FORRESTER®

For: Security & Risk Professionals

Evolve To Become The 2018 CISO Or Face Extinction

by Andrew Rose, August 20, 2014

KEY TAKEAWAYS

Pressure On CISOs Increases As Security Becomes More Essential To The Business

The integration of business and technology has created a more complex undertaking for security professionals. New skills and leaders are necessary to navigate this changing landscape and provide more support for the business goal of winning, serving, and retaining customers.

New Job Requirements Will Force A Consolidation Of Roles And New Org Structure

The additional responsibility that comes with the changing role will mean that the CISO career path will look very different. CISOs will have to decide whether to stay on the technology side or develop the business skills necessary to keep their job as it moves into the new organizational structure.

Providing Business Value Should Be The Goal Of The New CISO

Current and aspiring CISOs should work to develop business skills and relationships. They should focus their attention on ideas that truly add to top-line business value; this means extending their interests in domains that matter to business and consumer customers, such as privacy and compliance.

Evolve To Become The 2018 CISO Or Face Extinction

Vision: The S&R Practice Playbook

by Andrew Rose
with Christopher McClean and Andrew Hewitt

WHY READ THIS REPORT

As the role of technology leadership in the enterprise becomes more about managing third parties, battling complexity, controlling costs, supporting the business technology (BT) agenda, and aligning with business strategy, the role of the chief information security officer (CISO) is shifting to one of a business manager who specializes in change management and process oversight. This trend is giving CISOs their long-desired opportunity to interact with the high-level business decision-makers; however, it's also driving a difficult metamorphosis. CISOs will need to realign their priorities and build new skills if they want to remain in their jobs. This report highlights the dramatic changes occurring in the business world generally, and the information security function specifically, and what all this means for the career paths of security and risk (S&R) professionals moving forward. This report was originally published on September 6, 2013; Forrester reviews and updates it periodically for continued relevance and accuracy, and this time found that only light changes were needed, and updated it accordingly as of August 2014.

Table Of Contents

Notes & Resources

In developing this report, Forrester drew from an April 2013 survey to 56 Security & Risk Leaders, client interviews and engagements and a wealth of analyst experience, insight, and research with end users across industry sectors.

Related Research Documents

Security Needs To Accelerate Into The Age Of The Customer Or Risk Marginalization
May 16, 2014

Top 15 Trends S&R Pros Should Watch: 2014
April 18, 2014

Build An Information Security Management System
April 12, 2013

CISOS WILT UNDER INCREASED COMPLEXITY AND BUSINESS SCRUTINY

As business and technology become permanently intertwined as part of the business technology (BT) agenda, security is essential to maintaining efficient, reliable processes and to enabling sustained revenue growth. A breach can mean the loss of revenue, reputation, and resources, or it can mean handing advantage to a competitor; this makes a serious security breach one of the most significant risks to a majority of businesses, just ask Target, or Sony, or eBay.[1] The exposure that these risks represent is giving CISOs increased visibility at the senior executive level and it's directing an evolution of the security leadership role.

Innovation Drives The Need For Wider And Deeper Security Coverage

There's no denying that much of an information security professional's responsibility is focused on how technology interacts with and manipulates the organization's data. As companies embrace innovation, they're introducing layers of complexity that stretch, and in some cases surpass, their ability to operate in a secure yet cost-effective manner. CISOs can't say no to technical innovation anymore, and they can only ask for additional resources and money so many times before they become viewed as some form of pariah. Despite this, the challenges keep on coming:

- **New interfaces increase customer expectations of functionality and security.** New and more pervasive ways of interacting with businesses using emerging technologies are changing workers' and consumers' views and expectations, introducing new risks. Examples include social networking, personal cloud services, and wearable devices such as Google Glass. Furthermore, as individuals become more accustomed to using technology for every aspect of life, there is an increased expectation that it will "just work" and that privacy and security are built-in.

- **New business formats create naive business models ripe for exploitation.** The introduction of digital business models and economies, such as the new virtual currency Bitcoin, will stretch the imagination of the S&R community. Understanding the complexities of an unregulated currency that could possibly be incorporated into transactional systems will be a great challenge, made all the more difficult by the continual presence of organized criminals seeking ways to subvert and abuse these new models.

