MOVE TO A RISK-BASED SECURITY STRATEGY

Assessing and prioritizing risk can help organizations better protect their most important data and systems.

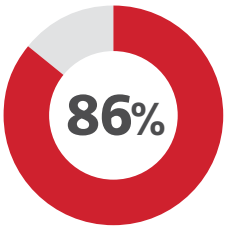
EXECUTIVE SUMMARY

Risk-based approaches to information security allow organizations to adopt strategies that are tailored to their unique operating environment, threat landscape and business objectives. Risk-based security strategies deliver value to an organization by allowing it to understand the impact of risk mitigation efforts, providing a comprehensive view of risk and filling gaps that may be left by other approaches to security. The use of a risk-based approach fits neatly within the enterprise risk management (ERM) strategies being adopted by many organizations.

Risk-based security strategies differ markedly from the approaches currently adopted by many organizations. Some organizations find themselves subject to strict regulatory requirements governing one or more areas of their operations, and they allow these regulations to drive their entire security strategy. This often leaves significant control gaps, as programs designed to satisfy compliance obligations often neglect areas not specifically addressed in the regulation. Other organizations take an ad hoc approach to security that implements controls on an as-needed basis, lacking a coherent strategy to bind them together. This approach also leads to significant gaps because the strategy was not designed in a holistic manner. Risk-based approaches allow organizations to carefully consider the policies, technology solutions and services that offer a well-rounded, defense-in-depth approach to cybersecurity issues.

A Risk-Based Approach to Security

Organizations approach cybersecurity from many different perspectives and, as a result, adopt different strategies for identifying and fulfilling security control objectives. Some organizations enter the security discussion with a focus on meeting a compliance obligation, while others begin a renewed security effort in the wake of a breach or after interest from a senior executive. These ad hoc approaches to cybersecurity often work in the short term to fill gaps and meet an immediate need, but they often fail to take a long-term strategic approach that leaves the organization well positioned to handle future threats. The fact is that organizations adopting these approaches to security often fail to follow any type of coherent strategy, leaving themselves vulnerable.



The percentage of security experts who feel that their organization's cybersecurity function does not fully meet their needs[1]

Compliance requirements drive the security programs at many organizations when technology and compliance teams scramble to meet legal, regulatory or contractual requirements. Obligations under the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) and other regulations often leave an organization implementing security controls in "check-the-box" mode. While this approach may lead to improved security, it fails to look at the operation in a comprehensive manner. Regulatory bodies have narrow scopes of interest, designing regulations specifically to protect the confidentiality of certain pieces of regulated information. While compliance with these regulations may be mandatory, it is usually not sufficient to protect an organization against cybersecurity risks.

A more effective option for organizations is to adopt a risk-based approach to security that performs a holistic assessment of the threats facing an organization and the vulnerabilities in its current operating environment. Risks occur when there is an intersection of an existing (or potential) vulnerability and an identified (or possible) threat. When performing a thorough cybersecurity risk assessment, organizations evaluate each possible risk and then assign it a risk score. These scores are based on a combination of the likelihood that a risk will materialize and the impact on the organization should the risk come to pass. This risk-based approach allows the organization to focus its efforts on the risks that are more significant to its operations.

A risk-based approach to security recognizes that risks do not fit into neat buckets of high and low. Instead, they fit along a spectrum ranging from risks that are so low that the organization may accept the risk without adverse impact, to those that are so severe they must be avoided at all costs. The vast majority of risks facing an organization lie somewhere between those two extremes, and the goal of a risk-based security program is to appropriately prioritize and mitigate those risks to an acceptable level.

