IBM **Center for Applied Insights**

A new standard for security leaders

Insights from the 2013 IBM Chief Information Security Officer Assessment

IBM

Am I doing enough? Do I focus on the right things? How do I compare against my peers? These questions arise time and time again for Chief Information Security Officers (CISOs) and other security leaders. Our research uncovered a set of leading business, technology and measurement practices that help to address these questions. It also revealed a range of challenges. Even established security leaders struggle with how to manage diverse business concerns, create mobile security policies, and fully integrate business, risk and security metrics. Those who have the right combination of practices and who are addressing these key challenges are evolving into more versatile security leaders – and setting a new standard.

About the study

Continuing and expanding on the work of the 2012 IBM CISO Assessment, titled ***Finding a Strategic Voice***, the IBM Center for Applied Insights, in collaboration with IBM Security Systems and IBM Security Services, conducted in-depth interviews with 41 senior leaders who have responsibility for information security in their organizations. The goal of the interviews was to identify specific organizational practices and behaviors that could strengthen the role and influence of other security leaders.

To maintain continuity, interviewees were recruited from the pool of 2012 research participants – 80 percent of those recruited were prior participants – with an emphasis on more mature security leaders. Interviewees were from a broad range of industries and four countries. More than 80 percent were associated with large enterprises, and roughly one-third had security budgets of over US$1 million.

The overall security environment, as described in the 2012 CISO Assessment, remains demanding. Increasingly sophisticated threats and rising mobility expectations are significant challenges. Perhaps as a consequence, security leaders are garnering greater attention from senior executives. Simultaneously, security leaders are ramping up their efforts to gain influence in their organizations.[1] There is also a rising chorus demanding that security leaders evolve to become information risk specialists for their organizations.[2] With increased focus on the CISO and calls to broaden this role beyond simply defending the enterprise, organizational leaders face a number of key questions: Do I have the right team and competencies? How do I compare to other security leaders in my industry? What practices should I follow that I currently don't?

In our previous CISO Assessment, *Finding a Strategic Voice*, we began to answer these questions.[3] Our analysis delineated three different types of security leader – Influencer, Protector and Responder – and examined the overall maturity and characteristics of each. We established at the time that more mature security leaders put more robust structure and management approaches in place, have greater organizational reach, and measure performance more rigorously.

In this year's study, we found a similar pattern but, going deeper, uncovered key findings, leading practices and a set of shortcomings that even mature security leaders are wrestling with. Looking in depth at three areas – business practices, technology maturity and measurement capabilities – a path emerges that can act as a guide for both new and experienced security leaders.

Business practices: Speaking the language and alleviating concerns

When asked what advice they would give a new CISO, what skills will be important in the future, and how they build trust with their stakeholders, the more mature security leaders shared similar advice. They recommend an emphasis on strong vision, strategy and policies, comprehensive risk management, and effective business relations. They report that they constantly build trust by communicating in a transparent, frequent and credible way. Security leaders believe these activities are increasingly important as they build on their technology competencies and expand their business acumen.

"Security is difficult, and security people are unique. They have a different way of looking at things. We try to get away from 'techno garble,' which isn't important to the business. The business needs it in black and white, no theoretical things."

— Chief Technology Officer, Insurance

What experienced security leaders say about achieving success in their role

Strong strategy and policy

"What's important when making security decisions? A strategic vision, risk assessments and prioritizing around security, understanding impact of new technology, having the ability to differentiate solutions and pick the winners."
(IT Director, Insurance)

"You need global consistency in your policy – one framework. Process is key. People question what they need to do if you don't have consistent security processes."
(Executive Vice President of IT, Financial Services)

Comprehensive risk management

"Risk assessment information is used to determine our security policy. It helps us decide what, where, when, and how to protect, and the cost of doing that – the cost to the business."
(Head of IT Group, Manufacturing)

"Holistic risk management requires that you understand the business – the model, the touch points with external parties, the regulatory framework, the business risks, not just IT risks."
(Chief Information Officer, Media and Entertainment)

Effective business relations

"Getting business support is about selling. You need somebody that has business savvy, but also understands the technology – who can speak business value and understands risk."
(Chief Technology Officer, Insurance)

"When working with the business, security leaders should demonstrate the greatest possible transparency, show business cases and alternatives, talk about solutions that match the business' approach."
(Head of IT, Pharma)

