existence of shadow IT and reframe the security team to be enablers of secure IT implementations throughout the organization. The latter approach makes the security team members trusted advisors on security matters to the rest of the organization, as well as the parties responsible for the organization's security infrastructure (except for what external partners may support, such as 24-hour security event monitoring). This approach only works if the organization has recognized and accepted that security is everyone's responsibility, not the security team's responsibility. It enables business units to make their own risk-based decisions, while also causing those business units to directly incur the costs associated with mitigating their risk.

Conclusion

Organizational security leaders who are taking a reactive approach and focusing on tactical issues are currently fighting a losing battle against attackers. The pressure to constantly address day-to-day security operations is overwhelming, so strategic security concerns are largely ignored, which means that, in the long run, attackers have even more of an advantage.

Given the limited resources and flat or declining security budgets, making the best use of those resources requires an organization to make key strategic changes such as developing a roadmap, leveraging multiple operational models and making security everyone's responsibility. Only by thinking and acting in long-term strategies can an organization hope to prevent most threats from succeeding and reduce the impact of the threats that are not stopped in time.

Sources:

[1] PWC, Pulling Fraud Out of the Shadows

[2] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity

[3] CMMI Institute

[4] PWC, Revitalizing Privacy and Trust in a Data-Driven World

[5] PwC, CIO and CSO, The Global State of Information Security® Survey 2018.

[6] ZDNet, Infographic: 2018 IT budgets are up slightly; spending focus is on security, hardware, and cloud

[7] Ponemon Institute, 2018 Study on Global Megatrends in Cybersecurity

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
UK House, 180 Oxford St
London W1D 1NN
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