IBM Center for Applied Insights

Finding a strategic voice

Insights from the 2012 IBM Chief Information Security Officer Assessment

IBM

About the study

To obtain a global snapshot of security leaders' strategies and approaches, the IBM Center for Applied Insights conducted double-blind interviews with 138 security leaders – the IT and line-of-business executives responsible for information security in their enterprises. Some of these leaders carried the title of Chief Information Security Officer (CISO), but given the diversity of organizational structures, many did not. The Center supplemented this quantitative research through in-depth conversations with 25 information security leaders.

Participation spanned a broad range of industries and seven different countries. Nearly 20 percent of the respondents lead information security in enterprises with more than 10,000 employees; 55 percent are in enterprises with 1,000 to 9,999 employees.

This study—along with **other security and risk management** resources for CIOs and CISOs—is available from **ibm.com/smarter/cai/security**.

With explosive growth in connectivity and collaboration, information security is becoming increasingly complex and difficult to manage. Yet, some security organizations are rising to the challenge. Our research reveals a distinct pattern of progression – and distinguishing traits of those that are most confident and capable.

These forward-thinkers are taking a more proactive, integrated and strategic approach to security, highlighting models worth emulating and the emerging business leadership role of the Chief Information Security Officer (CISO).

In today's hyper-connected world, information security is expanding beyond its technical silo into a strategic, enterprise-wide priority. It takes only a glance at news headlines to see why. In 2011, the corporate world experienced the second-highest data loss total since 2004.[1]

Security leaders are navigating a period of significant change. IT is no longer confined to the back office or even the enterprise. Entire value chains, from suppliers to customers, are electronically connected and collaborating as never before. Devices and ways of accessing information are proliferating. The number of mobile workers is expected to reach 1.3 billion by 2015. At the same time, mobile security threats are increasing – up almost 20 percent in 2011.[2] It all adds up to much greater vulnerability.

While many organizations remain in crisis response mode, some have moved beyond a reactive stance and are taking steps to reduce future risk. They see themselves as more mature in their security-related capabilities and better prepared to meet new threats. What have these enterprises done to create greater confidence? More importantly, can their actions show the way forward for others?

"Security leaders are becoming more closely integrated into the business – and more independent of information technology."

– Senior VP of IT, Energy and Utilities[3]

The changing security landscape: What we learned

Charged with protecting some of the enterprise's most valuable assets – money, customer data, intellectual property and even its brand – security leaders are under intense pressure. Our study findings point to major shifts in attitudes and clear recognition of the strategic importance of information security:

- **Business leaders are increasingly concerned with security issues.** Nearly two-thirds of security leaders say their senior executives are paying more attention to security today than they were two years ago, due in large part to media attention.
- **Budgets are expected to increase.** Two-thirds of security leaders expect spending on information security to rise over the next two years. Of those, almost 90 percent anticipate double-digit growth. One in ten expects increases of 50 percent or more.
- **Attention is shifting toward risk management.** In two years, security leaders expect to be spending more of their time on reduction of potential future risk, and less on mitigation of current threats and management of regulatory and compliance issues.

- **External threats are the primary security challenge.** Drawing far more attention than internal threats, technology introduction or regulatory compliance, outside threats top the list of security concerns.
- **Mobile security is a major focus.** Given increasingly mobile workforces and the high rate of wireless device adoption, more than half of security leaders say mobile security will be their major technology challenge over the next two years.

Across the board, we saw general agreement on the heightened importance of information security. And most companies report having a centralized security function. However, looking deeper – at the actions, plans and strategies of security leaders – we found great disparity in how organizations are actually implementing "centralized" security.