Concerted communications efforts

"To fully communicate the risk, you have to give a lot of specific examples of what other hospitals are doing. We give them snippets of articles, show them what a breach is like at a different hospital, and show them the penalty fees and fines."
(Chief Information Officer, Healthcare)

"Effective relationships require lots of communication, providing assistance to business leaders and requesting time in their meetings to communicate the importance of security, talk about wins and communicate the risks. You open minds when you have that constant background noise."
(Director of Infrastructure, Utility)

Business practices challenge: Managing diverse business concerns

Many security leaders understand what their C-suite is concerned about. This is good – it shows that they are engaged and communicating across the organization. More mature leaders tend to meet more regularly with their Board and C-suite, thereby improving relations. Not surprisingly, though, each C-suite executive has a different top security worry (Figure 1). The interviewees said that their CEOs are most sensitive about negatively impacting brand reputation or customer trust. CFOs fret about financial losses due to a breach or incident. COOs lose sleep over operational downtime. Finally, CIOs have a broad set of concerns, including breaches, data loss and implementing technology investments.

	Loss of brand reputation/trust	Financial loss	Operational downtime	Compliance violation	Other
CEO	49%	6%	15%	9%	21%
CIO	26%	0%	24%	18%	32%
CFO	14%	47%	6%	21%	12%
COO	38%	4%	42%	8%	8%
Average	32%	14%	22%	14%	18%

Figure 1 – According to security leaders, each member of the C-suite has a different top security concern.

This broad spectrum of worries poses a difficult challenge. To help allay these various concerns, the security leaders we interviewed regularly meet with their Boards and C-suites, with the most popular frequency being once per quarter. When they meet, the top topics that they discuss include identifying and assessing risks (59 percent), resolving budget issues and requests (49 percent) and new technology deployments (44 percent). The focus on risk is good. It gives security leaders a chance to help address all the various concerns of the C-suite.

The fact that security leaders believe, on average, that a loss of brand reputation or customer trust is the most important business concern across their organizations raises interesting questions. It is currently close to impossible to track the impact of security breaches and other incidents to brand reputation – even though there can be an impact to stock price or public perception. Very few of the security leaders we spoke with have any capability in the area. The concerns of the CEO may ultimately center on brand reputation and customer trust, but it is up to the security leader to have the business and communication skills to realistically outline what's possible to the C-suite. It is clearly an area in which the industry, as a whole, needs to make progress.

CISO perspective:
Finding a balance with business leaders

By Shamla Naidoo
Vice President, Information Risk & Security
Starwood Hotels & Resorts Worldwide, Inc.

Starwood has developed a comprehensive security strategy that has been reviewed and approved by executive leadership and the Board to make sure we vigorously protect the company's assets and our associate and guest data. To keep our leaders informed about changes in the industry and evolving threats, the IT Security Team provides regular progress reports on our strategy and potential security risks. The service-oriented nature of the hospitality industry, which operates in a rapidly changing business environment, increases our security profile significantly. Consequently, healthy debate and candid dialogue, coupled with measured and responsive decision making, help ensure we are advancing our business and appropriately managing security risks.

The best advice I can give new security leaders:

1. Develop a security strategy and obtain executive buy-in for the goals and plan.
2. Train or hire hands-on experience; you can't secure it, if you don't know how.
3. Keep abreast of ever-changing security risks and consider the legal issues when making security decisions.
4. Understand how your business generates revenue and find productive ways to aggressively support and manage risks that could impact business growth and innovation.
5. Communicate with business stakeholders to inform and educate them about potential risks and solutions, helping them become part of your security line-up.

"You have to be on the bleeding edge of business technology and consumer technology. Bring-your-own-device (BYOD) is starting to encompass almost everything. Devices are proliferating. Security leaders have to be smart, be savvy. Think like a user. Think about what users are doing."

— Chief Information Officer, Financial Services

Technology: Moving beyond the foundational

Although the focus of security leaders is shifting to risk management, stronger business relationships and better communication, security technology remains the most critical tool for the holistic security leader. In fact, those interviewed spend significant time evaluating technology (24 percent, the number one area overall).