- **The Internet of Things requires focus on safety ahead of security.** Machine-to-machine traffic will feed autonomous systems that will make intelligent, contextual decisions with an increasing impact on the physical world. Corporate S&R teams will have to take at least some responsibility for physical safety as smart meters, medical implants, connected cars, and building management systems become IP-enabled and self-governing.[2]

- **External threats get perpetually smarter and stealthier.** The political implications of cyberattacks and digital surveillance are unsustainable, and governments will eventually agree to some rules of engagement and preventive measures. Unfortunately, this will just drive the activity even further underground, and, as a result, attacks from both nation-states and criminals will become even more difficult to identify and track.[3]

Business Leaders Are Waking Up To Security But Not Finding The Answers They Seek

Business leaders are no longer able to turn a blind eye to information and cyber risk. Unfortunately, when they reach out to their S&R team, they rarely find the answers they seek in a language they understand. Executive expectations of balanced business cases, strategic thinking, innovation, and value are often left unfulfilled as they instead encounter a three-year technical road map based on knee-jerk reactions to recent incidents, arbitrary peer mirroring, and the CISO's "gut feeling." Business leaders and boards who care about revenue growth are left confused and frustrated. All too often, the S&R function disappoints.

Preconceptions And An Addiction To Operations Draw Attention Away From Key Areas

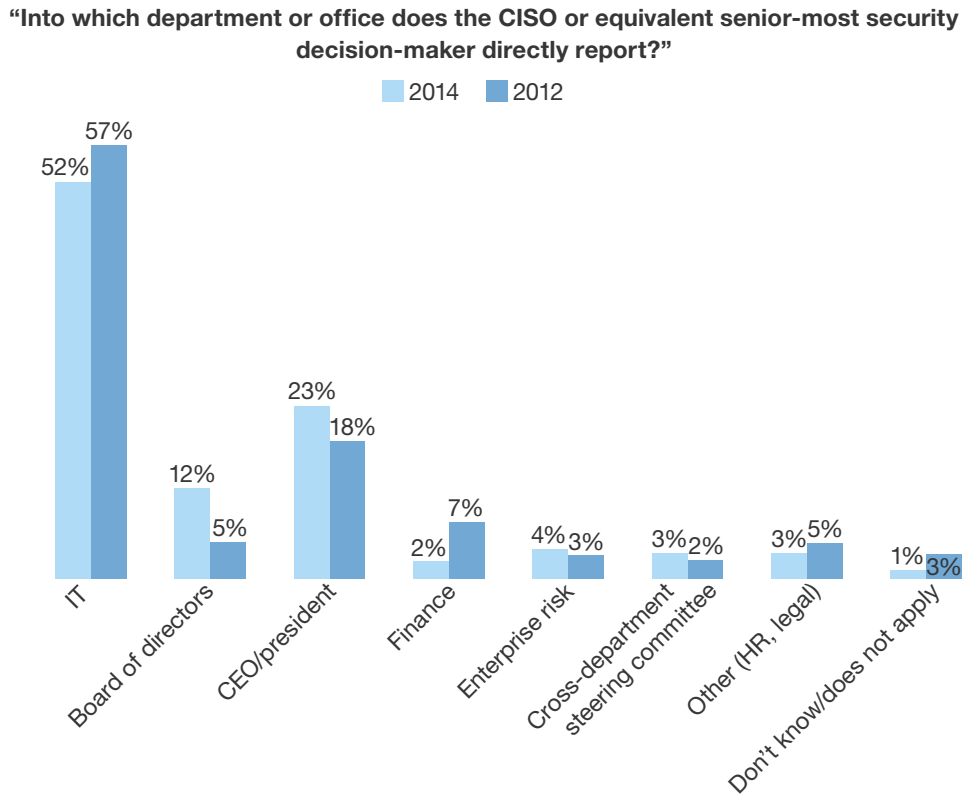
Security professionals have been talking about the increase in business focus for years now, so it's interesting to note that so many CISOs have ignored the writing on the wall by continuing to develop their technical skills and focus on technology solutions. Several factors have held back evolutionary progress:

- **Security leaders still tend to focus on technology.** Although there is a slow decline, more than half (57%) of CISOs from large organizations are mainly tech-focused, and a similar amount report into IT (56%) leaving only around 4% of technology decision-makers that have a more rounded, non-technology centric view of security and risk (see Figure 1). Consider that nearly 80% of S&R leaders originate from an IT or technical background and it's clear why most CISOs approach security from a certain perspective; they have a technology mindset, report into a technology leader and lack opportunities for true business engagement and focus.[4] These shortcomings mean that they often struggle with financial decisions, corporate communications, staffing, contractual hurdles, and other challenges that are increasingly within their jurisdiction as part of the BT agenda.

