MAD Security

8 BEST PRACTICES FOR MANAGING CYBER RISK

INSIDE THIS ISSUE

- Establish a robust risk management framework
- Invest in security training and awareness
- Implement a secure configuration management process

THE SUREFIRE GUIDE FOR STAYING AHEAD IN CYBERSECURITY PROTECTION

Here we highlight eight essential best practices for CISOs and their teams to effectively manage cyber risks.

TIPS AND EXAMPLES FOR A SECURE ORGANIZATION

Managing cyber risk must be a top priority for Chief Information Security Officers (CISOs) and their teams. With cyber threats constantly evolving, it's crucial to stay ahead by implementing proven best practices to safeguard sensitive data. In this blog post, we'll explore eight key strategies for managing cyber risk, complete with examples and tips to help you build a resilient security posture.

ESTABLISH A RISK MANAGEMENT FRAMEWORK

Establishing a robust risk management framework is one of the first steps to effectively managing cyber risk. This involves identifying assets, assessing risks, implementing mitigation strategies, and monitoring and reviewing the effectiveness of these strategies. A well-defined framework prioritizes resources and ensures security efforts align with the organization's overall risk appetite.

EXAMPLE

The NIST Cybersecurity Framework (CSF) is a widely recognized risk management framework organizations can use to identify, assess, and manage cyber risks.

By using the CSF, an organization can develop a comprehensive understanding of its risk landscape and prioritize security measures accordingly.

TIPS

Adapt the framework to suit your organization's size, industry, and specific needs. For instance, a defense industry-based organization should consider NIST, DFARS, and CMMC when assessing risks and implementing controls.

Involve stakeholders from different departments in the risk assessment process to ensure a holistic understanding of the organization's risk profile.

Regularly review and update the framework to accommodate changes in the threat landscape and business environment. This includes revisiting the risk assessment and making necessary adjustments to security controls.

MORE ON NIST

The NIST Cybersecurity Framework is a widely recognized risk management framework that organizations can use to identify, assess, and manage cyber risks.

Developed by the National Institute of Standards and Technology (NIST), the framework provides a comprehensive approach to cybersecurity that emphasizes risk management, situational awareness, and continuous improvement. The framework is based on five core functions: identify, protect, detect, respond, and recover.

DEVELOP AND MAINTAIN A COMPREHENSIVE SECURITY POLICY

A comprehensive security policy outlines the organization's commitment to information security and serves as a guide for employees and stakeholders. This policy should clearly define roles and responsibilities, acceptable use guidelines, and procedures for handling security incidents. You should regularly review and update the security policy to ensure it remains relevant in the face of evolving threats and changing regulations.

EXAMPLE

A well-structured security policy covers topics such as password requirements, mobile device usage, remote work guidelines, and incident reporting procedures. The policy should also outline the consequences of non-compliance, such as disciplinary actions or additional training requirements.

TIPS

Make the security policy easily accessible to employees and provide regular updates. Host the policy on the company intranet and incorporate it into onboarding materials for new hires. Your security policy can't be overcommunicated.

Assign a dedicated team to oversee policy enforcement and compliance. This team should regularly audit compliance with the policy and address any identified issues. The team must have the full support of upper management within the organization.

Align the security policy with industry standards, such as the NIST Cybersecurity Framework, and regulatory requirements like the Defense Federal Acquisition Regulation Supplement (DFARS) for organizations handling sensitive defense-related information.

IMPLEMENT A LAYERED DEFENSE STRATEGY

Defense-in-depth, or layered security, is a proactive approach to managing cyber risk that involves implementing multiple layers of security controls to protect against various types of threats.

This will include a combination of preventive, detective, and reactive measures such as firewalls, intrusion detection systems, encryption, and incident response plans.

EXAMPLE

A multi-layered defense strategy includes firewalls, intrusion detection systems, data encryption, and regular software updates.

For instance, deploying a web application firewall (WAF) will help to protect web applications from common attacks, such as SQL injection or cross-site scripting (XSS), in addition to the standard protections offered by a next-generation firewall enforcing network segmentation and authorized access.

TIPS

Continuously evaluate and update security controls to address emerging threats. For example, you should ensure that you use the latest encryption algorithms and technologies to protect sensitive data.

Implement real-time monitoring and alerting for potential security incidents. Security information and event management (SIEM) solutions help organizations aggregate and analyze security events from various sources, enabling faster detection and response.

Employ a managed security service provider (MSSP) for additional expertise and support, especially for small and medium-sized businesses that may lack the resources for a dedicated in-house security team.

INVEST IN SECURITY TRAINING AND AWARENESS

Human error is a leading cause of security breaches and data compromises. Regularly providing security awareness training will help employees recognize and avoid potential threats, such as phishing attacks and social engineering. Training should be tailored to the needs of specific organizational roles and updated to address emerging risks.

EXAMPLE

Phishing simulations are an effective way to assess employees' ability to recognize and report phishing attempts. By regularly exposing employees to simulated phishing emails, organizations can measure their susceptibility to these attacks and identify areas for improvement.

