Issue 4

GLOBAL PERSPECTIVES AND INSIGHTS:

Internal Audit as Trusted Cyber Adviser

The Institute of Internal Auditors | Global

Contributors

City of Cape Town – *South Africa*
Lindiwe Ndaba, CIA, Chief Audit Executive
Etienne Postings, CIA, CCSA, CISA, Senior Audit Manager: Information Systems
Andre Stelzner, Director, Information Systems and Technology

FirstRand Ltd – *South Africa*
Jenitha John, CIA, QIAL, CA(SA), Chief Audit Executive

Insurance Australia Group Limited – *Australia*
Jeff Jacobs, Chief Information Security Officer
Lee Sullivan, Chief Audit Executive

RSM US LLP – *United States*
Daimon Geopfert, National Leader of Security and Privacy Services

Saudi Basic Industries Corporation (SABIC) – *Saudi Arabia*
Gregory Grocholski, CISA, Vice President, Chief Audit Executive

The Institute of Internal Auditors – *United States*
Greg Jaynes, CIA, CRMA, CFE, CGFM, Chief Audit Executive
Charles Redding, Executive Vice President and Chief Information Officer

Universidad de Los Andes – *Colombia*
Jeimy Cano, CFE, Cobit5 Foundation Certificate, Distinguished Professor, Law Faculty

University of Virginia – *United States*
Jason Belford, Chief Information Security Officer
Gerald Cannon, CISA, CRISC, Director of IT Audits
Virginia Evans, Chief Information Officer
Ron Hutchins, Vice President of IT
Carolyn Saint, CIA, CRMA, CPA, Chief Audit Executive

Table of Contents

Reader Feedback

Send questions or comments to **globalperspectives@theiia.org**.

Internal Audit as Trusted Cyber Adviser

While it would not be practical for someone to know *everything* about a topic as complex and fast-changing as cybersecurity, it has become essential for a chief audit executive (CAE) or head of internal audit to be cybersecurity-savvy. In fact, given the dynamic nature of the risks and exposures cyber presents, a well-informed CAE could position internal audit to be an organization's trusted adviser in this high-profile and challenging area.

The statistics are shocking:

> In 2015, the average total cost of a data breach was US$3.79 million, up from US$3.52 million in 2014 and a 23 percent increase since 2013. The cost reflects abnormal turnover of customers, increased customer acquisition activities, reputation losses, and diminished goodwill.[1]
>
> Attackers had access to the organizations' environments for an average of 205 days before they were discovered, and even then, 69 percent of victim organizations learned they were compromised not from their own staff, but from a third party.[2]
>
> In the first half of 2015, nearly 246 million records across 888 disclosed incidents were breached. In at least half of those disclosed incidents, the number of breached records could not be determined.[3]
>
> Breaches occur worldwide. In the first half of 2015, most occurred in North America (707 incidents), followed by the U.K. (94) and Asia (63). Five of the top 10 breaches, by number of data records compromised, were in non-U.S. firms.[4]

In the face of statistics such as these, it is no wonder that Amit Yoran, president of RSA, has stated, "The [cyber] security industry is failing. It has failed."[5]

[1] IBM and Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis*, based on a study of 350 companies from 11 countries.

[2] Mandiant, "M-Trends 2015: A View from the Front Lines," based on a distillation of Mandiant's incident response investigations in more than 30 industry sectors.

[3] Gemalto, Breach Level Index (BLI), a database that records all publicly reported global breaches.

[4] *Ibid.*

[5] Hackett, R.; "'Security Has Failed': Exclusive Preview of RSA President's Conference Preview," *Fortune*, April 21, 2015.

Yet no one doubts the importance of cybersecurity — the measures taken to protect data in internet-connected systems from loss, destruction, unauthorized access, or misuse. Many bright, level-headed people have focused on the issue for years. Their expectations are realistic: there is no widely held belief that cyberattacks can be eliminated entirely. As Jeimy Cano, distinguished professor in the Law Faculty of the Universidad de los Andes, notes, today's digital environment is imbued with the "inevitability of failure." Cybersecurity is a damage minimization game. The goal is to block as many attacks as possible and, in the inevitable instance when someone breaks through, find the attackers before they reach the "crown jewels."

