The Institute of Internal Auditors

TONE at the TOP®

Issue 70 | November/December 2014

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

Cybersecurity: They're In. Now What?

Almost daily, we see news accounts of hackers breaking through firewalls and stealing data from major corporations. Placed on the defensive, most companies respond similarly: An alarmed public is told of plans to rectify the situation and protect customers.

Then it happens again, in a vicious cycle of hack and protect, hack and protect, moving from company to company (and sometimes back again) like a shopper on Black Friday snatching up the best deals.

But the cold reality is that, for many organizations — perhaps most — it's no longer a matter of when the breach will occur. It likely already has. It just hasn't been discovered yet. Malware and other fraudulent programs can have delayed fuses, planted long before the bombs go off.

In a study by Verizon Enterprise Solutions that compiled data from 50 global organizations, researchers found that it takes cybercriminals only days to breach even the most sophisticated data defenses, but months can go by before detection. Indeed, MarketWatch recently reported that a survey by the security firm Trustwave found it takes companies an average of 114 days to detect and contain a breach.

Clearly, something must be done to close that gap.

The question is, what is the best line of defense — or offense? Legal counsel for only a third of Fortune 1000 companies say they feel their organizations are prepared to prevent a significant attack, according to a survey conducted for *InsideCounsel Magazine*. That leaves a tremendous amount of room for disaster.

Boards Hold the Key

"For a long time, there was an assumption (among a majority of corporate boards and executives) that the director of security had everything in hand," said Christopher Novak, managing principal of investigative response at Verizon. "Over the last year, we've seen that, whether they want to be involved or not, senior management and board members are being dragged in."

Protiviti's 2014 IT Security and Privacy Survey found board engagement to be a key differentiator in the strength of IT security profiles. Still, less than 15 percent of respondents to The Institute of

Internal Auditors' Audit Executive Center Pulse of the Profession 2014 survey said their boards were actively involved in cybersecurity preparedness.

How can board members prepare to engage? First, by understanding the multifaceted approach that experts recommend to manage cyberrisks. These include: perimeter protection with internal monitoring and a proven, practiced process for detecting intrusions; shutting them down quickly; and communicating with stakeholders in a timely and thoughtful manner.

"Front Gate" Measures

A good first line of defense includes controlled penetration testing, in which an organization pays a consultant to try to hack into protected systems.

Dominique Vincenti, chief audit executive at Nordstrom, calls this "building a Fort Knox," but it's a protect-the-perimeter strategy that she also warns can create a false sense of security.

Why? Because, while risk managers are watching the front gate, cybercriminals are sneaking in by tricking an employee, or even an executive, into giving them the key — emailed malware that the recipient opens, not realizing the danger within.

By slipping in, rather than storming the ramparts, hackers are often able to conduct their business undetected, stealing trade secrets, defense intelligence, or customer account information, sometimes for months or years before getting caught or disappearing into oblivion.

Rapid Response Plans

Beyond the vulnerabilities that allow a breach, "companies getting killed in the public eye are those that did not respond well" once the thieves were in, said Glyn Smith, CAE at Sabre Holdings. Experts say every organization needs a documented response plan and regular rehearsals that are part of a holistic crisis management strategy.

To assuage concerns by the board, management should present a plan overview that includes the directors' roles.

Smith says it's like a football play, which needs to be drilled to perfection before any coach would consider using it in a game. "If they've never practiced that play; if the quarterback has never thrown the ball in the heat of battle, it's not going to go well," Smith said.

Communication and Collaboration

In addition to top-down and bottom-up communication within an organization, Novak recommends that organizations work together within their industries to share information and protect each other's flanks.

"If some group is targeting one company in your industry, there's a good chance they're also targeting you," he said. Hackers "work together. Organizations need to work together to narrow the gap between compromise and detection."

What Now?

A recent report by The IIA Research Foundation and ISACA, titled "Cybersecurity: What the Board of Directors Needs to Ask," cited a report on cyberrisks published by the National Association of Corporate Directors (NACD), in conjunction with American International Group (AIG) and the Internet Security Alliance (ISA). NACD offers five oversight principles that corporate board members should follow to stay abreast of cybersecurity concerns and plan for a greater protective shield. Those five principals are:

1 Approach cybersecurity as an enterprisewide risk management issue, not just an IT concern.

2 Understand the legal implications of cyberrisks as they relate to the company's potential vulnerabilities.

3 Tap the organization's cybersecurity expertise and give management of cyberrisk issues regular and adequate time on the board's meeting agenda.