- **Security managers love the thrill of operational emergencies.** It's undeniable; there's a great sense of satisfaction in wrestling with a problem and winning, and when that problem has a time-critical element, the adrenaline rewards can be additive. Too many S&R professionals are drawn back to this type of work at the slightest opportunity — it makes them feel valuable, but it takes time and draws focus and attention away from vital strategy and business goals.

- **S&R peer groups still value the CISSP above an MBA.** When security professionals get together and talk about professional development, they still talk about Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and other technical certifications, rather than an MBA or a business degree. There is little impetus across the industry to develop business and leadership skills, which means professional aspirations are generally locked into more-technical tracks.

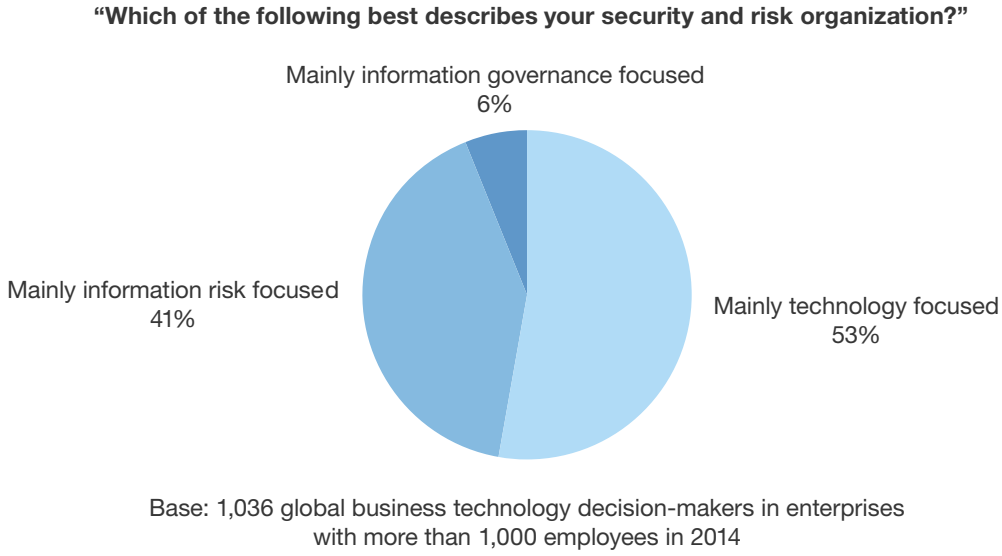
Figure 1 The Majority Of S&R Leaders Still Report Into IT And Remain Technology Focused



Base: 1,036 global business technology decision-makers in enterprises with more than 1,000 employees in 2014 and 2012

Source: Forrester's Business Technographics® Global Security Survey, 2014 and Forrester's Forrsights Security Survey, Q2 2012

Figure 1 The Majority Of S&R Leaders Still Report Into IT And Remain Technology Focused (Cont.)



Source: Forrester's Business Technographics® Global Security Survey, 2014 and Forrester's Forrsights Security Survey, Q2 2012

Savvy Business Leaders Are Threatening To Usurp Top Security Positions

Too few CISOs can interpret a financial report or demonstrate strategic prowess. Purse-holding execs want a fellow business professional who can look at information risk as just another business challenge and describe it in terms of winning, retaining, and serving customers; when they don't get that, they parachute business-skilled professionals into the organization above, or in place of, existing CISOs. If today's CISOs don't adjust to the BT agenda, they will be relegated to the role of an "information technology expert" whose job it is to advise on technical issues rather than manage the whole strategy.

"Too many CISOs have 'techno-machismo', and that is a real buzzkill for their career. They have tied their identity to subject matter expertise and not business value; as the market changes they will run out of room and have to go down-market." – S&R leader at Global Consultancy.

THE CAREER MODEL FOR CISOS IS CHANGING

With all of the changes taking place to support the BT agenda, will this be the end of the CISO position? It certainly won't become completely extinct, but the next several years will see notable evolution and the steady disappearance of the CISO role as it exists today.