Many of the security leaders view foundational and functional security technologies as the most vital components for their organization. These technologies include enterprise identity and access management (51 percent), network intrusion prevention and vulnerability scanning (39 percent) and database security (32 percent). More advanced or strategic technologies have not yet risen above the foundational technologies in importance, including advanced malware detection (20 percent), security intelligence analytics (15 percent) and alternative authentication mechanisms (12 percent). It will be interesting to see how this changes in the future.

Despite well-known concerns, security leaders are forging ahead with mobile security implementation and cloud-based security services. Mobile security is the number one "most recently deployed" security technology, with one-quarter of security leaders deploying it in the past 12 months. And although privacy and security in a cloud environment are still concerns, three-fourths (76 percent) have deployed some type of cloud security services – the most popular being data monitoring and audit, along with federated identity and access management (both at 39 percent).

Many of those interviewed are shoring up their security foundations while slowly testing more advanced technology and establishing cloud and mobile capabilities. Security leaders shouldn't chase every new technology, but rather concentrate on those that will transform their approach and advance their business goals.

Technology challenge: Advancing all aspects of mobile security

In the last CISO Assessment, mobile security was the top technology concern, with more than half of security leaders ranking it as a major technology challenge over the next two years. Mobile security continues to receive significant attention: out of 14 different technology areas, it ranked as both the "most important" and the "most deployed" over the last 12 months. Although mobile is top of mind and backed by investment, capabilities are still maturing.

Today, mobile security is at a foundational stage of development. The most frequently deployed practices are equipping devices with a mobile device management function (78 percent) and inventorying devices that use the corporate network or data (76 percent) – typical first steps when securely establishing mobile within an enterprise (Figure 2).

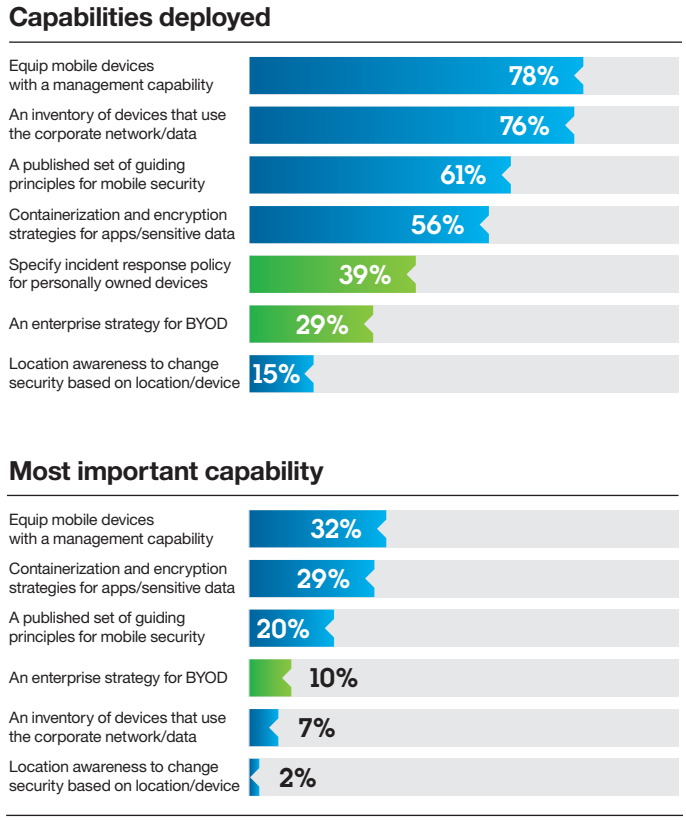


Figure 2 – Mobile security policy and strategy haven't yet taken priority.

The primary mobile challenge for security leaders is to advance beyond the initial steps and think less about technology and more about policy and strategy. For most of those interviewed, a comprehensive mobile policy and strategy for personal devices is not yet widely used or considered important. Less than 40 percent of organizations have deployed specific response policies for personally owned devices or an enterprise strategy for bring-your-own-device (BYOD), and very few consider these actions to be "most important."

However, security leaders are acknowledging and addressing this gap. Establishing an enterprise strategy for BYOD (39 percent) and an incident response policy for personally owned devices (27 percent) are the top two planned areas of development for the next 12 months.

CISO perspective:
Building trust to alleviate concern
By Ken Kilby, Chief Information Security Officer
BB&T

Our bank has been around for 141 years, and we completely expect to be around for at least another 141 years. To enable this, we approach security and risk as a team – it's everyone's responsibility. At the end of the day, all the organization has is its name. If you can't maintain secure access for your clients and customers, you should just pack your bags and go home. So our controls and policies ultimately have to focus on reputation.

