TONE at the TOP®

POWERED BY The Institute of Internal Auditors | Audit Executive Center

Issue 82 | June 2017

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics.

Insight That Internal Audit Brings to Cybersecurity Culture

The rapid spread of ransomware called WannaCrypt — swiftly dubbed #WannaCry on social media after it paralyzed an estimated 200,000 computers across Europe, Asia, and the Americas — has governance and risk management functions thinking more seriously about how they can strengthen cybersecurity controls. After so many years of often devastating cyber fails, why do organizations continue to be caught short when a new attack is launched?

These breaches may well be abetted unknowingly by organizations' cybersecurity cultures, wrote IIA President and CEO Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA, in a blog post shortly after #WannaCry swept the globe. "Providing assurance on cybersecurity involves more than just looking at whether the protocols and policies designed to block or discourage cyberattacks are in place and operating effectively," he wrote. "We must consider how the organization's culture influences how those protections are carried out."

One example of this is that some organizations may be willing to accept higher-risk behaviors in email practices in exchange for higher productivity. Another is how efforts to protect data through encryption can be undermined if rules prohibiting or limiting hard-copy versions of the data are not in place or are ignored. Chambers also offered caution about "IT mystique," where cybersecurity may be viewed as solely within the IT department's sphere and not open to questioning by other stakeholders.

Building cooperative relationships with IT, chief risk officers, chief information security officers, human resources, and others who manage cyber risks will help internal auditors strengthen their organization's cybersecurity culture. Otherwise, internal audit will not be able to gain a clear understanding of what drives cyber risks and what influences the organization's cybersecurity culture and share those insights with management and the board.

About The IIA

The Institute of Internal Auditors Inc. (IIA) is a global professional association with more than 190,000 members in more than 170 countries and territories. The IIA serves as the internal audit profession's chief advocate, international standard-setter, and principal researcher and educator.

The IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA

Complimentary Subscriptions

Visit **www.theiia.org/tone** to sign up for your complimentary subscription.

Reader Feedback

Send questions/comments to **tone@theiia.org.**

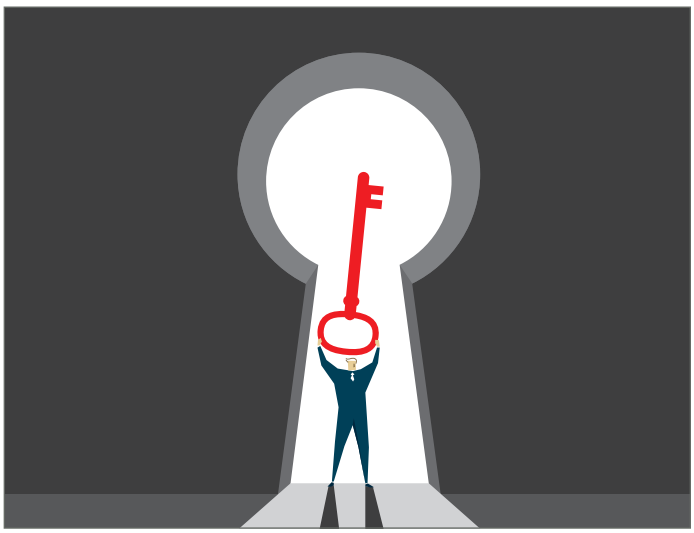
Content Advisory Council

With decades of senior management and corporate board experience, the following esteemed professionals provide direction on this publication's content:

Martin M. Coyne II

Michele J. Hooper

Kenton J. Sicchitano



Even security patches — the obvious fix that might have prevented #WannaCry's rampage — have a cultural component that goes beyond their narrow technology designation. Putting a patch in place to close a cybersecurity gap can be very complex because it is unclear what the impact will be on various operational systems without proper testing, said Doug Anderson, The IIA's managing director of CAE Solutions. "We cannot just blame IT on this one, or blame those overseeing IT. It is more complicated than that, because you are really trying to balance the cost and benefit in looking at a risk to an organization."