The Increasing Criticality Of Information Will Lead To A Consolidation Of Roles

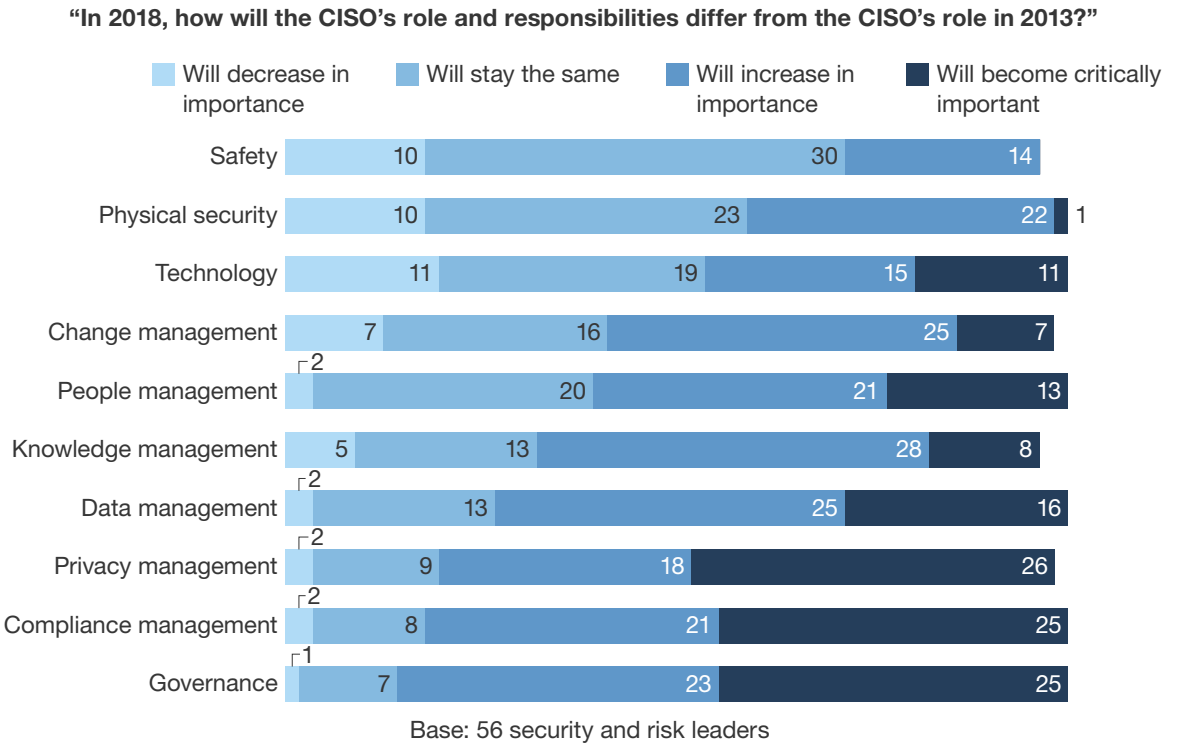
Security leaders now sit at an important intersection within their organization, with a hand in information management, risk management, brand protection, third-party relationship management, and other functions beyond their historically technical role. At this intersection, they will continue to take on a greater number of responsibilities (see Figure 2). This will lead to several changes in the CISO role profile, including a 180-degree flip in priorities (see Figure 3):

- **The CISO will become a privacy champion.** When the revision of the EU Data Privacy Directive is approved, there is likely to be a strong refocus on privacy. Featuring proposals such as 24-hour breach reporting requirements, penalty fines anywhere from 2 to 5% of global turnover, increased responsibility for the actions of data processors, and the translation of "Safe Harbor" into binding corporate rules, the EU Data Privacy Regulation is likely to race to the top of board-level agendas as it comes into force.[5] The urgent need for data and process controls related to privacy will place the CISO in an ideal position to lead the organization's response.

- **All of IT compliance will come under the CISO's jurisdiction.** This trend is notable as many CISOs already have partial responsibility for aspects of compliance. However, as companies increase their global footprint, their reliance on technology, and use of third-party ecosystems, the number and complexity of compliance requirements grows unwieldy. More-centralized focus will be required to consolidate and rationalize complex compliance requirements so that the organization can be as efficient as possible in the enforcement of controls and reporting of conformity.

- **Data governance will underpin the CISO's information risk management practices.** Data governance, including data classification, master data management, data retention, and even knowledge management, will increase in importance with the arrival of technologies and functionality enabling data analytics, big data, and the data economy.[6] The organization's ability to successfully collect and use data will depend entirely on how well it controls access, privileges, and authorization. Companies will fail to compete in the data economy without a CISO who can understand these issues and guide them appropriately.