Self-assessment of maturity and preparedness

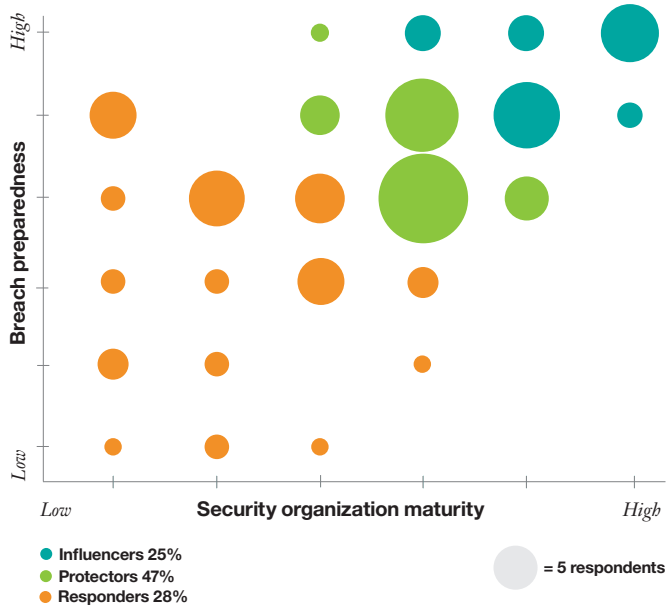

Figure 1: Only one-quarter of security leaders believe their organizations are mature and have high confidence in their ability to avoid or contain a breach.

"Security leaders are more accountable to the business now. Their audience is expanding."

– CIO, Insurance

How prepared are organizations…really?

When security leaders rank themselves on their organizations' maturity and their ability to handle or avoid a breach, three types of organizations emerge, as shown in Figure 1:

- **Influencers** – This group's members, 25 percent of those surveyed, see their security organizations as progressive, ranking themselves highly in both maturity and preparedness. These security leaders have business influence and authority – a strategic voice in the enterprise.
- **Protectors** – Comprising almost half of our sample, these security leaders recognize the importance of information security as a strategic priority. However, they lack important measurement insight and the necessary budget authority to fully transform their enterprises' security approach.
- **Responders** – This group remains largely in response mode, working to protect the enterprise and comply with regulations and standards but struggling to make strategic headway. They may not yet have the resources or business influence to drive significant change.

Knowing that some companies are very confident while others see gaps raises an important question. What are Influencers doing differently?

What makes Influencers stand out

Interestingly, these three security segments are not skewed toward certain demographics. The mix of industries, geographies and enterprise sizes is generally consistent across all groups. The key differences are found in their information security profiles – their structure, scope and accountability. Through an analysis of security leaders' responses, we discovered a distinct pattern of evolution among security organizations (see Figure 2) – and the distinguishing traits of those that are most advanced.

"Information security leaders will have a much larger say in the matter; influence and decision-making power within the company will grow."

– IT Division Head, Media and Entertainment

Security profiles

		Responders	Protectors	Influencers
Structure and management	Dedicated CISO	26%	42%	56%
	Security/risk committee	26%	52%	68%
	Budget line item	27%	45%	71%
	Budget authority	CIO (30%) IT VP/Director/Manager (24%) CFO (18%)	CIO (32%) CFO (20%) CEO (20%)	CIO (26%) CEO (26%) CISO (13%)
Organizational reach	Increased leadership attention	50%	68%	77%
	Regular board topic	22%	58%	60%
	Primary focus over next two years	New security technology (46%) Updating business processes (36%)	Employee education (53%) New security technology (42%)	Employee education (59%) Communications/ collaboration (24%)
Measurement	Standardized metrics	26%	43%	59%

Figure 2: Influencers are much more likely to have elevated information security to a strategic priority.

Structure and management

Because their senior management teams recognize the need for a coordinated approach, organizations in the Influencer group are more likely to appoint a CISO – a dedicated leader with a strategic, enterprisewide purview. Influencers also tend to have a security steering committee headed by a senior executive, often the CISO. The committee's main charter is to evaluate security issues holistically and develop an integrated enterprise strategy. It is responsible for systemic changes that span functions, including legal, business operations, finance, human resources and more.

The vast majority of Influencers benefit from a dedicated security budget line item supporting their efforts. Across the full sample, CIOs typically control the information security budget. However, among Protector and Influencer organizations, investment authority lies with business leaders more often. In fact, Influencers say CEOs are just as likely as CIOs to be steering their information security budgets.