To reach this goal, I spend a lot of my time building trust with the C-suite and the Board. I am constantly reaching out to the individual members of the Board and executive management team, developing personal relationships. Different members of the C-suite have different worries that I have to address.

BYOD is also a great concern for us. We are trying to keep up with technology, but always feel like we are playing catch-up to the latest and greatest. We have to manage and secure lots of different mobile platforms – and given the plethora of malware emerging, it is extremely difficult.

There are two recommendations that I would give to my peers looking for guidance. The first is that security leaders have to up their game. They have to be able to communicate to their Board in language that the Board understands. Stay engaged, and don't get sucked into the day-to-day grind. The second is something essential to my job: Develop relationships with law enforcement, industry partners and legislators. Fostering greater public and private communication will ultimately help reduce the total attack surface. We can do more together.

Measurement: Creating the right feedback loop

Today, security leaders use metrics mainly to guide budgeting and to make the case for new technology investment. In some cases, they use measurements to help develop strategic priorities for the security organization. In general, however, technical and business metrics are still focused on operational issues. For example, over 90 percent of interviewees track security incidents, lost or stolen records, data or devices, and audit and compliance status – fundamental dimensions you would expect all security leaders to track. Far fewer respondents (12 percent) are feeding business and security measures into their enterprise risk process, even though security leaders say the impact of security on overall enterprise risk is their most important success factor.

"We use metrics to continually improve our processes and awareness. They help determine what happens next in order to stay ahead of the game."

— Executive Vice President of IT, Financial Services

Measurement challenge: Translating security metrics into the language of the business

This gap between the perceived importance of feeding metrics into enterprise risk processes and actually doing so reflects the challenge CISOs and security leaders are facing. In the 2012 CISO Assessment, we found that more mature security leaders measure more things, more frequently (such as, education and training, risk, and so on). But what should be done with the information, how should it get communicated to the business to spur action?

Nearly two-thirds of security leaders do not translate metrics into financial results. They either lack resources or the business requirement to do so, or it's just too complex to calculate. Additionally, more than half don't fully integrate security metrics with business risk measurements (Figure 3). This failure to combine related measures of success can constrain security leaders' ability to communicate with other business leaders – making it harder for them to effectively and accurately represent the condition of the organization internally.

CISO perspective: Measuring for the benefit of the business

By Felix Mohan, Senior Vice President and Global Chief Information Security Officer Bharti Airtel Limited

We originally began our matrix measurement program at a much more operational, tactical management level. It was to help justify the resources we needed as a cost center. As we learned more and matured more, we shifted how we measured to become more strategic – adding risk, compliance, business continuity, awareness and training and critical application uptime.

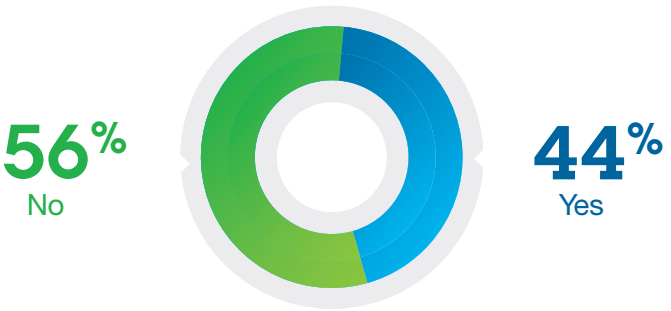
Today, we are still improving our matrix process, trying to become more automated, getting to the enterprise risk level and translating security measures into business impact. We are persistently trying to better understand the risk tolerance of the business and how to measure it.

As part of our latest matrix iteration, we identified all the critical processes that underlie our products and services – things that generate revenue for the company. We've identified all the IT and technology infrastructure that these processes depend upon (e.g., systems and applications, critical assets). We also answered the question: If these processes and assets were not available, what would the recovery time be? We then classified these processes as ultrasensitive, high, medium and low. The classification determines how fast we have to recover the infrastructure, ranging from a few hours to a few days.