A Team Effort

This is not a task solely for cybersecurity experts. Cybersecurity must be considered holistically and systemically, as the effects of failure can range from an inability to conduct basic transactions, to loss of intellectual property, to reputational damage. It is not solely a technology risk; it is a business risk and, as such, internal auditors have a critical role to play. Success in doing so is greatly dependent on the emphasis placed on the topic by the board or audit committee as well as the approach taken by the CAE. Cybersecurity offers a significant opportunity for CAEs to demonstrate their position as trusted advisers, going beyond simply ensuring that cybersecurity audits are executed according to plan, and instead offering anticipatory and strategic thought leadership to the business. This entails determining cybersecurity's risk and impact to business strategy and reputation; enabling timely and pointed discussions between management and senior officers; and championing the need for due care and resourcing of the same.

The CAE is also well served by establishing productive and highly collaborative relationships with the chief information officer (CIO) and chief information security officer (CISO). Such relationships can address the not-always-perfect understanding of what the security and IT teams want and need, and what internal audit can provide. According to Jenitha John, CAE for FirstRand Ltd, CISOs want an honest and proactive view from internal audit on current trends and topical, emerging issues that are prevalent in the environment — the proactive forward-looking view of a trusted adviser. She believes that internal audit needs to "articulate the issues in relation to the current exposure and impact facing the organization."

CIOs have needs that are similar to, yet distinct from, the needs of the CISO, according to Charles Redding, executive vice president and CIO of The IIA. He notes that CIOs tend to look at cybersecurity from the technical side. Internal audit broadens that perspective by providing the C-suite information that "helps us to evaluate the risk and define what the risk tolerance level should be." The internal audit function Redding refers to is headed by Greg Jaynes, The IIA's

CAE, who confirms the partnership between internal audit and the CIO: "When Charles and I are both in the office, not a day goes by that we don't talk about risk and cybersecurity. I don't see how CAEs can be effective if they are not fully engaged with their CIO."

Gregory Grocholski, vice president and CAE of Saudi Basic Industries Corporation (SABIC), agrees with the importance of team effort, but he points out that the CAE's role relative to cybersecurity goes quite a bit further than promoting partnerships within the organization. The CAE must understand that data exists in structured mode (developed applications) and unstructured mode (Excel, Word, etc.), each of which may be of interest to unwanted parties.

The CAE must be familiar with all the cyber pathways entering and exiting the organization, and ensure those pathways receive proper consideration at all levels of the organization relative to their necessity, appropriate controls, risk impacts, and risk tolerance. At all times, the CAE should be focused on anticipating, not just preparing to react.

Support From the Top

In virtually every organization, for every major project, buy-in from the top is critical. Yet boards have been reluctant to show full support for cybersecurity efforts. According to one recent study, 26 percent of the individuals surveyed indicated that their CISO or chief security officer (CSO) makes a security presentation to the board only once a year; roughly an equal number (28 percent) reported no presentations at all. Almost one-third said no board committees or members are engaged in cyber risk; only 15 percent indicated engagement in cyber risk by the audit committee.[6]

But the traditional reluctance to engage in cybersecurity seems to be fading. Boards are beginning to ask for more information on cybersecurity and related risks within their organization. This is not only because they have recognized the potential magnitude of damage that an attack can cause; regulatory pressures are also on the board's mind. In June 2014, Securities and Exchange Commission Commissioner Luis Aguilar announced, "Board oversight of cyber risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. …boards that choose to ignore or minimize the importance of cybersecurity oversight responsibility do so at their own peril."[7]

[6] PwC, "US cybersecurity: Progress stalled, Key findings from the 2015 US State of Cybercrime Survey," July 2015.

[7] Security Intelligence, "Why is Your Board of Directors Finally Asking about Cyber Risks?," October 13, 2015.

Boards, audit committees, and senior executives need information to perform their responsibilities effectively. Internal audit, with its privileged access to these groups, can help keep cybersecurity on their agenda. John believes the role of CAEs is clear: "CAEs must position audit findings appropriately at the right governance levels so they receive the requisite attention and then monitor and provide updates on remediation efforts." Lee Sullivan, CAE of Insurance Australia Group Limited (IAG), says his reporting provides the board "an independent view of the real state of IAG's cyber-threat readiness."

CAEs may find they can be most effective in their cybersecurity-related reporting responsibilities by focusing on trends in the industry, such as upcoming changes in regulation, new insurance coverage requirements, and new class action lawsuits, and how these trends are being used as a consideration in the scoping of internal audits. They may also wish to provide assurance that the appropriate people and teams — incident response teams and third parties performing risk assessments, for example — are in place to address cybersecurity specialties.