Adopting a risk-based approach to information security requires the involvement of numerous stakeholders from throughout an organization. IT teams should not undertake such assessments in a vacuum, because security risk is more than just a technology risk; it's an operational risk as well. Risk mitigation decisions may have a serious impact on operations, and IT leaders often lack the context, subject matter expertise or scope of authority to make these decisions in isolation. Rather, they must engage other leaders in the conversation and create a forum for a comprehensive risk discussion. Organizations with mature approaches to ERM may already have an executive-level committee set up to discuss risks that come in diverse forms:

Another Option for Dealing with Risk: Insurance

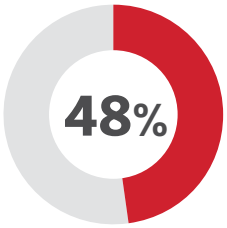
Cybersecurity programs traditionally approach risks in one of three ways: implementing controls to mitigate the risk, modifying business practices to avoid the risk, or accepting the current level of risk and continuing operations as they are. A fourth option exists that is growing in popularity among organizations: transferring the risk to someone else. This normally occurs through the purchase of a cyber liability insurance policy that protects the purchaser against the financial impact of a cybersecurity breach.

Insurance companies understand risk assessment better than perhaps any other industry. They've been writing policies for centuries based on actuarially sound risk assessments, and they bring those same practices to the world of cybersecurity. Before underwriting a policy, insurance companies will likely conduct a thorough risk assessment of an organization's cybersecurity environment. This assessment determines the maximum possible risk facing the organization based on the types of data that it handles, evaluates the effectiveness of existing security controls and recommends improvements that may be a condition of issuing the policy.

Source: [1]EY, "Path to cyber resilience: Sense, resist, react – EY's 19th Global Information Security Survey 2016-17," January 2017

financial, operational, reputational and strategic. Adding technical risk to that mix is an excellent way to elevate the conversation to an appropriate level.

The bottom line is that a risk-based security program must be very closely aligned with the goals of the organization. IT groups exist to facilitate the operations of the rest of the organization so that the entire operation succeeds. The technical decisions made within a security program may have a dramatic effect on the ability of the organization to achieve its goals, and a risk-based program must take this into account. Not all risks are technical. Strategic, operational and financial risks may justify accepting a higher level of technical risk than might seem otherwise appropriate. Balancing these considerations is an art that requires insightful qualitative analysis from a broad group of leaders.



The percentage of organizations that actively monitor and analyze information security intelligence [2]

Benefits of a Risk-Based Strategy

Risk-based security strategies bring several important benefits to organizations. First, they allow organizations to understand the value achieved from their security investments. Second, they provide the organization with a comprehensive view of risk. Finally, they fill in the gaps in an organization's security strategy, providing a robust, defense-in-depth approach to cybersecurity.

Security isn't cheap. In fact, 60 percent of healthcare organizations responding to a 2017 survey by the Healthcare Information and Management Systems Society reported spending at least 3 percent of their budgets on security, while 11 percent reported that they spent 10 percent or more of their budgets on this category of expense. If organizations are going to make such significant investments, leaders must understand the return on that investment. Risk-based approaches to security provide justification for specific security investments by allowing the organization to tie the investments directly to the risks that they mitigate and the value that this brings to the organization. In addition, risk-based approaches allow an organization to adapt to changes in the threat landscape, shifting the investment of time and money to areas that pose the greatest risk.

A risk-based approach to security also helps organizations adopt a broader risk-based approach to business. The concepts of risk management discussed in cybersecurity conversations apply equally to many other areas of an organization. These include other technology matters, such as disaster recovery and fault tolerance, as well as issues that do not involve technology, such as media relations and industrial compliance. Organizations that adopt an ERM-focused approach can apply the concepts implemented during a cybersecurity risk assessment to many other areas of their operations, addressing a wide variety of strategic, operational, reputational and financial risks.

Finally, a risk-based approach leads an organization toward a robust set of security controls that are designed to meet the specific business needs of the organization. Rather than blindly adopting a regulatory framework or industry standard, organizations can customize a set of controls to their unique technical and operational environment. Thorough risk analyses can provide the information required to adopt a defense-in-depth approach to cybersecurity. Such an approach uses overlapping controls to mitigate the most serious risks in a manner that is not dependent on any single control. In this way, organizations can provide themselves with a resilient level of protection that will continue to safeguard information and other IT assets even in the wake of a single control failure.