Among Responders, CISOs and steering committees are less common, which suggests their approach to security is more tactical and fragmented. The lack of a dedicated budget line item may force their security organizations to constantly negotiate for funding or limit the scope of initiatives to specific functions or silos.

A CISO perspective: Wider view, broader role

By Paul Connelly

Vice President and Chief Information Security Officer, Hospital Corporation of America

The security leader role is changing because of several key dynamics. The value and volume of information are increasing for many companies, threats to that information are becoming more sophisticated and relentless, and the impacts of security breakdowns are becoming more costly. And among business leaders, customers and the public at large, expectations for the protection of information are higher than ever.

As a result, security leaders have to focus on innovative and highly efficient ways to protect company data, and take a wider view of information protection that extends beyond just security measures. The priority of – and spending on – information protection needs to be a business decision, which may drive change in traditional reporting structures within IT. Alignment with risk management and privacy, disaster recovery and business continuity planning, and physical security offers a clear advantage. It can potentially eliminate overlap, create synergies and drive company efficiencies in information protection – enabling the security leader to become a broader information risk-management player.

Organizational reach

The Influencers have the attention of business leaders and their boards. Security is not an ad hoc topic, but rather a regular part of business discussions and, increasingly, the culture. These leaders understand the need for more pervasive risk awareness – and are far more focused on enterprisewide education, collaboration and communication (see Figure 3). They are working closely with business functions to create a culture in which employees take a more proactive role in protecting the enterprise. Because they are more integrated with the business, these security organizations are also able to influence the design of new products and services, incorporating security considerations early in the process.

Differences in focus over the next two years

Responders		Influencers
	Improving enterprisewide communication and collaboration	4x *more*
	Providing education and driving awareness	2x *more*
2x *more*	Incorporating new technology to close current gaps	

Figure 3: With foundational security technology and practices in place, Influencers are turning their attention to people and building a risk-aware culture.

Responders are more tactically oriented. They are concentrating on foundational building blocks: incorporating new security technology to close security gaps, redesigning business processes and hiring new staff. While technology and business processes are still important to Influencers, they are in the mode of continuously innovating and improving rather than establishing basic capabilities.

Across all three groups, mobile security is the top technical challenge, dominating the agendas of Responders (60 percent) and Protectors (63 percent). Among Influencers, however, mobile security is part of an end-to-end strategy. These Influencers are focused not only on securing mobile access (33 percent), but also protecting cloud (30 percent) and database storage (30 percent).

"Security leaders are going to become more key to their organizations, their budgets will increase and they will move from the fringe to being embedded."

– Line-of-business Director, Banking

Measurement

Influencers are twice as likely as Responders to track their progress. Given their intent to build a more risk-aware culture, these organizations measure user awareness and educational programs more than Protectors and Responders do (see Figure 4). And because they are concerned with broader, more systemic risks, Influencers are also more likely to assess their ability to deal with future threats and the integration of new technologies. Generally speaking, Influencers are not only gaining the attention of business leaders and working collaboratively across the enterprise; they are also being held responsible and accountable for what they do through formal measurements.

> *"In general, the role of information security will be moving away from specific risks to global risks. The role will be much larger than it used to be."*
>
> – Finance Director, Insurance

Importance of metrics

Figure 4: Influencers are more likely to measure progress through a wider variety of metrics and devote more attention to systemic change than the other groups.

A CISO perspective: Why measures matter

By John Meakin

Global Head of Security Solutions & Architecture, Deutsche Bank

Given the dynamic nature of the challenge, measuring the state of security within an organization is increasingly important. Since threats are always moving and solutions are more complex, dynamic and often partial, knowing where you are is essential. Leading indicators could include a variety of measures from the number of applications that have had specific security requirements defined and tested prior to going live to the speed and completeness of correcting known vulnerabilities.