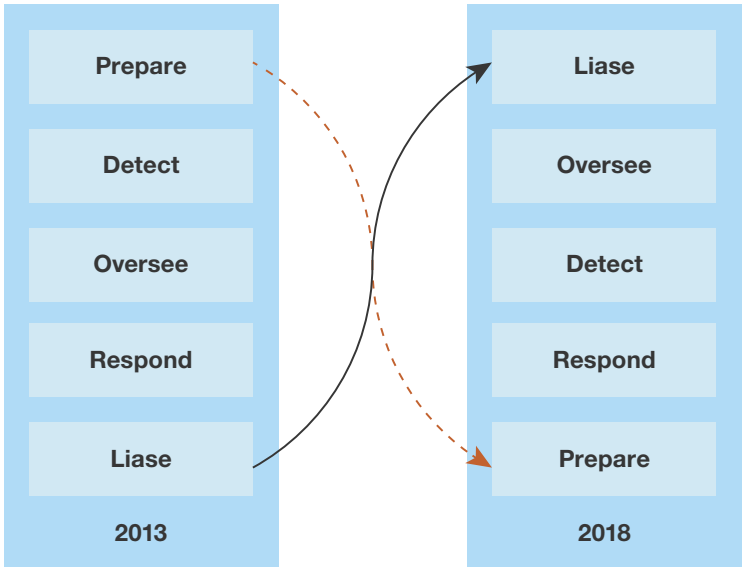
Figure 2 The Growing Importance Of Key Areas Of Responsibility Over The Next Five Years



Base: 56 security and risk leaders

Source: Forrester's Q2 2013 North America/EMEA Role Of The CISO Online Survey

Figure 3 As The CISO Role Approaches 2018, Priorities Flip 180 Degrees



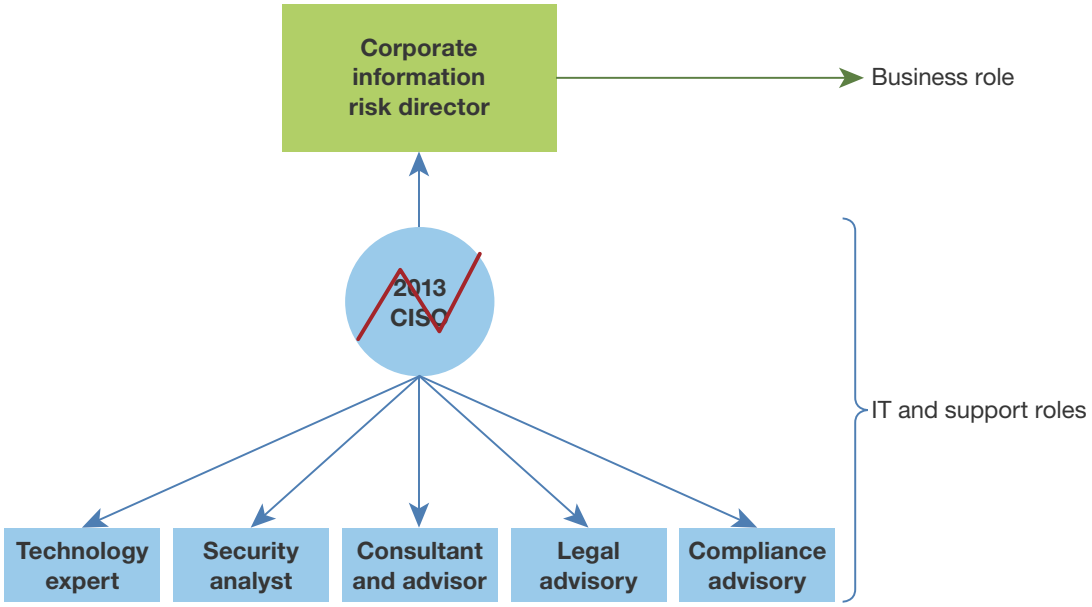
100761 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

A New Organizational Structure Will Arise

As new responsibilities are piled onto the current security leadership role, and the demands from the IT agenda and the BT agenda increase, the current CISO model will become unsustainable. This will drive an evolutionary step, and a business-facing role will emerge, which we arbitrarily title the "corporate information risk director" (see Figure 4).

