Fortifying for the future

Insights from the 2014 IBM Chief Information Security Officer Assessment

IBM **Center for Applied Insights**
ibm.com/ibmcai | **ibmcai.com**

They say that the future is limitless. For information security leaders, that might be a scary thought. Already tasked with protecting companies from a multitude of ever-changing threats, they must now prepare for not only more avenues of attack but also more sophisticated attackers as well.

Our research pinpoints what worries today's security leaders and what they can do to manage the approaching uncertainties.

In the world of IT, the role of watchman is becoming increasingly difficult. Computing innovation speeds forward, producing new technologies that, while impressive and impactful, often expand the defensive responsibilities of security leaders. For all the excitement surrounding the growing power of mobile, cloud and big data, equivalent diligence must be dedicated toward their security. And that's not to mention the existing challenges, such as managing IT risk, dealing with regulation and compliance, and collaborating effectively.

Success is far from assured – how many times this year alone did the news recount data breaches or information security breakdowns? Even as today's Chief Information Security Officers (CISOs) try to illuminate various threats to their enterprises, they themselves are under an intense spotlight.

The IBM Center for Applied Insights' 2012 CISO Assessment, the first in this series, established three archetypes for security leaders – the Responder, the Protector and the Influencer – and began to explore their characteristics. A year later, the 2013 CISO Assessment provided practical steps to help security leaders to reach the position of Influencer, and demonstrated how that transition could set a new standard for security leadership.

About the study

To obtain an understanding of security leaders' current conditions and views of the future landscape, the IBM Center for Applied Insights, in collaboration with IBM Security, conducted in-depth interviews with 138 security leaders – the senior-most IT and line-of-business executives responsible for information security in their organizations. Some of these leaders carried the title of Chief Information Security Officer, but given the diversity of organizational structures, some did not. Others interviewed included CIOs, VPs of IT Security and Security Directors. Sixty-three percent of organizations interviewed had a named CISO. Participation spanned a broad range of industries and five different countries.

The 2014 edition of the CISO Assessment evaluates the current state of security leadership and what leaders expect to face in the next three to five years. Security leaders are in the midst of an evolution. Driven by the specter of external attacks and the needs of their own organizations, they are continuing the shift toward a business leadership role that focuses on risk management and taking a more integrated and systemic approach.

What is the next stage in the evolution of security leadership? With their plates already full, what can security leaders do to strengthen their preparations and improve their foresight?

Key themes

1 Rising over a transformed landscape

2 Worrying a lot about external threats

3 Expecting more external collaboration

4 Still focusing on today's technology

5 Uncertain about government action

Rising over a transformed landscape

Security leaders and their organizations are seeing dramatic shifts in the surrounding landscape: 82 percent of respondents said that the very definition of security had changed in the last three years. Companies aren't merely polishing the details of their security policies, they're reconsidering entire strategies to account for the expansion of data, devices, user needs and overall importance of security at every business junction.

With this transformation comes a corresponding growth in the role of CISOs and the like. While in past years, many security professionals aspired to be strategic influencers, 61 percent of this year's respondents categorized themselves as such. In addition, 64 percent rated their documented enterprise-wide security strategy as very mature. This shift is evidence of the maturing role of security leaders within their ever-more aware organizations.

This expanding authority is not based on a speculative need. Security leaders will have to use their influence to manage a broader array of external threats and higher expectations across the business. A more extensive scope of what requires protection (e.g., cloud, mobile, etc.) and new security technologies also contributed to this trend toward increased complexity. CISOs are no longer stewards of security technology but rather decision makers who must always take business operations into account. Security leaders are obtaining more clout and wielding it to contribute to companies' broader goals while managing risk at every step along the way.

Gaining more influence and support

Influence

90%	Strongly agree that they have significant influence in their organization
76%	Say that their degree of influence has significantly increased in the last three years

Organizational support

71%	Strongly agree they are receiving the organizational support they need

Internal collaboration

82%	Participate in strategic/C-suite meetings quarterly or more frequently
62%	Develop their security strategy in conjunction with other strategies (primarily IT, risk and operations)

Figure 1. This growing maturity and influence is needed to address the more challenging external threat landscape.