CAEs must also advise on current cybersecurity projects and whether these projects are effective in mitigating the risks being faced, make efficient use of resources to direct effort at the most important risks, and are robust and rigorous enough to prevent and detect threats. Carolyn Saint, CAE at the University of Virginia, notes that internal audit's involvement in cybersecurity projects can benefit management's efforts by amplifying the message about resourcing needs to the highest levels of the organization.

Related Issues

The challenges inherent in cybersecurity have surfaced a focus on cyber resiliency — activities undertaken before, during, and after incidents to render information and communications systems (and those who depend on them) resilient in the face of constant attacks on cyber-related resources. These activities include enhancing the cybersecurity knowledge and awareness of all employees, so that an organization's staff better understands the nature and impact of related risks and forms a stiffer front line of defense against cyberattacks. The CAE can lead the way through efforts to increase cybersecurity knowledge and awareness among internal audit staff. According to The IIA's 2016 North American Pulse of Internal Audit, a lack of cybersecurity expertise among internal audit staff is the biggest obstacle affecting internal audit's ability to address cybersecurity risk.[8]

[8] The IIA, "2016 North American Pulse of Internal Audit," February 2016.

Jason Belford, CISO of the University of Virginia, considers cyber resiliency a basic tenet of cybersecurity — addressed separately, but not as a major stand-alone effort. Ron Hutchins, vice president of IT at the university, agrees. "We aim for high availability and high reliability, but we also appreciate that not all services require the same level of protection."

Further, Andre Stelzner, director of information systems and technology for the City of Cape Town (Republic of South Africa), sums up the concept behind it neatly: "A cyber-resilient organization is one that knows how vulnerable it is." Clearly, the best way to be secure and resilient starts with knowing your vulnerabilities and the actions being taken to mitigate those vulnerabilities, and establishing plans for reacting to and recovering from cyberattacks.

Privacy and confidentiality, too, are key elements of cybersecurity in terms of what data is being handled, how it is stored, where is it being stored, and who is accessing it via which means. At Insurance Australia Group Limited, maintaining the trust of customers is so critical, the chief customer officer also engages with the privacy officer and the CISO to protect customer data. In many organizations, the privacy function also assists with defining the organization's relevant standards and developing policies and procedures; it is also often responsible for educating employees on cybersecurity issues.

Internal audit should view those responsible for privacy as key stakeholders, and compliance with privacy-related legislation should be a key element in all relevant audits. Inquiry into and observation of the privacy function can provide additional clues as to the strength of cybersecurity within the organization. The data owners, the technology owners, and the privacy/legal team should all be talking to each other and working together within the broader framework the organization is deploying. If they are not, it may be an issue worth investigating.

Conclusion

The views of CAEs and information technology/security executives are clear: cybersecurity is an issue that is not going away. It is, in Cano's view, "a new industrial revolution, and a new era of transformation dominated by the digital, the disruptive and resilient." Organizations that hope to avoid becoming yet another data breach statistic must ensure they acquire the appropriate expertise, fund their defense efforts, stay on top of pertinent regulation, follow global cyberattack trends, and engage all stakeholders in an unrelenting effort to combat the compromise or loss of data. No lesser effort will do.

Fulfilling the trusted adviser role, the CAE has a significant part to play in bringing about this outcome. The CAE fulfills this role by achieving and demonstrating cybersecurity expertise, developing trust, and using diplomacy and political awareness to ask the right questions of the right audiences at the right time. Does the company demonstrate a consistent philosophy relative to cybersecurity? Do the policies and procedures support the philosophy? What are other organizations doing and where do we stand in comparison? Questioning must be accompanied by active and attentive listening, followed by application of industry expertise, business acumen, and technological insights in pursuit of answers.

Success in cybersecurity requires the recognition there are people within the organization and outside the organization who will dedicate themselves to acquiring the company's data. They will not relent. Neither should the organizations they target. Grocholski's words form a well-suited mantra for the current reality: "We live in a digital world. Protect your assets like you would protect your home and family."