These evolved CISOs will have strong parallels to the chief business technology officer (CBTO) in that, although they're no longer technical staff, they understand technology, change management, and process improvement, and they can make strategic decisions based on input from a suite of key advisors, many of whom will remain focused in the IT agenda (see Figure 5).

Figure 4 The CISO Role Becomes Unsustainable And Takes An Evolutionary Step



100761 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 5 The Technical Advisor Roles Provide Support And Insight To The New S&R Leader

Technical advisor role	Outline responsibilities
Technology expert	The technology experts will provide deep technical insight into potential threat issues related to infrastructure, architecture, and applications. With a view to the future, they would also bring insight into technology innovation such as mobile and cloud. Subgroups of experts may manage aspects such as IT audit, security architecture, and innovation.
Security analyst	Although the future of information security relies much more heavily on third-party-managed security service providers (MSSPs), each firm will require its own security analysts. This role liaises with the third parties to deal with alerts, investigate anomalies, provide context for threat intelligence, and manage incidents. This role will also scrutinize the ever-increasing complexities and interdependencies of the supply chain, rooting out risk issues.
Consultant and advisor	External parties, contracted as necessary, may well fill the consultant/advisor roles. This role will be diverse but will provide a wider insight into threats, trends, legislation, and technical solutions and purchases. They will also have a responsibility to guide and advise the organization in order to leverage maximum value from the partner MSSPs.
Legal advisory	Global organization will need advice and guidance to ensure that their systems and processes remain legal in each jurisdiction in which they do business. A legal advisory role will fulfill this need.
Compliance advisory	Similar to the legal advisor role, this role will provide insight and leadership around compliance, including requirement mapping, conformity measurement, audit, and reporting.

100761 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

The Death Of The Traditional CISO Career Path

With this evolution, S&R pros need to be ready to act — if you're not prepared to seize the role of corporate information risk director at its inception, you will face severe competition at every subsequent stage. Truthfully, many S&R professionals will find that this new leadership position is out of reach. Leadership of the S&R practice is starting to be perceived as an aspirational role and this is attracting the top talent who have the business skills and connections to simply push the current CISO out of their path. In addition, it's not simply that experienced business leaders will apply for the role; the S&R pro also faces competition from the wider support group, including legal, compliance, and audit professionals (see Figure 6).

Figure 6 The Traditional CISO Role Career Path Opens Up To External Competition

100761 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

S&R PROFESSIONALS NEED TO REFOCUS TO SEIZE THE TOP SECURITY ROLE

Change is always uncomfortable, and although S&R professionals have become accustomed to a landscape of moving goals and evolving threats, the current evolution of their career path is unprecedented. S&R professionals have to react and refocus if they aspire to attain, or retain, the top roles.

Reinvent Yourself As A Business Professional With This Five-Step Plan

When we spoke to CISOs about their vision of the future, they listed leadership, strategic thinking, and business knowledge as the top three skills required to succeed in the role (see Figure 7). Ultimately, the evolved S&R leader must be seen as a competent business professional. Seize control of your destiny by following these five steps:

- **Build a self-development plan that addresses the right issues.** Too many S&R professionals forgo training because they're too busy, but it's essential that you break this habit. Leverage your annual training allocation to build your knowledge of business essentials. Getting an MBA is not the only option — self-study works, too. Learn how to read a financial report, understand the nuances of marketing and sales, and figure out how to manage strategic planning and human capital. One CISO we interviewed told of how he'd just returned from a "speaking to inspire" course. Seek coaching in being an effective leader, and never look at a SANS course catalog again.

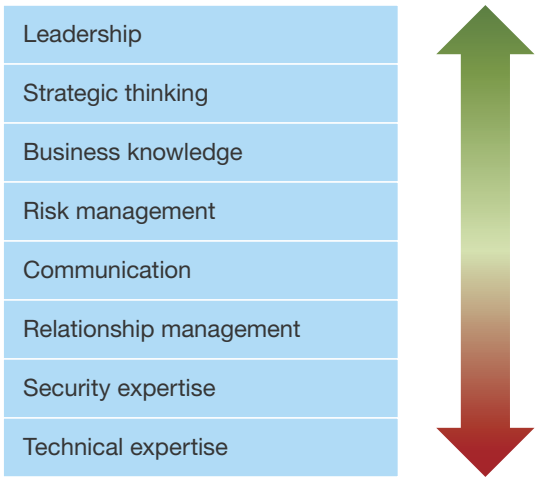
- **Understand your business and the industry.** Broad business knowledge is essential, but it must be drawn into context. Understand your organization from top to bottom, and learn how it's differentiated from competitors: What's the main value proposition, and how will that develop going forward? Become an avid reader of your chairman's letter to the shareholders and identify the cash cows, stars, and dogs in your firm.[7] Learn the processes your organization has in place to win, serve, and retain customers; nearly all of them have security and risk implications.