CISO for Hire

Smaller organizations may not be able to justify investing in a full-time CISO to lead their cybersecurity efforts because they simply don't have enough work to fill the plate of a highly skilled security leader. However, organizations of all sizes may still benefit from the security expertise of a seasoned professional. Some consulting firms now offer CISO consultation services. Organizations adopting this approach consult a CISO on a per-hour or per-project basis and obtain input on risk assessments, security architecture designs, policies and procedures, threat profiles and other issues requiring security expertise.

Common Elements of a Risk-Based Strategy

While each risk-based security strategy is tailored to the unique needs of a specific organization, there are still many common elements that exist across organizations. These come in the form of cybersecurity policies, technology solutions and services designed to help organizations manage cybersecurity risk.

Policy

Policy forms the cornerstone of every information security program. It sets out the guiding principles for cybersecurity efforts within an organization, formalizes the leadership support for those efforts and provides a justification for actions taken in the name of cybersecurity that might negatively affect other activities of the organization. In an organization adopting a risk-

Source: [2]PWC, "Strengthening digital society against cyber shocks," October 2017

based approach to security, policies should spell out the nature of the risk-based approach and describe how the organization expects to avoid, mitigate and accept cybersecurity risks.

Fortunately, cybersecurity policy is a well-established field, and organizations do not need to start writing from a blank slate. Many government agencies and other organizations publish their cybersecurity policies on the internet, and organizations are free to peruse them for ideas as they begin to shape their own policies. The SANS Institute offers a free library of policy templates that organizations may use as the basis for their own policy documents.

Organizations may also choose to base their policies on an established cybersecurity framework, such as the security standards published by the National Institute for Standards and Technology or the International Organization for Standardization (ISO). A firm wishing to adopt a standards-based approach to security may benefit from bringing in a third-party consultant to perform a gap analysis of its existing controls, identifying areas where there are significant deviations. This can then be used as the basis for a risk-prioritized approach to applying new controls that mitigate identified gaps.

Solutions

Years ago, organizations seeking to formalize their risk management processes had very little in the way of outside resources to assist them. Over the past decade, new tools emerged to assist with this work. These range from comprehensive governance, risk and compliance solutions to specialized tools designed to assist with risk assessment and mitigation.

GRC solutions help tie together three functions that often exist in different silos within an organization. Policies are the product of governance processes, which often occur at the highest levels of an organization. Risk assessments and mitigation take place either within the IT function or as part of a dedicated risk management group. Compliance activities may occur within the legal or regulatory function. Each of these activities is extremely important to managing the organization's overall risk exposure, but it is often difficult for them to share information. GRC solutions break down these walls by presenting each function with a function-specific view of important information, but allowing those views to draw from each other. For example, if internal auditors seek to determine the effectiveness of a security control at enforcing a policy objective, a GRC solution can help by linking security controls (risk management) to policy objectives (governance) and determining whether they are functioning properly (compliance).

Newer tools seek to dive deeper into risk management by leveraging artificial intelligence to help evaluate an organization's risk profile. These tools can assess an organization's internet footprint, previous data breaches and known security risks, and develop an independent risk score that can serve as a feedback loop for the risk assessment process. Other technologies deploy agents inside an organization's IT infrastructure that continuously report back configuration information. These agents assess deviations from a security baseline that may represent cybersecurity risks.

Services

Many organizations find themselves ill equipped to provide a full range of security services internally. They may address this situation by contracting with vendors who offer security services. For example, managed security service providers offer clients numerous security operations center capabilities on a contract basis. Organizations that are unable to staff their own SOC on a continuous basis can hire an MSSP to monitor their security infrastructure around the clock for anomalies. When the MSSP detects suspicious activity, it may either immediately execute a planned response or escalate the issue to the organization's own security team for resolution.