For More Information

International Organization for Standardization, "ISO/IEC 27001 – Information security management," 2013 (*www.iso.org*)

National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," February 2014 (*www.nist.gov*)

Privacy by Design, (*www.ipc.on.ca/english/Privacy/Introduction-to-PbD*)

The IIA, "Cybersecurity: Keeping IP Under Lock and Key," Tone at the Top, February 2014 (*www.globaliia.org/Tone-at-the-Top*)

The IIA, "The Cybersecurity Imperative," Internal Auditor, August 2015 (*https://iaonline.theiia.org*)

The IIA, "Logging In: Auditing Cybersecurity in an Unsecure World," 2016 (*www.theiia.org/AuditingCybersecurity*)

Exhibit 1

Effective CAEs Set Themselves Apart by Forming Advisory Relationships With Stakeholders

Insurance Australia Group

At Insurance Australia Group Limited (IAG), CISO Jeff Jacobs has overall accountability for the management of cybersecurity in the organization. To reduce IAG's exposure to cybersecurity risk, he works closely with CAE Lee Sullivan, the second-line risk function, and the team that focuses on privacy.

Sullivan and Jacobs recently collaborated on the creation of a cybersecurity strategy. Jacobs led the creation of the content for the strategy, which involved an assessment of current state capability, articulation of emerging risks, an outline of strategic imperatives, and a detailed road map and plan for dealing with these risks. Sullivan assigned a team to independently review the outcomes of the strategy soon after its development. They agreed to use the same cybersecurity framework to ensure consistency of language and messages to the executives and the board and collaborated throughout the review process.

Among the challenges addressed in the strategy are:

- The importance of getting the fundamentals right — The best example is a set of principles that will guide the organization as to what is acceptable or not from a cybersecurity perspective.
- The need to enhance detection and response rather than just focus on protection — Gone are the days of assuming that the organization can be protected by throwing money into protective tools. The truth, according to Jacobs, is that "we can never be totally protected so we need to become better at detecting and then responding if we have been breached."
- Ensuring cybersecurity by design — Too often cybersecurity is an afterthought. Designers and developers must build security into their solutions from the beginning.
- Cybersecurity awareness — Even if the best technology, processes, and experts are in place, the weakest link is always people. The challenge is to get them thinking about security so they are more aware of the dangers and can deal with threats appropriately.

There is agreement within IAG that the external threat is escalating and becoming more sophisticated every day and a sound cyber-threat framework is necessary to address it, but there is an acknowledgment that it is not always clear how much should be invested in uplifting the cyber capability when

compared to building out other parts of the strategy. There is the danger that some in the organization might be concerned that a focus on cybersecurity will slow down the planned digital transformation. Jacobs disagrees: "It is not a matter of either/or but rather how we must do both."

The University of Virginia

The University of Virginia team of Carolyn Saint, CAE, Virginia Evans, CIO, Jason Belford, CISO, Ron Hutchins, vice president of IT, and Gerald Cannon, director of IT audits, focus on what Hutchins describes as the "three-legged stool" approach to cybersecurity: set policy, implement policy, and audit compliance to policy. The key is for all the functions involved in each stage to be independent, but working together. As Evans notes, "The only way cybersecurity will work well is if we work as a team."

Saint takes a framework-driven approach to internal audit to deliver comprehensive and standardized coverage of cybersecurity efforts and to ensure that internal audit assesses for the effectiveness of controls, not just their existence. Evans confirms, "The previous audit team dealt entirely with compliance. Now we focus more on proactively finding risks."

Belford, Hutchins, and Evans also agree that the collaborative, consultative role internal audit now espouses is extremely beneficial. They see more of a partnership approach, a sense of being "on the same team" as opposed to the traditional internal audit reputation of, in Belford's words, "looking for ways to make you look bad."

Saint admits that raising awareness of internal audit's role and value in cybersecurity to the CIO and CISO is an education process, but considers that one of the CAE's responsibilities. She adds, "Part of the CAE's role is to ensure that risk is on the agenda at every level of the organization."

The university's current efforts to comply with the requirements of the U.S. Federal Information Security Management Act (FISMA) have united the team, along with other cross-functional representatives, over and above the usual cybersecurity efforts. Progress is being made, but the challenge of using a programmatic approach to build a scalable environment to meet the FISMA requirements is daunting.

Still, the combined effort must be made. As Saint points out, "Cyber is the top risk in every internal audit plan and probably will be for years to come."

City of Cape Town

The team at the City of Cape Town (Republic of South Africa) appreciates that technology will always move faster than mitigating controls, so there is a need to continue to invest in developing preventive, detective, and corrective measures. Even then, there is no guarantee of escaping attack, so success will depend on how quickly the team can detect a breach of security and how effectively, efficiently, and economically it can mitigate the threat.

The team consists of Lindiwe Ndaba, CAE, Etienne Postings, senior audit manager: information systems, and Andre Stelzner, director of information systems and technology. Their approach to cybersecurity is risk-based. The first consideration is to determine the type of IT risks identified within the organization by various sources or assurance providers. This is supplemented by a detailed discussion between IT audit and the CIO on cyber-risk trends within the organization, related risks outside organization, and global trends that may impact the organization.