- **Seek out business allies who can educate, inform, and support you.** Once you have a good grounding in the business language and models in use in your firm, seek out allies who can advance your education and support your goals. You won't find these allies within the CIO's organization; look for friendly business leaders or colleagues in marketing, finance, sales, or risk management, and leverage board-level relationships whenever possible. Set up regular meetings and be forthright about your development goals. The idea is to understand the deeper business story behind corporate strategy and the techniques that win favor at executive level.[8]

- **Get executive attention by creating innovative ideas to add business value.** Forrester has long extolled the virtues of directly linking your security strategy with business goals, and now you must go beyond that. This new, evolved S&R leader must get ahead of the company's ravenous appetite for innovation by contributing new ideas that address security issues while driving new business opportunities that increase revenue and better serve the customer base. Examples may include increasing customer service by enabling knowledge-sharing through secure content systems, or improving customer experience by enabling customers to have direct access to transactional systems via a controlled interface.

- **Seek out opportunities to deliver programs of work.** The evolved S&R leader has to be a proven program manager, capable of delivering change across the enterprise. Too often, CISOs step back from the delivery of security projects and act as a simple stakeholder. S&R professionals who seek to develop their career should look for opportunities to drive the delivery of wide-ranging programs, showing they can effectively manage budgets, resources, and timescales.

Figure 7 Leadership Skills Are Paramount As Security And Technical Skills Wane In Importance



100761 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Seize The Initiative — Build The Role You Want To Evolve Into

As the changing CISO role disrupts the traditional career path, there's one way to approach the challenge that will place you in the best possible position to take this step up: Build the role yourself! By molding the CISO function, you can keep pace with growing business expectations and avoid the critical decision point that organizations reach when they notice the gap in your delivery. Build the solution with you already at the helm and that's the way it's likely to stay:

- **Plan a path away from operations.** You and your team need time to be strategic, innovative, and business-focused. Look for ways to shed operational responsibility. Consider managed security service providers (MSSPs) and outsourcing and clearly define roles and responsibilities to prevent your being drawn into every tiny technical discussion.

- **Revise your risk management processes to speak the business language.** Too many information security risk assessments have a simplistic output of "high," "medium," or "low"; these mean nothing to business leaders. Engage with the enterprise risk team to align your output and language, and consider ways to move beyond guesswork to more statistical risk insight. Make your risk reviews comparable with the financial risk reports that your board reviews and you will construct a foundation of credibility on which to build.

- **Widen your risk vision to include privacy, compliance, and data management.** As you free up time by limiting your operational involvement, invest it in broadening the scope of your risk management efforts. Start to bring compliance, data management, business continuity, third party risk, and other domains within your jurisdiction. Raise your head up from the IT agenda,

and seek out business processes where you can add value and reduce risk. One proactive CISO we spoke to sent members of his team on short-term reassignments to business units, and they came back with greater business awareness, departmental connections, influence, and insight into ways to lessen risk without breaking business processes.

- **Build a support network that you can rely on for insight and advice.** The evolved S&R leader will be a business animal but must retain an awareness of the ever-shifting threat landscape. To function, they will need insight and advice concerning technical threats, legal requirements, regulatory demands, threat intelligence, and current best practices. Identify expert sources internally and externally for these five areas of insight, then leverage their advice and guidance to grow the scope of your organization while you focus on governance and oversight.

- **Leverage your new business skills and focus to impress senior leaders.** Bring these aspects together to show the board how you and your team are changing. Demonstrate how the security and risk strategy supports business goals and helps drive innovation that can support the top line. Display pragmatism, frugality, creativity, and innovation as you prove the security function is able to deliver on time and on budget, and show how an anticipation of the threat landscape and visibility of peer activity means that, given the right resources, your team can keep your organization one step ahead of the competition.