Measure financial impact

"Measuring financial impact is important when we want to implement technology. What is the ROI, the cost avoidance of an incident? We use it to prove that there is value." (Chief Technology Officer, Insurance)

Integrate IT and business risk metrics



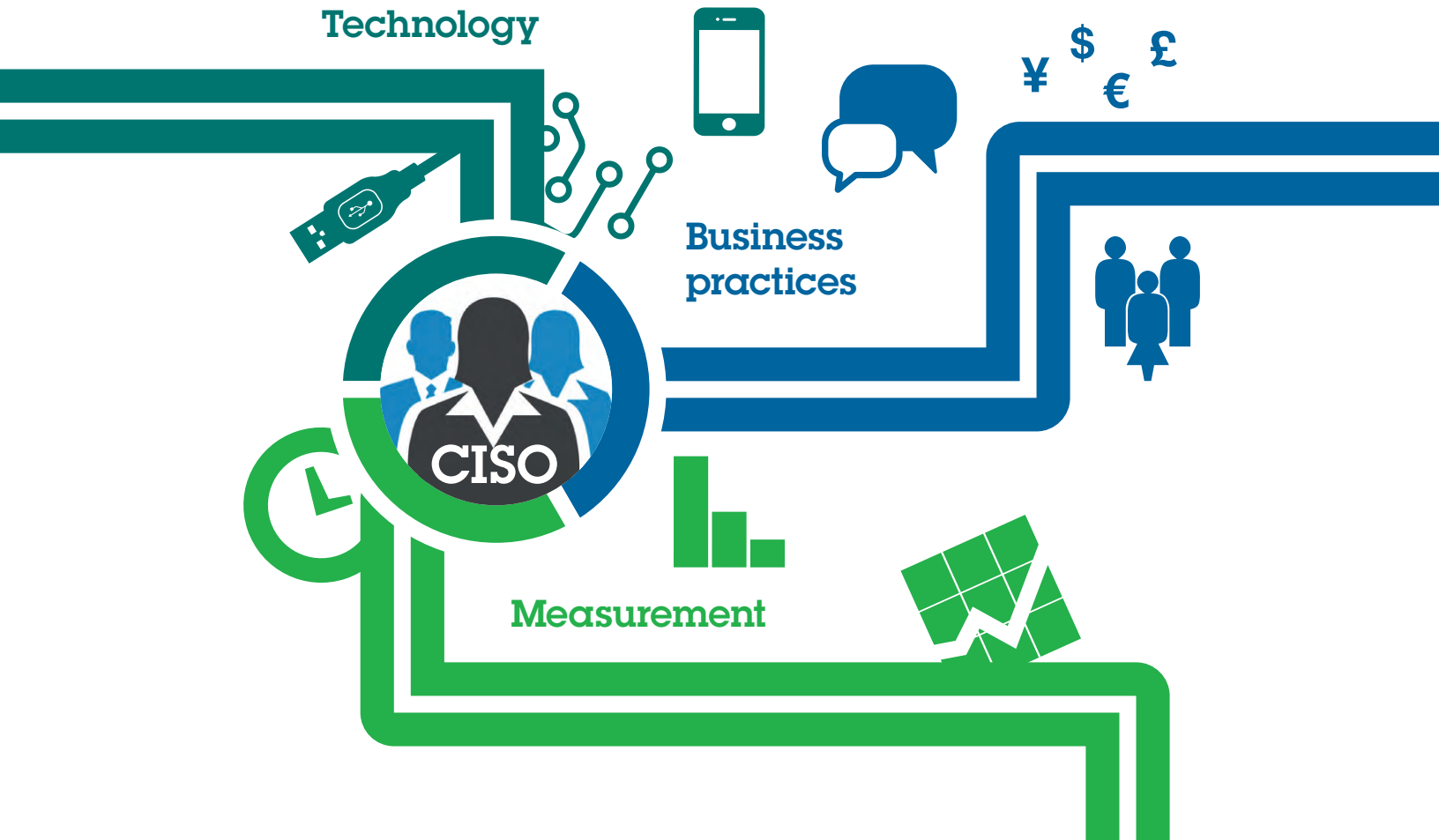
"Security metrics get combined with customer satisfaction as part of a broader scope of continuity and business impact analysis. Cybersecurity is integrated into the risk analysis along with other issues." (Director of IT, Utility)

Figure 3 – Shortcomings are apparent in gauging financial impact, integrating security and risk.