CISO perspective: A higher profile for tougher challenges

By Jonathan Klein
CISO, Broadridge Financial Solutions

My profile as a CISO has increased in recent years. I have more influence and regularly meet with members of the C-Suite and other senior executives. But because information security continues to grow more complex, there are still many challenges – so my overall responsibilities and capabilities need to keep pace. Broadridge provides a range of technology and processing services for financial institutions. In this role, we handle one of our clients' most valued assets: customer information.

One of the biggest challenges companies face today is integrating security technology with the appropriate business processes. New technologies are often promised to solve the latest security threat, but they are ineffective if not properly integrated with business processes. I engage Broadridge's executives to integrate security and risk considerations into the early stages of their business decisions and ensure that security technology not only protects our organization, but also evolves with our business processes and policies.

For example, there are a variety of data standards that are supposed to be airtight. Companies too often expect that compliance with these standards ensures that sensitive information will be secure through the entire data lifecycle without supplementary measures. This has proven to be a dangerous assumption, as many high profile data breaches have demonstrated. At Broadridge, we focus on securing the data we process and not just fulfilling a checkbox in a compliance standard.

The consumerization of IT creates complications as well. There's no longer a clear distinction between personal and professional use of devices and applications. This often leads to public access of technologies originally designed to be private. It also causes security to lag behind new technologies that are rapidly adopted by consumers. More focus is placed on new features rather than security, making it difficult for companies to adopt these new technologies quickly while also evaluating their full security implications.

Ensuring that security is a cornerstone and not a finishing touch will be a key imperative of the growing influence of the CISO role.

Worrying a lot about external threats

Increased maturity and influence is essential in light of the challenge posed by advanced persistent threats, criminal enterprises, state-sponsored hackers, hacktivists and other cyber criminals. This threat is considered *so* great by both security leaders and their organizations that many feel they are losing the fight. Close to 60 percent of security leaders interviewed said that the sophistication of attackers was outstripping the sophistication of their organization's defenses. More than 80 percent of security leaders have seen the external threat increase in the past three years, and it is viewed as the top current challenge. Moreover, the focus on the external threat won't subside in the future, as half of leaders interviewed said that it will require the most organizational effort to address over the next three to five years.

The foremost challenge

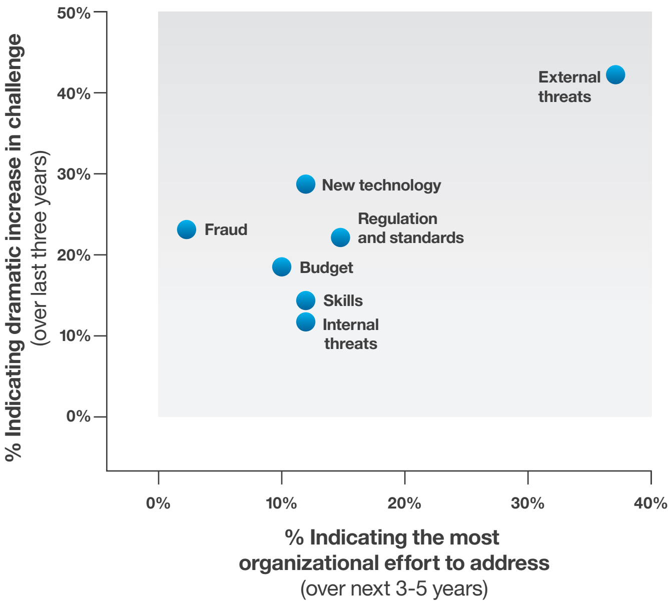


Figure 2. Security leaders will continue to focus on external threats for the foreseeable future, working to diminish the risk.