There are well-known barriers to internal audit's ability to address organizational culture. The IIA's 2016 North American Pulse of Internal Audit reported that 24 percent of those surveyed do not believe internal audit has the freedom to assess the entire organization and staff, while 35 percent do not believe they have executive management's full support to do so, and 23 percent believe they lack the full support of the board and audit committee to do so.

Earning a Seat at the Table

As long as senior management continues to see cybersecurity as IT's exclusive domain, the tendency to point fingers when a problem arises will persist. That impedes effective collaboration and makes it harder for a more cooperative cybersecurity culture to emerge.

"Internal audit is one of the few voices that is purposely positioned to go across the entire organization, and it is able to look at how the different parts work with each other and make sure the right information is getting to

the right people," Anderson says. The better internal audit does that, the more it will be asked to give input and be involved in strategic business planning, which should include decisions around cyber risks.

Earning an opportunity to influence the organization's overall risk-management culture also largely depends on how internal auditors understand their role. Those who believe their purpose is to identify and report problems will not get very far, says Jim Pelletier, The IIA's vice president of Professional and Stakeholder Relations. Recognizing they are in a position to help the organization achieve its objectives is a sign that a chief audit executive or an audit committee chair has an understanding of the organization's maturity level. This helps them better leverage internal audit's resources to positively impact the organization.

"That will permeate the culture, because the chief audit executive will earn trust over time by demonstrating he or she is not there to come in and slap you around, embarrass you a bit, and walk away," Pelletier says. The audit committee, in turn, is then less likely to use the information it gets from internal audit simply to punish management for failing to do something, he adds. There will still be situations where fraud or abuse occurs, which need to be handled separately, but "the day-to-day work should be to have a positive impact on the organization."

Boards and Audit Committees Need to Protect Internal Audit's Role in Cybersecurity

Frequent and proactive engagement on the part of the board of directors — especially the audit committee — is necessary for overseeing a successful cybersecurity program, according to Deloitte & Touche. "The audit committee chair can be a particularly effective liaison with other groups in enforcing and communicating expectations regarding security and risk mitigation," the 2015 report says. Deloitte also recommends recruiting directors with cybersecurity experience to serve on the audit committee so that informed decisions are made about the sufficiency of the efforts they are overseeing.

The board and the audit committee help internal audit preserve its independence, says Pelletier, by staying engaged in their oversight of the function. "In some situations, boards might say, 'Where was internal audit?' And my response is, 'Internal audit is where you put them,'" he says. It is up to the board and audit committee to ensure internal audit has an elevated standing that guarantees necessary access, and where "there is no fear or concern over what they are able to touch on. They are touching on the things the board finds to be the most important."

Shortly after the #WannaCry attack, The IIA's Audit Executive Center published tips clarifying what the board should expect from internal audit for optimal cyber risk protection:

- A careful evaluation of the organization's critical operational activities that identifies the supporting electronic infrastructure to ensure the scope of its cyber risk assessment is adequate. Instead of starting from a list of systems or protections already in place, start from critical business activities and tie them back into supporting infrastructure.
- A re-evaluation of the robustness of the risk assessment for cyber risks, ensuring it is geared toward considering all the inherent complexities and nuances of cyber risks rather than less difficult risks.
- A review of business continuity plans to ensure they cover all the various scenarios that can result from cyberattacks and that they address how the business will keep operating — not just whether the crown jewels are protected.
- Initiation of ethical hack routines to find vulnerabilities that a cyberattack could exploit. Faster changes in technology require this be done on an ongoing rather than a periodic basis only when an issue arises.
- A review of basic IT operations around patch management, which likely is already on the audit plan but needs to be accelerated given current events.
- A review of programs and efforts to keep employees well-trained and informed of their critical role in preventing cyberattacks from succeeding.