4 Set the expectation that management will establish an enterprisewide risk management framework with adequate staffing and budget.

5 Identify which risks to avoid, accept, mitigate, or transfer through insurance, and ensure discussion with management on specific plans associated with each approach.

A Checklist of Questions for Directors

- When was our last cybervulnerability assessment?
- What did we learn from it?
- If we are being attacked, how would we know?
- How would we react?
- Do we have a written response plan?
- Does it include a communications strategy?
- Have we rehearsed the plan as part of our crisis management and response activities?

Quick Poll Questions

1. A cyberattack is under way. How prepared is your organization to respond? (Scale of 1-5, with 1 being "extremely prepared" and 5 being "not at all prepared")
2. Does your organization have a quick-response team in place for damage control and remediation?

Visit **www.theiia.org/goto/quickpoll** to answer the questions and see how others are responding.

Beware of Malware

Why break in when you've got a key or access through a back door or open window? Hackers are skilled electronic pickpockets. You've probably heard of "phishing," a scam involving bogus email that, in some forms, infects employee computers with keystroke-tracking malware to capture passwords.

Here are two you might not have heard of:

Spear phishing: Targeted, phishing emails personalized to capture executive passwords. Based on the assumption that executives have higher security clearance, hackers will hone their emails using information drawn from social media profiles, news reports, and other publicly available sources to craft an email that appears to be a legitimate communication from some organization, or topic, of interest to the target. Once the email is opened, it works just like any other phishing attack.

Watering-hole attack: Indirect attacks in which self-loading malware and spyware are planted in lower-security websites, such as those set up by public utilities, country clubs, and churches, but frequented by executives of high-security companies. Again, the objective is to gain access to an executive's computer — in this case, by lying in wait on a less-secure server until the executive logs in and unknowingly uploads key-tracking software that will allow the hacker to capture passwords to secured information.

Source: Christopher Novak, Verizon Enterprise Solutions

About The IIA

The Institute of Internal Auditors Inc. (IIA) is a global professional association with 180,000 members in 190 countries. The IIA serves as the internal audit profession's chief advocate, international standard-setter, and principal researcher and educator. www.globaliia.org

Complimentary Subscriptions

Visit **www.globaliia.org/Tone-at-the-Top** or call +1-407-937-1111 to order 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
Nancy A. Eckl
Kenton J. Sicchitano

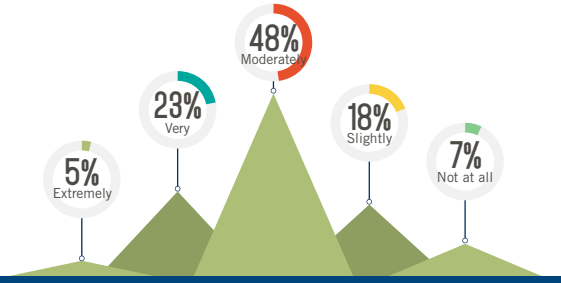
The Institute of Internal Auditors | TONE at the TOP®

NONPROFIT ORGANIZATION
U.S. POSTAGE
PAID
THE INSTITUTE OF
INTERNAL AUDITORS

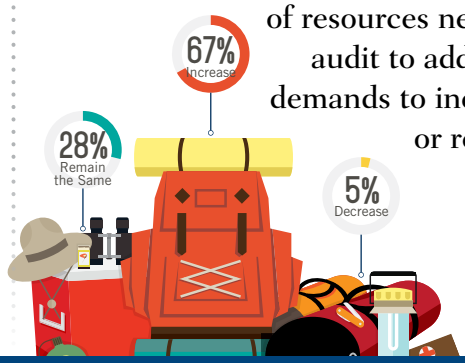
247 Maitland Ave.
Altamonte Springs, FL 32701-4201 USA

Quick Poll Results:

How confident are you that your organization is effectively balancing compliance demands with other strategic risks?



Over the next 3 years, do you expect the level of resources needed by internal audit to address compliance demands to increase, decrease, or remain the same?



Based on 352 respondents. Source: The Institute of Internal Auditors *Tone at the Top* August/September 2014 survey.