PUBLICATION

Ten Best Practices to Protect Your Organization Against Cyber Threats

Authors: Alexander Frank Koskey, III, Matthew George White
November 04, 2024

The conclusion of Cybersecurity Awareness Month is a reminder of the importance for organizations to implement robust security measures and promote good cyber hygiene. As we noted in our State of the Cyber Landscape webinar, cyber threats are continually evolving with malicious actors exploiting new vulnerabilities and more sophisticated attacks each day. Organizations of all sizes must adopt comprehensive strategies to guard against these threats and mitigate the extensive operational, financial, reputational, and legal risk presented by such threats. Below are ten essential best practices that all organizations should implement as foundational components of their cybersecurity framework.

1. Review and Update Your Incident Response Plan

An organization's incident response plan is a critical document that outlines a step-by-step response to cybersecurity incidents. Its effectiveness lies in its clarity, timeliness, and adaptability to evolving threats. An outdated plan can lead to confusion, extended downtime, regulatory penalties, and significant reputational damage. As threats continue to evolve and new cyber reporting regulations become effective, organizations must review and update their plan to align with these evolving threats, new regulations, and any changes in the organization's processes and technology.

2. Conduct Tabletop Exercises

In conjunction with updating their incident response plan, organizations should test that plan with a tabletop exercise. A tabletop exercise is a simulated, scenario-based environment where key stakeholders across various departments are tested on how they would respond to a cyber incident in real time. These exercises are often facilitated by outside legal counsel and enable organizations to identify weaknesses, enhance coordination, and implement necessary updates to their incident response plan before an actual crisis occurs.

3. Implement Comprehensive Security Awareness Training

Human error is a major contributor to cyber incidents, with employees frequently targeted through phishing, social engineering, and other attacks designed to exploit gaps in awareness. Effective cybersecurity awareness for all employees, including executives and other management, empowers personnel to detect, avoid, and respond to these threats, reducing the organization's overall risk. Mandatory training programs tailored to the unique risks faced by organizations should be implemented to enhance relevance and retention.

4. Identify and Engage Key Third-Party Partners for Incident Response

In the event of a cyber incident, having pre-identified third-party experts can significantly enhance an organization's ability to respond quickly and effectively. Outside legal counsel, forensic investigators, and crisis communication firms, among others, bring specialized knowledge and resources essential for managing the multifaceted challenges of a cyber incident. Organizations should formulate partnerships with key vendors proactively in order to establish clear expectations, reduce administrative hurdles, and align third-party actions with the organization's response strategy. Special consideration should be given to structuring these relationships through outside legal counsel in order to preserve the attorney-client privilege. Having trusted third-party partners on standby enables organizations to address the legal, technical, and reputational aspects of cyber incidents swiftly and accelerates response and recovery efforts.

5. Prioritize Proactive Cyber Defense Measures and Controls

Proactive cyber defenses, including Multifactor Authentication (MFA), Endpoint Detection and Response (EDR), and Security Information and Event Management (SIEM) systems, are essential tools for preventing, detecting, and responding to threats in real time. While technical implementation may fall to IT teams, executives play a crucial role in prioritizing and supporting these investments. Understanding these core defenses enables leadership to make informed decisions, align cybersecurity initiatives with organizational goals, and champion a resilient security posture.

6. Focused Collaboration and Reporting on Cyber Issues

Establishing regular, collaborative reporting between IT, management, and other executive leaders is essential for aligning cybersecurity efforts with organizational goals. Executives should set a consistent reporting cadence where IT and information security teams share insights on key metrics, such as threat detection rates, response times, system vulnerabilities, and compliance with security policies. This collaborative approach fosters transparency and allows information security personnel to provide updates on emerging threats, new vulnerabilities, and the overall effectiveness of security defenses. This collaboration also allows organizations to consider financial support and updated budgets to fund additional tools that may assist in meeting evolving security needs.

7. Optimize Cyber Insurance Coverage

Cyber insurance is a critical component of a comprehensive risk management strategy, helping organizations manage financial exposure from cyber incidents, including ransomware attacks, regulatory violations, and litigation. Organizations should ensure that their cyber insurance policy is tailored to the organization's unique risk profile, offering adequate coverage for direct and indirect costs, including regulatory penalties, legal fees, business interruption, and reputational damage, and ensure that such coverage reflects the organization's evolving risk landscape. Optimizing cyber insurance coverage can protect organizations from the substantial financial and reputational impacts and ensure resilience in an increasingly complex threat environment.

8. Enhance Your Third-Party Risk Management Program

It's no secret that third-party vendors are prime targets for threat actors. One vendor compromise can potentially provide a gateway to the sensitive data and critical systems of all of their customers. Organizations must ensure that third-party relationships incorporate stringent security standards and continuous risk assessments to protect the organization's information assets. This includes assessing the vendor's security practices prior to onboarding, establishing contractual security obligations mandating that the vendor adhere to specific security controls, and implementing processes to monitor vendor compliance, conduct periodic reviews, and oversight of any changes in their security posture. This proactive approach enables organizations to identify and mitigate risks promptly and reduce exposure to external threats.

9. Evaluate Your Data Backup and Recovery Strategy

The continued proliferation of Ransomware-as-a-Service (RaaS) has resulted in more unpredictability and uncertainty in responding to ransomware attacks. Therefore, a resilient data backup and recovery strategy is indispensable for minimizing data loss, operational disruption, and costly downtime. An effective backup strategy safeguards critical data and enables swift restoration, ensuring that business operations can resume with minimal interruption. Practical steps may include investing in multiple backup locations to ensure data availability in case of localized disruptions, establishing frequent backup schedules with clear protocols for data encryption and access control, regulatory testing data recovery processes, and understanding the order of operations for bringing critical systems back online following an attack. A focused backup and recovery strategy allows organizations to quickly recover from cyber-attacks and maintain business continuity with minimal loss or impact.

10. Prioritize Risk Assessments and Audits

Identifying and addressing cybersecurity risks is essential for developing a resilient security program that aligns with organizational goals and compliance requirements. Regular risk assessments and cybersecurity audits provide a detailed understanding of potential vulnerabilities, enabling executives to make informed decisions about resource allocation, risk mitigation, and strategic priorities. Organizations would be wise to commission routine assessments, including vulnerability scans, penetration testing, and internal audits, to evaluate security measures across all systems, applications, and networks. This proactive approach helps reveal gaps that could otherwise remain undetected until exploited.

There is never a better time for executives and leadership teams to reflect on their organization's cybersecurity practices and strategic priorities. The best practices outlined above provide a framework for addressing cyber risks in a proactive, structured manner and enable organizations to be more resilient to cyber threats. Please contact Alexander F. Koskey, CIPP/US, CIPP/E, PCIP or Matthew G. White, CIPP/US, CIPP/E, CIPT, CIPM, PCIP if you'd like further guidance on implementing these strategies or would like to arrange a comprehensive cybersecurity review.