Shifting the Focus From Security Toward Resilience

The IIA's 2016 Pulse report highlighted the need to shift the focus from cybersecurity to cyber resiliency, given the growing consensus among experts that it is a matter of when, not if, a company will experience a cyberattack. Among the more than 90 percent of survey respondents who reported that their organizations have a business continuity plan, only 25 percent said the plan provided clear, specific procedures for responding to a cyberattack, with 17 percent of respondents reporting that their plans do not provide any procedures. If a business continuity plan lacks detailed procedures for responding to a cyberattack, the report recommends, internal audit should ensure that procedures are included elsewhere, such as in an incident response plan, which may or may not be linked to the business continuity plan.

Deloitte & Touche's report, Cybersecurity: The Changing Role of the Audit Committee and Internal Audit, cites resilience as one of the three core characteristics of a viable cybersecurity defense plan. The Center for Audit Quality also appears to agree that organizations need to be paying more attention to planning how they will respond to and rebound from an attack rather than focusing only on preventive measures.

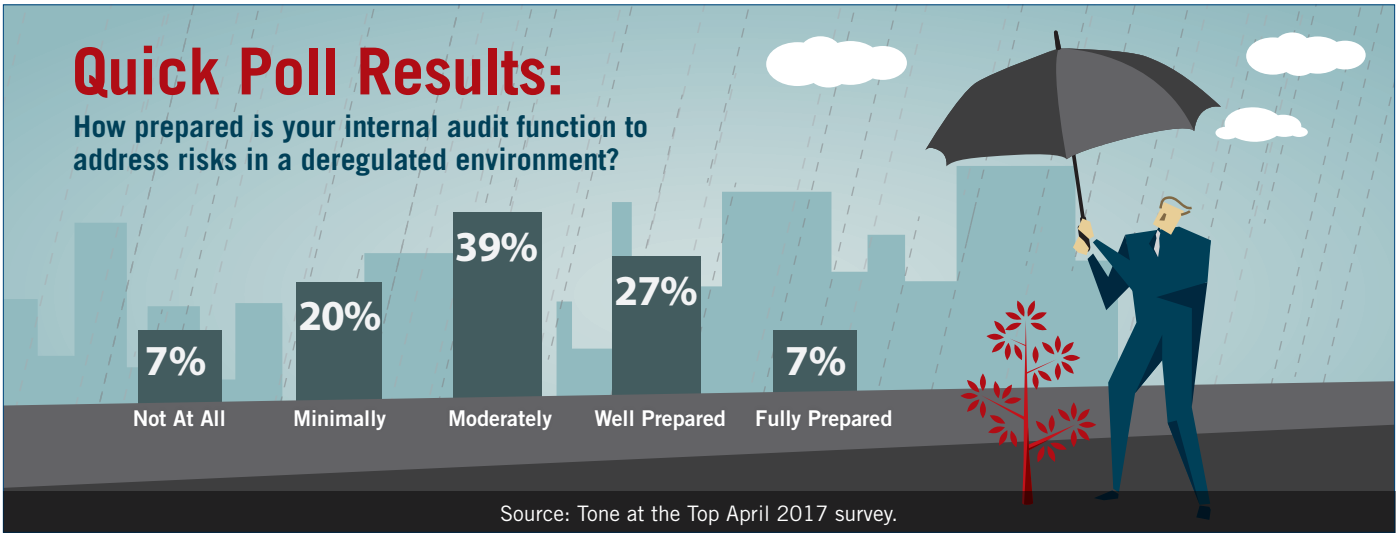
The CAQ whitepaper, The CPA's Role in Addressing Cybersecurity Risk: How the Auditing Profession Promotes Cybersecurity Resilience, due for release soon, will discuss how the auditor's role in cybersecurity can evolve.

Quick Poll Question

How well does your organization's culture positively influence its cyber resiliency?

Not at all | **Minimally** | **Moderately**
Extensively | **I don't know**

Visit **www.theiia.org/tone** to answer the question and learn how others are responding.



2017-0135