Organizations can also turn to service providers to assist with assessments of their internal infrastructure. Some MSSPs offer vulnerability scanning services that constantly monitor client networks for vulnerable systems and provide a remediation workflow that allows engineers to monitor the status of issue resolution. Other MSSPs provide penetration testing capabilities that use trained ethical hackers to probe an organization's defenses using the same tools leveraged by cybercriminals. These attacks provide valuable insight into an organization's security posture, allowing them to correct issues that pose a significant risk of exploitation.

Facing Risk: An Ongoing Challenge

Security threats are constantly changing, and an organization's priorities may shift over time as well. An effective risk-based security program must recognize the dynamic nature of both the threat landscape and an organization's operations. The program should be designed with a spirit of continuous improvement.

The most important way that organizations can prepare their security programs for change is by recognizing that risk assessment is an ongoing activity, rather than a project conducted every few years. Security leaders must stay informed about changes in the threat landscape as well as business operations, and they should update the risk assessment when those changes are significant. The process of updating a risk assessment may highlight new areas of concern or identify the need for additional controls or more detailed assessments.

Make the Move to Risk-Based Security

Organizations that currently approach security using an outdated ad hoc approach or a compliance focus will benefit from moving to a more comprehensive, risk-based approach. After conducting a thorough risk assessment, IT and business leaders come together to develop an approach to cybersecurity that appropriately balances security needs and business requirements. Security professionals then work to implement a set of controls that align with this business-focused security strategy and develop an ongoing approach to security monitoring. Organizations that decide to adopt this strategy will benefit from seeking broad leadership support, benchmarking with other organizations, and changing the mindset of technical staff and other users.

Seek Leadership Support

Risk-based security strategies are successful only if they enjoy broad support from an organization's leadership. If security is seen as an IT initiative, it risks being placed on the back burner by other leaders who consider it a distraction from more pressing matters. On the other hand, if the CEO and CIO show united support for the initiative and consistently describe its importance to managing risk, the program has a much higher likelihood of success. Most organizations do place responsibility and accountability for their cybersecurity efforts within the IT organization, but that does not preclude showing broad executive support. While cybersecurity might be a component of IT, security governance should embrace a risk-based approach that includes decision-making at the executive level.

At the same time, the CIO and other IT leaders should develop a network of other organizational leaders who speak the language of security and will contribute to a risk-based decision-making process. For example, if a security scan detects a critical issue in an internet-facing payment application that requires a 12-hour outage to correct, the security team will have a much easier time gaining the support of functional users if the CIO and CFO approach the organization together, explaining the importance of the outage and supporting the effort. If the IT department proposes the outage unilaterally, it would be far more likely to encounter resistance from the finance team.

Benchmark with Third Parties

IT leaders may also gain support for security initiatives by demonstrating that their proposals are not security overreach but, rather, represent industry best practices. There are several ways to convey this message to business leaders:

