Crowe

Checklist

8 Critical cybersecurity best practices for internal auditors

Smart decisions. Lasting value.™

The Internal Audit Foundation and Crowe, in collaboration with The Institute of Internal Auditors' (IIA's) Audit Executive Center, conducted a limited survey of IIA members in order to gain insights into both the current and future role of internal audit in dealing with cybersecurity risk.

Based on the findings of that research and augmented by industry experience and observation, Crowe professionals have developed a checklist of top cybersecurity principles and strategies that today's leading internal audit groups are pursuing in order to help their organizations more effectively address cybersecurity concerns.

✓ Look beyond compliance

Many organizations focus their cybersecurity efforts on ensuring compliance with their industry's relevant information security standards, such as the Payment Card Industry Data Security Standard (PCI DSS) or *Health Insurance Portability and Accountability Act* (HIPAA) requirements. Such compliance is essential, but a truly effective cybersecurity program should take a broader and more holistic approach. Beyond regulatory or standards compliance alone, the goal should be to reduce or mitigate cybersecurity risk to a carefully determined level.

✓ Involve upper management

Upper management should take the lead in deciding an acceptable level of risk. Best-in-class organizations are those in which board members – and audit committee members in particular – are willing to ask probing questions about the organization's cybersecurity efforts. They need not be technical experts, but board members and senior executives should possess adequate understanding of both the risks and the available mitigation tools and techniques. Furthermore, they need to have enough knowledge to understand the high-level issues identified throughout the organization to gauge this risk.

✓ Manage relationships proactively

Many internal audit departments have more collaborative relationships with the compliance and risk management functions of their companies than with the IT or information security (InfoSec) departments. Industry experience confirms that the most difficult audits are those in which IT and InfoSec work to deflect internal audit away from areas of potential concern. The most effective audits are those that involve InfoSec and IT in the initial scoping meetings to help identify areas where internal audit resources can be used most effectively. Collaborative relationships help avoid overlapping and duplication of effort, while also improving the quality of the testing and reviews by all concerned.

✓ Acknowledge that cybersecurity extends beyond IT

Typically, IT departments handle initial responses to potential breaches, confirm the breach, asses its potential damages, and identify the areas at risk. Ultimately, however, an effective cybersecurity response involves numerous other responders, including disaster recovery, business continuity planning, incident response, legal, and compliance teams, as well as the affected lines of business. Internal audit must build relationships with all these teams to assess their understanding of cybersecurity risk and their roles.

✓ Prevent, detect, and respond

Cybersecurity professionals generally agree that breaches are no longer a matter of "if," but "when." Their attention has broadened from preventive controls to encompass detective controls that identify intrusions or malicious activity quickly, and response tools, which help minimize damage and expedite the return to normal operations. Reflecting this growth, an effective internal audit team must broaden its scope to identify ways that current audit activities such as penetration testing could be expanded to test the organization's detection and response capabilities.

✓ Create dynamic and risk-based audit plans

The scope of the annual audit should be dynamic, evolving, and responsive to the changing threat landscape. A first-year cybersecurity audit plan might focus on policies and procedures, patch management processes, and other foundational elements. But over time, the annual plan should expand in scope to reflect prior years' findings and to address newly identified areas of risk. This planning could involve the addition of more specialized assessments, such as vulnerability assessments rather than penetration testing alone. Here, again, a collaborative relationship with IT and InfoSec can help determine areas in which a broader scope could be most beneficial.

✓ Approach frameworks realistically

Popular cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Control Objectives for Information and Related Technologies (COBIT), often contain hundreds of individual controls, many of which might not be fully relevant to every organization. Obviously, there is no room for compromise when regulatory compliance or certifications such as PCI DSS, the Federal Deposit Insurance Corporation (FDIC) Information Technology Risk Examination (InTREx), or HIPAA are at stake. But when the use of a cybersecurity framework is voluntary, the internal audit function should approach such frameworks realistically and focus on those controls that are most applicable and material, considering each organization's profile and risk appetite.

✓ Develop and upgrade skills

Many audit executives recognize some persistent skills gaps in their departments, particularly in technical areas such as network design and administration and the development of critical technology applications. Recruiting new audit team members with the needed technical skills can be challenging and costly. In many instances, audit executives would do better by working to develop the needed skills internally through additional training of current employees. These employees' existing organizational knowledge can be invaluable, and the challenge of a "stretch" assignment can help ambitious employees looking for career growth opportunities.

Learn more

Christopher Wilkinson
Principal
+1 214 777 5288
christopher.wilkinson@crowe.com

crowe.com

Text created in and current as of February 2018; Cover and artwork updated in August 2021.

RISK-18000-002D