As people access information from a wider variety of locations and devices, protecting it becomes more difficult. Organizations may need to track servers and end-points that store higher classifications of information.

Although metrics can be a challenge to define and capture, that should not deter organizations from implementing them. Measurement may be imprecise at first but will improve over time – and the process itself can drive valuable insight.

The case for security leadership

Despite constant threats and a growing range of risks, some organizations are more confident and capable. Their approaches highlight the importance of a broader charter for the security function – and a more strategic role for information security leaders. Yet, adopting this more holistic strategy involves significant change.

Security leaders must assume a business leadership position and dispel the idea that information security is a technology support function. Their purview must encompass education and cultural change, not just security technology and processes. Leaders will need to reorient their security organizations around proactive risk management rather than crisis response and compliance. And the management of information security must migrate from discrete and fragmented initiatives to an integrated, systemic approach. Security has to be designed to protect the entire enterprise, not just pieces of it.

To accomplish these objectives, security leaders should construct an action plan based on their current capabilities and most pressing needs. They will also need to gain the support of the entire C-suite to drive enterprisewide change.

Responders can move beyond their tactical focus by:

- Establishing a dedicated security leadership role (like a CISO), assembling a security and risk committee, and measuring progress
- Automating routine security processes to devote more time and resources to security innovation

Protectors can make security more of a strategic priority by:

- Investing more of their budgets on reducing future risks
- Aligning information security initiatives to broader enterprise priorities
- Learning from and collaborating with a network of security peers

Influencers can continue to innovate and advance their security approaches by:

- Strengthening communication, education and business leadership skills to cultivate a more risk-aware culture
- Using insights from metrics and data analysis to identify high-value improvement areas

The integrated approach, strategic reach and measurement systems of Influencers point to a new kind of security organization and a new breed of leader. These forward-thinking security leaders can make steady progress because they have authority, accountability and impact. By following their example, those who are not as far along can begin to find their strategic voice.

For more information

Visit the IBM Center for Applied Insights information security website (**ibm.com**/smarter/cai/security) for additional insights, including perspectives from IBM's security leaders. In addition, you can collaborate with peers from around the world as part of the IBM Institute for Advanced Security (instituteforadvancedsecurity.com).

About the authors

David Jarvis is a Senior Consultant at the IBM Center for Applied Insights where he specializes in fact-based research on emerging business and technology topics. In addition to his research responsibilities, David teaches on business foresight and creative problem solving. He can be reached at djarvis@us.ibm.com.

Marc van Zadelhoff is the Vice President of Strategy for IBM Security Systems. In this role, he is responsible for overall offering management, budget and positioning for IBM's global security software and services portfolio. He can be reached at marc.vanzadelhoff@us.ibm.com.

Jack Danahy is the Director for Advanced Security for IBM Security Systems. He is a national speaker and writer on computer network and data security and a distinguished fellow at the Ponemon Institute. In addition, Jack is a frequent contributor to industry and governmental security groups in the areas of data privacy, cybersecurity, cyberthreats and critical infrastructure protection. He can be reached at jack.danahy@us.ibm.com.

Contributors

IBM Center for Applied Insights
Angie Casey, Steve Rogers, Kevin Thompson

IBM Market Development & Insights
Subrata Chatterjee, Doron Shiloach, Jill Wynn

Office of the IBM CIO
Sandy Hawke, Kris Lovejoy

IBM Security Systems
Tim Appleby, Tom Turner

About the IBM Center for Applied Insights

The **IBM Center for Applied Insights (ibm.com/smarter/cai/value)** introduces new ways of thinking, working and leading. Through evidence-based research, the Center arms leaders with pragmatic guidance and the case for change.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
May 2012

[1] *Verizon 2012 Data Breach Investigations Report.* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

[2] "Mobile Worker Population to Reach 1.3 Billion by 2015, According to IDC." January 2012. http://www.idc.com/getdoc.jsp?containerId=prUS23251912

[3] All industry quotes derived from IBM Center for Applied Insights research.

Please Recycle

CIE03117-USEN-00