INTERNAL AUDIT'S ROLE IN CYBER PREPAREDNESS

THE IMPORTANCE OF A HOLISTIC APPROACH

Most organizations in today's cyber-threatened world focus their cybersecurity resources on prevention. Indeed, spending on IT security is forecast to reach $77 billion in 2015, an 8 percent increase from a year earlier, according to Gartner Inc., a leading global IT research and advisory company.

But it is shortsighted and potentially disastrous to focus solely on keeping cyber invaders out. Recent breaches in both large corporations and government agencies have illustrated an inability to stop attacks even when significant investments have been made in cyber defense. It's not a matter of if there will be a breach, but when. And that means organizations must create a holistic approach to cybersecurity to be truly prepared before, during, and after an attack.

A strong internal audit function that is sufficiently resourced and trained is one of the most important tools available to boards and audit committees as they craft and refine strategies, policies, and protocols to provide holistic protection to the organization from cyber threats.

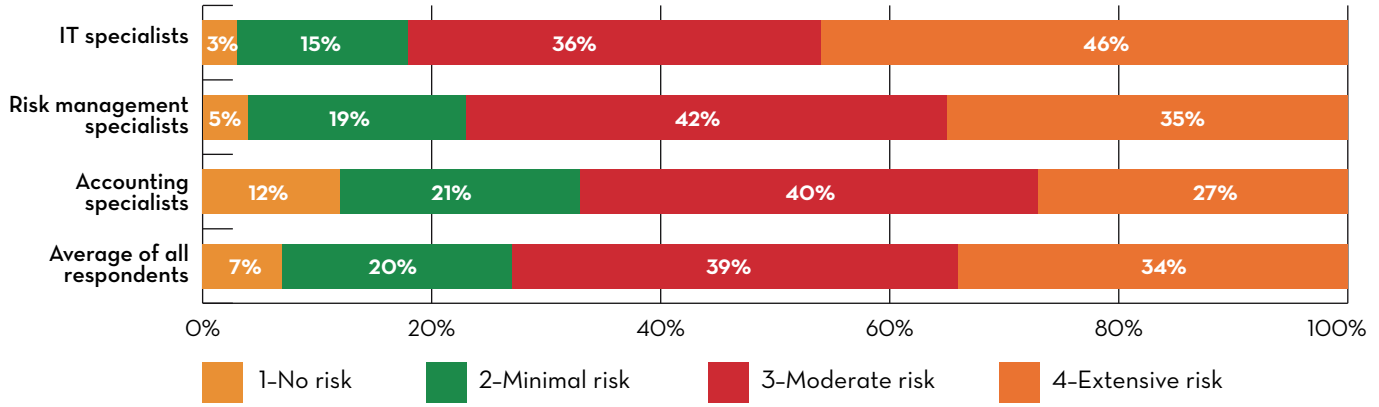
An effective internal audit function has the enterprise-wide perspective to help businesses anticipate, withstand, and recover from a cyberattack. In addition, its function as an independent assurance provider delivers the experience, skills, and knowledge needed to recognize the organization's cybersecurity strengths and weaknesses and to test and improve capabilities.

It's no surprise, then, that internal auditors already see a serious risk of cyberattacks harming their organizations. Seven in 10 who responded to The IIA Research Foundation's 2015 Global Internal Audit Common Body of Knowledge (CBOK) study estimated the inherent risk for data breaches that could damage their organization's brand as moderate or extensive (see exhibit 1).

"I don't think, based on my experience, that organizations have taken a holistic approach to cybersecurity," said James Reinhard, CPA, CIA, CISA, auditing director at Simon Property Group, Inc.

The Institute of Internal Auditors Research Foundation

Exhibit 1: Risk Levels for Data Breaches That Can Damage the Brand



Note: From the CBOK 2015 Global Internal Audit Practitioner Survey administered by The IIARF. Q93: In your opinion, what is the level of inherent risk at your organization for the following emerging information technology (IT) areas? All global respondents. Those who answered "not applicable/I don't know" were excluded from the calculations. Due to rounding, some totals may not equal 100%. n = 9,426.

Reinhard, who also teaches IT auditing, believes that chief audit executives (CAEs) are in a unique position to educate board and audit committee members about an organization's diverse efforts to battle cyber threats, including where chinks in the armor may exist.

"The challenge with cybersecurity is that it is an unknown risk, and boards and audit committees don't see it in the same way they see other risks that can create business disruptions," Reinhard said. "It's up to the CAE to possibly bring in the chief information officer (CIO) or someone from corporate communications to begin to build awareness about what's already being done within the organization."

Boards and audit committees also must, therefore, be kept up to date on technologies that not only can help meet business objectives, but also may make an organization more vulnerable to attack. When properly resourced and supported, internal audit will develop the skills and perspective to provide review and assurance services in this area.

> IT governance provides a foundation for IT to better manage its responsibilities and support of the organization through defined processes and roles/responsibilities of IT personnel. By having such formality in place, IT has the ability to better identify potential anomalies on a daily and trending basis, leading to root cause identification.
>
> *Source: GTAG 17: Auditing IT Governance* (Altamonte Springs, FL: The Institute of Internal Auditors, 2012), 5.