Toward a more versatile security leader

What can these insights and challenges tell us about the focus and approach of information security leaders? Can they help us construct a model for gauging progress? Or find a path to follow?

For starters, they suggest that security leaders must combine a strong security strategy with holistic risk management that considers the economic impact of IT security, while developing effective business relations and engendering trust with senior leaders. They have to maintain foundational security technologies, but not at the expense of implementing more advanced and strategic capabilities. Leaders need to approach mobile security comprehensively – emphasizing policy and enabling use of personally owned devices.



They must create the right feedback loops, as well. Both security technology and business metrics must be fed into the risk management process, not just as line items, but through deep integration. Those metrics must translate into the language of the organization. Without this, security cannot enable business initiatives, and it becomes more difficult to rationalize the need for spending on organization-wide security projects.

Charting a path to higher CISO performance

Some of the security leaders interviewed were closer to this model of versatility than others, however very few were doing everything the model entailed. Those who have the right combination of business practices, technology and measurement capability and are addressing the key challenges set the standard for maturity in security leadership. They are transforming the role that information security plays in their organizations. They are demonstrating mastery of a number of disciplines, both technology and business-related – and advancing what is rapidly becoming a renaissance in security leadership.

For more information

You can learn more about the changing role of security leadership by visiting ibm.com/ibmcai/ciso.

Business Practices

Essential steps

Formalize your role as a CISO to make sure you are recognized as the single, senior security leader with organizational and budget authority.

Establish a security strategy that is updated regularly, communicated widely, and developed in conjunction with other strategies in the organization (such as product development, risk and growth).

Develop effective business relations and meet with the C-suite and Board on a frequent basis and develop an approach to manage their diverse concerns. Take those concerns into account when determining what to measure.

Build trust by communicating with business stakeholders in a transparent, frequent and credible way.

Technology

Essential steps

Invest in advanced technology when it meets a business goal. Don't spend all of your resources on just foundational security technologies; look for advanced technologies and methods that will transform your approach.

Fortify your mobile security, not just with technology but also with a set of business practices and policies – for both individually and business-owned devices.

Share information with other groups, including industry peers. This will improve your confidence [as you make technology investments] and help to answer questions about security priorities and leading practices.

Measurement

Essential steps

Focus on overall economic impact of risk to the organization rather than just audit and compliance. Determine how to protect the business and understand security's impact on brand value and reputation.

Address concerns around reputational risk and customer satisfaction with your Board and C-suite, realistically outlining what is possible.

Translate metrics into financial impacts and fully integrate IT and business risk metrics.

Figure 4 – Essential steps for becoming a stronger security leader.

About the authors

Marc van Zadelhoff, Vice President, Strategy and Product Management, 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.

Kris Lovejoy, General Manager, IBM Security Services
In this role, she is charged with development and delivery of managed and professional security services to IBM clients world-wide. Prior to her role in Services, Kris was IBM's VP of Information Technology Risk and Global CISO, responsible for managing, monitoring and testing IBM's corporate security and resiliency functions globally. She can be reached at klovejoy@us.ibm.com.

David Jarvis, Manager, IBM Center for Applied Insights
David specializes in fact-based research on emerging business and strategic technology topics. He is co-author of a number of IBM security studies including the 2012 IBM CISO Assessment and *Cybersecurity Education for the Next Generation*. David can be reached at djarvis@us.ibm.com.

Special acknowledgements

Caleb Barlow, *Director, Mobile Security, Application Security, Data Security, Critical Infrastructure Security*

David Puzas, *Global Marketing Executive, IBM Security Services*

Adam Trunkey, *Global Marketing Manager, IBM Security Services*

About the IBM Center for Applied Insights

ibm.com/ibmcai

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.

Notes and sources

[1] Gottlieb, Joe. "Being great: Five critical CISO traits." *SC Magazine*. June 13, 2013. http://www.scmagazine.com/being-great-five-critical-ciso-traits/article/298686/

[2] Ashford, Warwick. "CISOs must shape up or ship out, says Forrester." *ComputerWeekly.com*. June 11, 2013. http://www.computerweekly.com/blogs/david_lacey/2013/07/where_next_for_the_enterprisin.html

[3] *Finding a strategic voice: Insights from the 2012 IBM Chief Information Security Officer Assessment*. IBM. May 2012. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=CIE03117USEN

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
October 2013

CIW03087-USEN-00