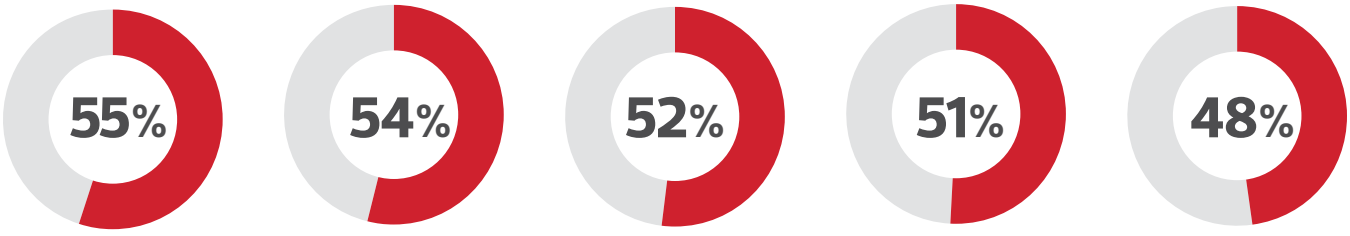
- **Benchmark with similar organizations:** If you can demonstrate that organizations in the same industry or similar lines of business are implementing controls that you lack, this lends credence to a project proposal. Organizational leaders will want to understand clearly why "everyone else" is implementing a particular control while they are not.
- **Reference industry standards:** Many industries have standards that address cybersecurity issues. The financial industry is familiar with PCI DSS. Healthcare organizations understand HIPAA. Manufacturers understand ISO guidelines. Security leaders who tie their requests to standards already familiar to organizational leaders improve their chances of success.
- **Bring in an independent consultant:** Organizational leaders, particularly boards of directors, tend to respond well to independent assessments of a wide range of issues. Even when IT leaders are confident of the appropriate direction for a security program, they may still gain credibility by receiving the endorsement of outside consultants for their plans.

Many different external resources exist that may ease an organization's transition to a risk-based information security program. Leaders who leverage benchmarking, industry standards and independent consultants will improve the likelihood of success for their programs.

Involve the Entire Organization

Risk-based approaches to security require the participation of a diverse set of individuals from across an organization. This is particularly true of technologists, who often view security as a silo within the IT department — a task for "someone else" who specializes in security. In today's operating environment, this couldn't be further from the truth. All technologists must be able to assume an attack mindset when they design,

IT security experts identified the threats and vulnerabilities that have most increased their risk exposure over the past 12 months:



Source: EY, "Path to cyber resilience: Sense, resist, react — EY's 19th Global Information Security Survey 2016-17," January 2017

implement or monitor IT systems. Adopting this mindset allows IT professionals to ask themselves important questions: If I were a hacker, how would I try to circumvent the system? How would I compromise the security of this environment? How could I exfiltrate sensitive information?

While technologists play a critical role in security programs, they're not the only participants. Defense-in-depth approaches to security require the involvement of an entire organization. All end users need to understand the significance of security and the role that they play in preventing outsiders from gaining access to buildings and networks. Without appropriate security training, helpful individuals may hold a door open for some burdened with a large load of paperwork rather than offering to hold the supplies while the individual swipes his or her badge. Unsuspecting users may give out seemingly innocuous information over the phone or online that may later be used to lend credibility to a social engineering attack against another employee. Risk-based security requires the full support of the entire organization.

CDW: A Security Partner That Gets IT

CDW's solution providers are available to serve as your organization's security partner. The CDW team offers a variety of security services that will help you improve your security posture. CDW's account managers and solution architects stand ready to assist you in every phase of your project. They will guide you through the selection and implementation of policies, solutions and services that will help your organization take a risk-based approach to security in today's sophisticated threat environment. CDW can assemble the resources required to help you successfully complete your implementation project.

CDW takes a comprehensive approach to identifying and meeting the needs of every customer. Each engagement includes five phases designed to help you achieve your security objectives in an efficient, effective manner. These phases include:

- Initial discovery session
- Assessment review
- Detailed manufacturer evaluations
- Procurement, configuration and deployment
- 24/7 telephone support

In addition to assisting with the design and implementation of security solutions, CDW staff are available to perform a wide range of security assessments.

The CDW Approach

ASSESS

Evaluate business objectives, technology environments, and processes; identify opportunities for performance improvements and cost savings.

DESIGN

Recommend relevant technologies and services, document technical architecture, deployment plans, "measures of success," budgets and timelines.

MANAGE

Proactively monitor systems to ensure technology is running as intended and provide support when and how you need it.

DEPLOY

Assist with product fulfillment, configuration, broad-scale implementation, integration and training.

To learn more about CDW's security solutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/threat

Explore Our Featured Partner

FIREEYE™

CDW® PEOPLE WHO GET IT™