There are five key components crucial to cyber preparedness. Here's how internal audit can contribute to each one:

PROTECTION:
An ally to help keep the invaders out

Internal audit provides a holistic approach to identifying where an organization may be vulnerable. Whether testing bring your own device (BYOD) policies or reviewing third-party contracts for compliance with security protocols, internal audit offers valuable insight into protection efforts. Having effective IT governance also is crucial, and internal audit can provide assurance services for that area as well.

DETECTION:
Identifying tell-tale signs of breaches

Good data analytics often provide organizations the first hint that something is awry. Increasingly, internal audit is incorporating data analytics and other technology in its work. The 2015 CBOK practitioner survey found that five in 10 respondents use data mining and data analytics for risk and control monitoring, as well as fraud identification and more (see exhibit 2). CAEs should work with IT to develop and monitor key risk indicators and build strong professional relationships with the CIO and the chief information security officer (CISO) to ensure adequate and effective controls are in place.

BUSINESS CONTINUITY: **The show must go on**

Proper planning is important for dealing with and overcoming any number of risk scenarios that could impact an organization's ongoing operations, including a cyberattack, natural disaster, or succession. Ensuring that customers and other stakeholders are continuously served, no matter the circumstances, is essential to an organization's survival. Internal audit can provide assurance that plans are effective and efficient and have an enterprise-wide perspective.

CRISIS MANAGEMENT/ COMMUNICATIONS: **Don't panic**

Similar to business continuity planning, preparedness in crisis management and crisis communications can significantly and positively impact an organization's customers, shareholders, and brand reputation. Internal audit can help with plan development, provide assurance checks of its effectiveness and timeliness, and ultimately offer analysis and critiques after plans are executed.

CONTINUOUS IMPROVEMENT: **Sifting through the ashes of a cyber battle**

This is where internal audit may provide the most value, by contributing insight gleaned from its extensive scope of work. Cyber preparedness assumes survival of a cyberattack, but such victories are hollow if the organization does not evolve and improve its strategies and protocols to be better prepared for the next attack.

Ways in which the internal audit staff can maximize the business continuity plan:

1. Work with management to understand the plan and management's objectives.
2. Brainstorm ideas with management to continuously improve the process.
3. Help management provide a framework for making appropriate risk-mitigation decisions and building organization resilience.

Source: GTAG 10: Business Continuity Management (Altamonte Springs, FL: The Institute of Internal Auditors, 2008), 21.

CONCLUSION

Cyberattacks are woven into the new business reality, and new technology-driven risks will continue to emerge at ever-increasing speeds. Internal audit can play a number of important roles in helping an organization survive in a cyber-threatened world, including helping boards ask the right questions about cybersecurity. Only organizations that develop the skills to cope with these threats at strategic and tactical levels will survive and grow, and a strong, well-resourced, and supported internal audit function is an essential partner in this endeavor.

Exhibit 2: Use of Data Mining and Analytics

Note: From the CBOK 2015 Global Internal Audit Practitioner Survey administered by The IIARF. Q96: Does your internal audit department use data mining or data analytics for the following activities? All global respondents. *n* = 10,088.

QUICK POLL RESULTS
Survey of internal audit stakeholders

TONE *at the* TOP

Does your organization have a quick response team in place for damage control and remediation?

Yes	No	Don't Know
50%	32%	18%

A cyberattack is underway. How prepared is your organization to respond?

Extremely Prepared	5%
Very Prepared	24%
Moderately Prepared	44%
Slightly Prepared	19%
Not at All Prepared	8%

How confident are you that your organization's controls can prevent a significant cybersecurity threat?

34%	Little to No Confidence
54%	Somewhat Confident
12%	Very Confident

Source: Tone at the Top (Altamonte Springs, FL: The Institute of Internal Auditors, March/April 2014 and January/February 2015).

IMPROVING BOARD ACCESS TO CYBER EXPERTISE

Building up cyber or IT security expertise on boards is increasingly becoming a consideration for organizations. There is clearly a need for this. The National Association of Corporate Directors' Public Company Governance Survey found that fully 87 percent of respondents reported that their board's understanding of IT risk needed improvement.

Nominating and governance committees must balance many factors in filling board vacancies, including the need for industry expertise, financial knowledge, global experience, or other desired skill sets, depending on the company's strategic needs and circumstances.

Whether they choose to add a board member with specific expertise in the cyber arena, directors can take advantage of other ways to bring knowledgeable perspectives on cybersecurity matters into the boardroom, including:

- Scheduling "deep dive" briefings from third-party experts, including specialist cybersecurity firms, government agencies, industry associations, etc.
- Leveraging the board's existing independent advisors, such as external auditors and outside counsel, who will have a multi-client and industry-wide perspective on cyber-risk trends
- Participating in relevant director education programs, whether provided in-house or externally

Source: Cyber-Risk Oversight, Director's Handbook Series (Washington, DC: National Association of Corporate Directors, 2014), available at https://www.nacdonline.org/cyber.

8/20151543_CX