Stelzner notes that achieving cybersecurity requires every member of the team to play to his or her strengths. For this reason, he believes that internal audit needs to be an independent assurance provider on the organization's security posture and review the policies, systems, and services put in place by the IT organization to mitigate the threat. He admits, though, that at this point, "We get this to an extent, but only to the level of evaluating adherence to IT's own policies rather than a brute force testing of security measures deployed."

The commitment to team effort is reflected in the close collaboration between internal audit and the security team. Internal audit attends the security forum meetings, where common issues are discussed and solutions formulated. Everyone is dedicated to the same goal: making tasks, systems, and processes as secure as possible.

Echoing Saint's comment on the importance of cybersecurity in internal audit's ongoing plans, Ndaba and Postings confirm that, at the City of Cape Town, "Cybersecurity and IT audit will always be an integral part of internal audit's strategic agenda."

Exhibit 2

Being a Trusted Cyber Adviser

As a trusted cyber adviser, the CAE is positioned to drive change in the organization. Focused effort in awareness and understanding, risk management, and assurance activities can help CAEs progress toward being trusted cyber advisers.

	BEING A TRUSTED CYBER ADVISER IS MORE THAN…	IT ALSO IS…
AWARENESS AND UNDERSTANDING	Understanding the concepts, workings, and elements of cybersecurity.	❑ Expanding current IT audit capabilities to provide proactive, actionable insights on cybersecurity. ❑ Maintaining a strong working knowledge of upcoming changes in regulation, new insurance coverage requirements, new class-action lawsuits, and other trends. ❑ Ensuring that audit programs consider these trends.
	Collaborating with appropriate functions within the organization to address cyber awareness.	❑ Providing strategic advice to functional leaders regarding their cyber roles and responsibilities.
	Relying solely on IT staff to provide cybersecurity expertise to the organization.	❑ Ensuring cybersecurity competencies for the CAE and staff through effective talent management/ professional development programs. ❑ Strategically leveraging co-sourcing to ensure the right talent and competence is available as needed.
RISK MANAGEMENT	Conducting a risk assessment to determine the likelihood of cyber risks and their potential impact on the organization.	❑ Staying abreast with the frequency and magnitude of cybersecurity lapses. ❑ Understanding the full impact of cyber threats on the organization and embedding this in the audit plan. ❑ Proactively identifying emerging cybersecurity risks.
	Being aware of how the organization addresses cybersecurity and the actions management has taken to mitigate related risks.	❑ Understanding the organization's risk posture to combat cyber threats. ❑ Performing continuous auditing on management's cybersecurity controls to test adequacy and effectiveness.
	Reviewing third-party audit reports.	❑ Partnering with the CIO/CISO to assess third-party candidates. ❑ Contributing to third-party candidate risk profiles. ❑ Advising on third-party compatibility with the cybersecurity strategy/philosophy.

	BEING A TRUSTED CYBER ADVISER IS MORE THAN…	IT ALSO IS…
ASSURANCE	Assessing compliance with cyber-related policies and procedures.	❑ Providing an independent review of the cybersecurity strategy before the policies and procedures are developed. ❑ Being part of technology project implementation teams to ensure cyber risks are addressed and built-in, rather than added on later. ❑ Benchmarking and testing the adequacy and effectiveness of policies and procedures against applicable frameworks.
	Assessing compliance with employee cybersecurity training requirements.	❑ Evaluating training outcomes and knowledge retention. ❑ Providing insights on how to align training with the cybersecurity strategy.
	Providing assurance on the organization's cybersecurity program.	❑ Leveraging internal audit capabilities with existing bench strength in first and second lines of defense while maintaining objectivity. ❑ Leading collaborative cybersecurity efforts among the three lines of defense.
	Providing assurance on incident response, disaster recovery, and business continuity plans.	❑ Providing insights on the coordination of plans and alignment with business strategy. ❑ As appropriate, preparing for internal audit staff to be able to step in and help wherever needed during a crisis.
	Reporting cybersecurity-related engagement results to management and the board/audit committee.	❑ Engaging management and the board/audit committee in forward-looking discussions, helping them to think through the cyber vulnerabilities facing the organization. ❑ Advising on or facilitating a process for establishing the organization's cybersecurity risk appetite.

2016-0637

globaliia.org