CISO perspective: Improving security strategies through collaboration

By John Taylor
Former Global Head of IT Security, British American Tobacco

External collaboration gives security leaders a chance to observe industry practices and evolve with their peers – to better understand where the "good stuff" is happening. In addition, it enables the formulization of ideas that can be used within your own environment. At British American Tobacco, we employed a variety of collaborative measures – formal and informal – to make sure we were practicing sufficient networking.

Our strongest relationships were with industry colleagues, followed by suppliers and partners, with governments bringing up the rear. I would send team members to global advisory boards and invite experts in to lead discussions, but I also gathered insights from casual dinners or discussions over coffee. The aim was to gather ideas and understand what people were seeing as emerging challenges or threats. It might seem slightly paradoxical, but as privacy and data retention become more difficult, the key to being more secure is being more open.

However, one still must reserve a healthy dose of cynicism about which groups to join or create, since having too many of them will dilute the purpose and reduce value. We need to support only the more effective groups, and make sure they have a 360-degree view of potential risks.

For collaboration to evolve, some groups need to be exclusively security professionals, but others have to be supported by member organizations, end suppliers and partners. CIOs need to also be included in the broader groups, not just security leaders. When it comes to collaboration, we in manufacturing can look to more experienced industries for guidance. The banking sector has always gone to great lengths to share information (particularly threat information) to help protect its large volume of private information and financial assets, creating a model that other industries should aspire to.

The reality of today's expansive threat landscape is that we can't fully protect everything. Other firms face the same challenge, so hearing the perspectives of my peers helps to improve our strategies around our most sensitive information.

Expecting more external collaboration

As the information security boundary of organizations expands, blends and disappears, security leaders will increasingly need to secure entire ecosystems instead of just their own organizations. Protection through isolation is less and less realistic in today's world: 62 percent of security leaders strongly agreed that the risk level to their organization was increasing due to the number of interactions and connections with customers, suppliers and partners. But despite the widespread interconnectivity that drives modern business, security leaders themselves aren't sufficiently collaborative. Currently, only 42 percent of organizations that we interviewed are members of a formal industry-related security group. However, 86 percent think those groups will become more necessary in the next three to five years.

Sharing threat information

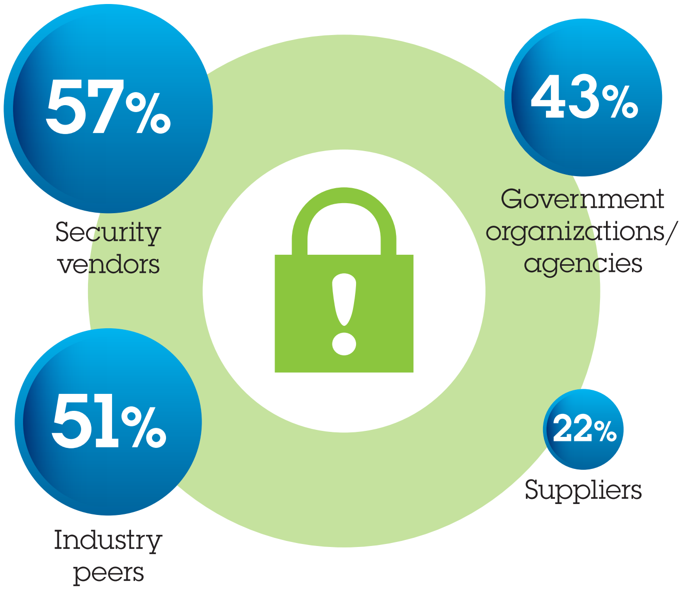


Figure 3. To reduce the risk from tighter connections with customers, suppliers and partners, a "secure the ecosystem" approach is warranted.

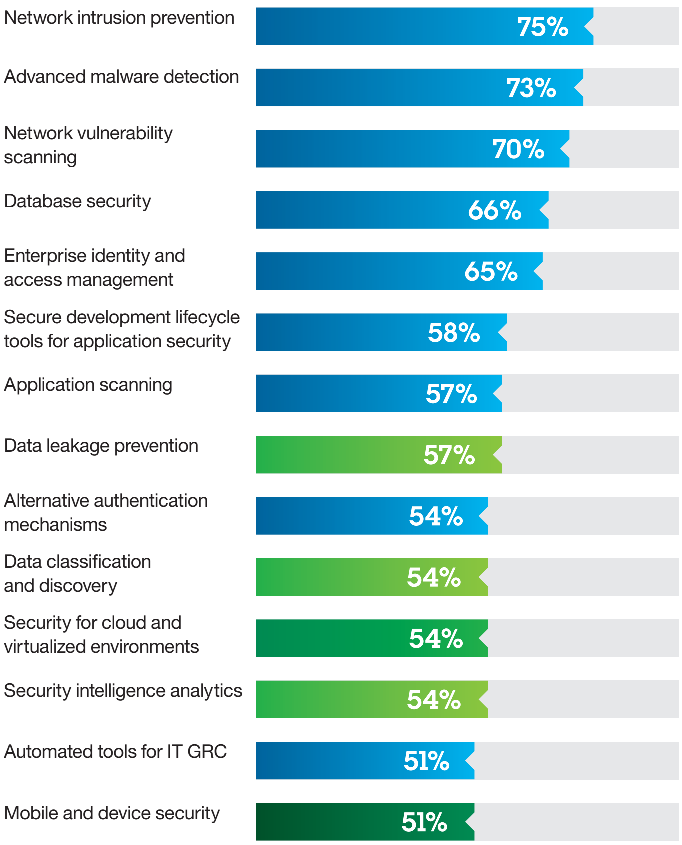
Still focusing on today’s technology

Nearly half of respondents put the deployment of new security technology in their top three initiatives, making it the highest focus area for security leaders. They reported that they are proficient in the established security technologies – their “bread and butter.” More than 70 percent see themselves as very mature with respect to network intrusion prevention, advanced malware detection and network vulnerability scanning.

However, newer areas such as data leakage prevention, cloud and mobile security are proving more problematic: each was identified by 28 percent of respondents as needing a dramatic transformation or improvement, topping the list of areas in need of some renovation or a different approach.

- **Data** – 72 percent of security leaders said that real-time security intelligence is increasingly important to their organization. And yet, areas such as data classification and discovery and security intelligence analytics have relatively low maturity and a higher need for improvement or transformation.
- **Cloud** – High concern over the security of cloud still exists, but cloud consumption is nevertheless widespread and will continue to grow. Eighty-six percent of respondents have adopted cloud or are planning cloud initiatives. Over the next three to five years, three-quarters of security leaders expect their cloud security budget to increase or increase dramatically.
- **Mobile** – The majority of security leaders said they don’t have an effective mobile device management approach. In terms of maturity, mobile and device security ranked at the very bottom of technologies.

Security technology maturity



Seventy-two percent of security leaders said that real-time security intelligence is increasingly important to their organization

Over the next three to five years, three-quarters of security leaders expect their cloud security budget to increase or increase dramatically

Less than half of security leaders told us that they have an effective mobile device management approach

Figure 4. Security leaders see themselves as very mature in more traditional areas, while confidence is not as high in emerging areas such as analytics, cloud and mobile.

Just over half of respondents said that the increasing pace of security innovation is straining their organization's ability to properly address security needs. Pressured to deploy, integrate and improve current systems, security leaders have little remaining capacity to contemplate developing technologies. Consequently, when looking to the future, over half of the respondents could not envision another security capability beyond what currently exists. Leaders are concentrating on the security technology of today.

Uncertain about government action

Regulations, standards and compliance are things that all security and risk leaders deal with on a regular basis. Respondents told us that this area will continue to be a major factor going forward, but there is substantial uncertainty over exactly how.

Much of a company's outlook in this arena depends on its geography, as regulations and standards differ across countries and are constantly changing. For businesses operating on a global level, such variety in regulation creates even more complications.

CISO perspective: Addressing legal and privacy challenges by reducing complexity

By Jamie Giroux
VP of Security and Audit, MAXIMUS

The complexity of security will continue to grow, which means future security leaders are going to need to promote simplification in their processes. Heightened communication between the technology side of security and the legal and privacy side, or a complete integration of is imperative. You will not be able to secure a system properly without knowing everything that goes into it – legal, privacy, contracts, negotiations – and coordinating those disparate parts.

Several potential developments in the marketplace and on the legal front may help tomorrow's security leaders. More compatibility between vendors' services and products allows for a panoramic security picture, a single pane of glass that shows where true risk is from the top to the bottom. While knowing the location of an attack on the front end is valuable, it is more useful to track that attack all the way through to a server or desktop. This is difficult if you have dozens of dashboards and toolsets that do not work in unison.

However, much of the opportunity is in the hands of lawmakers. One of our largest shortcomings in the United States is that we do not have a national standard, a lowest common denominator across the country that establishes a set of security criteria. When you work for a company like MAXIMUS that conducts business in multiple industries in every state, all the different regulations often come into conflict.

While some of information security's future lies in our hands, some of it is contingent upon achieving the appropriate legislation. Whatever business and legal requirements arise, security leaders must shape their technology to meet them in the most uncomplicated way possible.

Regardless of location, there appear to be some widespread questions: Will government be a barrier or a help? Will there be more or less collaboration and transparency in the future? How will privacy be balanced with the growing needs of security?

- More than three-quarters of respondents (79 percent) said the challenge from government regulations and industry standards has increased over the past three years.
- Regulations and standards was one of the areas requiring the most organizational effort to address, second only to external threats.
- Sixty percent are uncertain about whether governments will handle security governance on a national or global level and how transparent they will be.
- Only 22 percent thought that a global approach to combating cybercrime will be agreed upon in the next three to five years.

Fortifying for the future

So what can security leaders do to manage these challenges? How can leaders avoid actions that might inhibit business? What can they do to prepare their organizations for tomorrow? We found four things that security leaders can do:

Shore up cloud, mobile and data security

A maturity gap exists between companies using more traditional security technologies and those advancing into newer areas. To free up resources to focus on newer areas, think about which of your capabilities are mature enough to delegate, automate or outsource.

- Enterprises are widely adopting cloud and devoting significant resources to securing it. There may be worry about cloud, but it is a part of business today. Ensure your organization gets the most out of the cloud opportunity with the least risk.
- Mobile device security is generally lagging. As more devices become connected and the promise of the "Internet of Things" is realized, these problems will just compound themselves. Focus your efforts on bolstering mobile security capabilities.
- With increasing amounts of data being generated by enterprises, don't get overwhelmed – concentrate on your most critical assets. To help manage the rising external threat, advance your approach to real-time security intelligence and analytics.

Enhance education and leadership skills

Asked what skills they anticipate a need for in the next three to five years, security leaders told us that providing training and education for their organizations and preparing to take more of a leadership role were most important. Remember to complement technological knowledge with core business skills, since they are taking on a role commensurate with the growing influence of security leaders.

Engage outside your organization

With the widespread expectation that connections with customers, suppliers and partners will increase levels of risk, security leaders must figure out how best to protect their ecosystem, not just their organization. Make a concerted effort to determine how to clearly assess each other's security–how can you best build trust in one another and broader ecosystems? This requirement is especially critical considering only 14 percent think that a standardized way to assess and quantify information security risk will be widely used in the next three to five years. Use industry groups as critical communication avenues for good ideas.

Plan for multiple government scenarios

Because of the uncertainty over what governments may or may not do with respect to cybersecurity, plan for multiple possibilities. While it's conceivable that governments will enact higher security standards and guidelines that would directly aid enterprises, you cannot rely on such a circumstance.

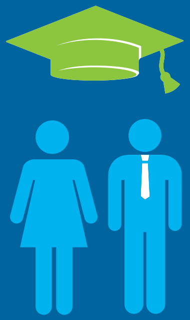
Make sure you have regular dialogue with your chief privacy officer (CPO) and general counsel to better understand what requirements may arise. Seventy-two percent of respondents say customer privacy is increasingly a topic of discussion with their business leadership, yet only 9 percent of security leaders put the CPO as one of their top three strategic partners in the business. Plus, only 14 percent listed their general counsel as one of their top three partners. Take a comprehensive approach that draws upon advice from voices outside the security function.

A more influential future

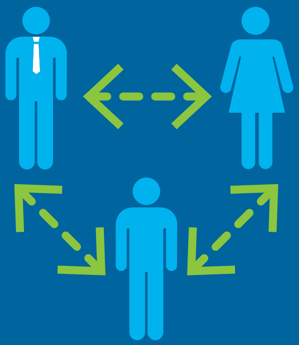
There's no doubt that the advancing perils of information security will prove difficult for those assigned with the protection of their companies. But CISOs should view the future not as an unconquerable challenge, but rather an opportunity to raise their contribution level. The rising tide of threats over the past decade has already forged a higher class of security leader, one capable of captaining his or her company through a persistent storm of acute risks. By understanding the dangers to businesses and enacting keen measures to address them, we can continue to provide the necessary environment for businesses to thrive.

There are a number of actions security leaders can take today to begin fortifying their organizations for the future.

Shore up cloud, mobile and data security
Leaders are not waiting for future technology capabilities to solve their problems, they are focused on deploying today's security technologies to minimize their gaps.



Enhance education and leadership skills
Technology skills continue to be important, but pure business skills will take on more importance with security leaders' growing influence.



Engage in more external collaboration
Leaders should make a concerted effort to determine how to build trust and clearly assess the security of their ecosystem.

Plan for multiple government scenarios
Regular dialogue with chief privacy officers and general counsels is essential for leaders to understand what requirements may arise.

About the authors

Marc van Zadelhoff is the VP, Worldwide Strategy, Marketing and Product Management for IBM Security Systems. He has over 20 years of experience in strategy, venture capital, business development and marketing in the IT and security space. Marc works with customers globally to advise them on security strategy and develop new technologies to meet their needs. He also runs the IBM Security Board of Advisors, staffed with 25 top CISOs who advise IBM on its security portfolio. Marc was a member of the executive team of Dutch-based Consul before it was sold to IBM in 2007. Marc can be reached on LinkedIn and at marc.vanzadelhoff@us.ibm.com.

Kristin Lovejoy is the General Manager of the IBM Security Services Division, charged with development and delivery of managed and professional security services to IBM clients world-wide. Previously, Kris was the IBM VP of Information Technology Risk and Global CISO, responsible for managing, monitoring and testing IBM's corporate security and resiliency functions globally. Today, Kris is a member of a number of external boards and advisory panels. She is a recognized expert in the field on security, risk, compliance and governance, with appearances on CNBC, NPR and WTOP. Kris can be reached on LinkedIn and at klovejoy@us.ibm.com.

David Jarvis is the manager of the research team and agenda for the IBM Center for Applied Insights. He specializes in emerging and strategic business and technology topics. He is co-author of a number of IBM studies including the 2012-2014 IBM CISO Assessments. In addition to his research responsibilities, David teaches on business foresight and creative problem solving. David can be reached on LinkedIn and at djarvis@us.ibm.com.

Contributors

Walker Harrison
Tanya Dhamija
Yana Krasnitskaya
Ellen Cornillon
Sue Ann Wright

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
December 2014

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Please Recycle

About the IBM Center for Applied Insights

ibm.com/ibmcai | **ibmcai.com**

The IBM Center for Applied Insights introduces new ways of thinking, working and leading. Through evidence-based research, the Center arms leaders with pragmatic guidance and the case for change.