TIPS

Provide regular, role-specific security training for all employees. This should include general security awareness training for all employees, as well as more specialized training for employees with access to sensitive data or systems.

Deploy gamification techniques to make training engaging and interactive. For example, you can create security-themed quizzes, games, or competitions to motivate employees to learn about cybersecurity best practices.

Establish a clear communication channel for employees to report security concerns, such as a dedicated email address or hotline. Encourage employees to report any suspicious activity or incidents without fear of repercussions, as this will help identify potential threats early.

CONDUCT REGULAR VULNERABILITY ASSESSMENTS AND PENETRATION TESTS

Proactively identifying and addressing vulnerabilities is critical for managing cyber risk. Regularly conduct vulnerability assessments to discover weaknesses in your organization's systems, networks, and applications.

Complement these vulnerability assessments with penetration tests, which simulate real-world attacks to test the effectiveness of your security controls by exploiting them.

EXAMPLE

Vulnerability assessments will identify unpatched software, misconfigured systems, and other potential weaknesses that attackers could exploit.

Penetration tests, on the other hand, involve ethical hackers attempting to breach the organization's defenses to uncover vulnerabilities that may have been missed during the vulnerability assessment.

TIPS

Schedule vulnerability assessments and penetration tests at least annually or after significant changes to your IT environment, such as the introduction of new systems or major software updates.

Use a combination of automated tools and manual testing for comprehensive results. Automated tools can quickly scan large networks for known vulnerabilities, while manual testing can uncover more complex issues that may be missed by automated scans.

Address identified vulnerabilities promptly and verify their resolution. Implement a process for tracking and managing discovered vulnerabilities to ensure they are remediated promptly.

MONITOR AND MANAGE ACCESS

Implement a strict access control policy to ensure that only authorized individuals can access sensitive data and systems. Utilize the principle of least privilege, granting employees access to the minimum level of resources necessary to perform their job functions. Regularly review and update access permissions and implement multi-factor authentication for added security.

EXAMPLE

Implementing role-based access control (RBAC) helps ensure that employees have access only to the resources necessary for their job functions.

By defining specific roles and assigning permissions based on those roles, organizations can minimize the risk of unauthorized access to sensitive data.

TIPS

Regularly review and update access permissions to prevent unauthorized access, especially when employees change roles or leave the organization.

Implement an offboarding process that includes revoking access to all systems and applications.

Employ multi-factor authentication (MFA) for an additional layer of security. MFA requires users to provide multiple forms of verification, such as a password and a one-time code sent to their mobile device, before granting access to a system.

Monitor user activities for signs of potential insider threats or compromised accounts. User and entity behavior analytics (UEBA) solutions help detect anomalous behavior that may indicate a security incident.

CREATE AND TEST AN INCIDENT RESPONSE PLAN

Despite the best efforts to prevent security breaches, incidents can still occur. Develop a comprehensive incident response plan that outlines the steps to take when a breach is detected, including how to contain, mitigate, and recover from the incident. Regularly review and test the plan to ensure its effectiveness and keep stakeholders informed.

EXAMPLE

A well-defined incident response plan should outline roles and responsibilities, communication protocols, and steps for containment, eradication, and recovery.

The plan should be designed to minimize the impact of a security breach and ensure a swift return to normal operations.

TIPS

Conduct regular tabletop exercises to assess the effectiveness of your incident response plan. These exercises help identify gaps in the plan and provide valuable practice for the incident response team.

Establish clear escalation paths and decision-making authority during incidents. This can help ensure a coordinated response and prevent confusion or delays in addressing the incident.

After each exercise or incident, perform a post-incident review to identify lessons learned and improve the response plan. This review should include all stakeholders' input in the incident response process.

COLLABORATE AND SHARE THREAT INTELLIGENCE

Collaborating with industry peers, security researchers, and law enforcement agencies helps organizations stay informed about the latest threats and vulnerabilities.

Participate in threat intelligence sharing initiatives and integrate this information into your risk management processes to better protect your organization from emerging threats.

EXAMPLE

Joining industry-specific Information Sharing and Analysis Centers (ISACs) can help organizations stay informed about the latest threats and vulnerabilities.

ISACs facilitate sharing threat intelligence among members, enabling organizations to defend against emerging threats proactively.

TIPS

Actively participate in threat intelligence sharing initiatives and integrate this information into your risk management processes. Sharing information about security incidents and observed threats can help other organizations protect themselves and contribute to a more robust overall security posture within the industry.

Foster relationships with law enforcement agencies, security researchers, and industry peers. Building a network of trusted contacts can provide valuable insights and support during a security incident.

Establish a process for sharing threat intelligence within your organization. Ensure that relevant information is disseminated to the appropriate teams, such as the security operations center (SOC) or incident response team.

CONCLUSION

Effectively managing cyber risk requires a proactive, multi-faceted, continuously evolving approach to address emerging threats.

By implementing best practices such as robust risk management frameworks, layered defense strategies, and employee training, organizations can better protect their assets and reduce the likelihood of a successful cyberattack.

By staying vigilant and adapting to the evolving threat landscape, CISOs can foster a more secure and resilient organization.