WHAT IT MEANS

YOUR CAREER IS IN JEOPARDY: THE TIME TO ACT IS NOW

The first stage of dealing with loss is denial, so let's get it over with – your expected career path is dissolving; it's happening slowly, but make no mistake, it is happening, and you need to come to terms with that. The next stages of loss are anger, depression, and bargaining, before finally reaching acceptance. S&R professionals need to move through these stages as rapidly as possible, accept that change has arrived, and take back control of their careers.

The window of opportunity is closing and the time to choose between evolving into a more business-focused S&R leader or staying focused on the IT agenda is rapidly approaching. Choose technology and it's likely that your future job roles will be architect, advisor, or consultant, but never again CISO; choose BT agenda and you'll be catapulted into a potentially unfamiliar environment and will never see a system console again.

Perhaps most at risk are those existing CISOs who postpone the choice and decide to continue with the status quo; trapped half way between "technical" and "business," once the transition comes, they will struggle to fit in or excel in either role, and their careers will stall.

Seize the initiative. Reinvent both yourself and security within your organization, and start your firm on the journey before the board mandates the evolution and promotes someone else to lead it.

SUPPLEMENTAL MATERIAL

Methodology

Forrester's Forrsights Security Survey, Q2 2012 was fielded to 2,383 IT executives and technology decision-makers located in Canada, France, Germany, the UK, and the US from small and medium-size business (SMB) and enterprise companies with two or more employees. This survey is part of Forrester's Forrsights For Business Technology and was fielded from March 2012 to May 2012. LinkedIn Research Network fielded this survey online on behalf of Forrester. Survey respondent incentives include gift certificates and research reports. We have provided exact sample sizes in this report on a question-by-question basis.

Forrester conducted a mixed methodology phone and online survey fielded in April-May 2014 of 3,305 business and technology decision makers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, UK and the US from companies with two or more employees.

ENDNOTES

[1] One firm estimates the 2013 Target breach to have a total cost of around $2.6 billion, and states that Sony suffered a similar scale of loss as a direct repercussion of their breach in 2011, being around $2 billion. Source: Rippleshot (http://www.rippleshot.com/expected-target-losses/)

[2] The Internet of Things will mark a significant change for Information Security professionals, safety will become paramount and security will need to take second place. For further insight, see the October 23, 2012, "Prepare Your Security Organization For The Internet Of Things" report.

[3] These "no-spy" agreements are not imminent. The recent test case of US and Germany did not reach a satisfactory conclusion, and China remains adamant that they are not participating in international industrial espionage despite evidence to the contrary. The stakes will continue to rise but a point will be reached within the next four years where governments will start to agree rules of engagement around digital espionage; unfortunately these rules are likely to be only political rhetoric and will have little real impact. Source: NY Times (http://www.nytimes.com/2014/05/02/world/europe/us-and-germany-fail-to-reach-a-deal-on-spying.html?_r=0)

[4] The career paths that CISOs took to their current role always make for interesting conversation. The vast majority of current CISOs, however, had a technological element to their role before taking the position. That is changing, and a new breed of S&R leaders who have never been technical is arriving.

[5] The new European Union regulation around data protection is due to be ratified sometime during 2015. This will bring a notable change from the previous regulations, which were generally agreed to be reasonable but weakly enforced due to negligible penalties. The same will not be true of the 2015 iteration. For further insight, see the March 12, 2014, "Q&A: EU Privacy Regulations" report.

[6] The data economy originates from organizations recognizing the latent value in their data stores and leveraging that data to create value to their customers and, subsequently, build additional revenue. For further insight, see the May 8, 2013, "Introducing Adaptive Intelligence" report.

[7] The Boston Consulting Group originated a "Growth-Share Index" that utilized simple terms to describe a firm's financial model and enable product focus and succession planning. Source: "BCG Growth-Share Matrix," QuickMBA.com (http://www.quickmba.com/strategy/matrix/bcg/).

[8] The age of the customer is redefining business challenges for organizations of all types. Rather than paying lip service to "customer care," they now must become "customer-obsessed" to retain market share. This escalation requires new strategies and dedicated leadership, and the chief marketing officer (CMO) is stepping up to deliver. As technology sits at the heart of customer engagement strategies, marketing functions are becoming increasingly influential in IT decisions, and their demands are often greater than the CIO's — faster adoption of technology, shortened development cycles, and greater flexibility of solutions. CISOs who fail to engage with their CMO colleagues will find themselves constantly on the back foot and fighting too many losing battles to retain their credibility. See the January 9, 2014 "Executive Spotlight: Selling Security To The CMO" report.

FORRESTER®

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals