How To Become A Superstar Security Leader

Vision: The S&R Practice Playbook

by Christopher McClean and Claire O'Malley

September 25, 2018

Why Read This Report

As companies seek to innovate and engage customers through digital channels, they need superstar security leaders — business executives who know how to protect, support, and drive performance. This report looks at the biggest changes in firms' expectations of their chief information security officers (CISOs) and provides specific examples of how top information security professionals rise to those occasions.

Key Takeaways

Requirements For The CISO Have Changed
To stay ahead of changing customer expectations and digital disruption, businesses need security leaders to focus on external demands, exert more distributed influence, become a resource rather than an authority, and anticipate business change instead of aligning to current strategy.

Top CISOs Are Most Adept At Harmonizing Security Within Complex Environments
To meet growing demands, superstar CISOs have developed new ways to explain why security matters, extended their knowledge about their firm's technical ecosystem, and fostered a diverse team to scale their efforts.

CISO Superstardom Is More About Thoughtful Tactics Than Dashing Personality
While most CISOs keep hearing about the traits that great leaders must have, superstar CISOs are more likely to distinguish themselves with the savvy tactics they employ.

How To Become A Superstar Security Leader

Vision: The S&R Practice Playbook

by Christopher McClean and Claire O'Malley
with Stephanie Balaouras, Laura Koetzle, Jinan Budge, Paul McKay, Jeff Pollard, Kate Pesa, and Peggy Dostie

September 25, 2018

No Surprise — Security Is More Important And Difficult Than Ever

Chief information security officers are busier than ever. Their role is expanding to take on brand protection, third-party risk management, information governance, disaster recovery, and privacy — piled on top of the rest of their cybersecurity responsibilities. Many other factors are contributing to the rising pressure that CISOs are facing every day, such as:

- **Customers are exerting more pressure on security and privacy practices.** Among US online adults, a full 32% agree that they usually read a company's privacy policy before completing a transaction or downloading an app; 43% agree that they are likely to cancel a transaction if they read something they don't like in the privacy policy.[1] At the same time, regulatory requirements such as those from the General Data Protection Regulation (GDPR), Federal Financial Institutions Examination Council (FFIEC) and Health Insurance Portability and Accountability Act (HIPAA) that require stronger third-party risk management oversight are driving burdensome customer questions in B2B markets as well.[2]

- **New technologies, like IoT, are opening the door wide to new risks.** While security leaders have watched the growing adoption of internet-of-things (IoT) devices, they are only now seeing attackers apply their skills from more traditional endpoints to connected ATMs, home automation equipment, medical devices, and more.[3] In February 2017, we saw the damage such attacks can cause when a popular internet-connected smart toy for kids, CloudPets, left a large database of user information unprotected online. The emails of over 800,000 users, as well as voice messages left between parents and their children were left exposed.[4] And according to Symantec, the number of IoT attacks rose from 500 in 2016 to 60,000 in 2017.[5]

- **Gender bias is contributing to a staffing shortage in the millions.** The cybersecurity industry is predicting 1.8 million unfilled jobs by 2020.[6] However, this staffing gap seems self-inflicted considering that just 11% of cybersecurity professionals are women.[7] It's even more alarming to read the many accounts from women describing systemic experiences of professional biases, sexual harassment, and even assault, poisoning cybersecurity teams and industry events.[8]

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Your Business Needs A New Breed Of Security

If your company is going to be successful long term, it is currently undergoing substantial transformation to better engage with customers through digital channels. As a CISO, the challenges your CEO wrestles with every day will (and should) change how you approach your position:

› **Customer expectations require you to shift focus to commercially relevant projects.** In 2014, US businesses and government entities began spending more on new technology projects to help win, serve, and retain customers than they did on technology projects to support internal processes and systems.[9] CISOs not plugged into these projects are missing out on budget and opportunities to support top-line growth. For example, the CISO at a global financial services company said his firm restructured its security and IT teams to be more aligned to business objectives as a front-end rather than back-end function. He emphasizes using an "and" not an "or" approach when discussing innovation and security, which has helped improve security's reputation as an enabler of success instead of a roadblock.

› **Business complexity pushes expertise needs from a central team to a wide network.** A growing number of business functions have their own technology budget, which frequently eludes CIO and CISO oversight. In fact, on average, global data and analytics decision makers estimate that 29% of the budget their firm spends on technology represents purchases by a business unit or department without IT involvement.[10] Security teams without involvement in these initiatives are blind to significant sources of potential risk.

› **Your organization and customers need you as an authority *and* a resource.** Considering the number of technology projects, applications, third parties, and customer interactions that have security implications, it's impossible for CISOs to enforce policy for every scenario. Instead, they must set basic ground rules and then show enough value to encourage stakeholders to seek their advice. The CISO of a major US university told Forrester that as an authority, she's protecting her organization but also proactively teaching students about security awareness. Specifically, she provides resources for students to learn how to set up and protect bank accounts and establish other channels of communication for them to come to her with questions. After learning that students are more likely to ask questions online, she created an online chat function for them.

› **Market changes demand you move beyond alignment and become predictive.** In a recent Forrester survey, 44% of global marketing decision makers said that improving customer experience was a high or critical priority.[11] However, few security leaders say that embedding security into their company's products and services or developing secure customer-facing mobile and web applications will be a priority for the next 12 months.[12] This misalignment is not necessarily from lack of effort; security leaders need to anticipate how their business will adopt new technologies and engagement models a year or more ahead of time, so that when the business introduces new technologies and business models — and the inherent risks that come with them — the security team has solutions ready.

Be The Security Leader Your Fellow Executives Want In The Room

Increasing risks, tighter regulations, and more customer expectations will force other executives to work with you. But if you're a superstar CISO, other executives will invite you into their business decisions when they want your insight, not just when they need your blessing. Our research reveals that to become a superstar security leader, you must make three specific changes to the way you communicate, approach technology, and extend your network (see Figure 1):

FIGURE 1 The Superstar CISO Checklist

Goal	Best practice	Tactics
Explain why security matters	Use stories before metrics	• Describe real-life and hypothetical scenarios. • Make your colleagues and their business the main characters. • Craft positive and negative scenarios, and describe the difference.
	Tie every effort to business objectives	• Memorize your corporate objectives. • Document how each project, initiative, and budget item supports at least one. • Report your security metrics using this alignment.
	Communicate with the board	• Build a profile of each board member. • Consider their backgrounds when developing your presentation. • Ask them questions about priorities, risk tolerance, and reputation.
Know your technology touchpoints	Get involved in product development	• Work with marketing to understand customer security expectations. • Work with legal and compliance to meet privacy requirements. • Use DevOps processes to streamline security reviews.
Prioritize employee growth potential	Invest in raw, diverse talent	• Hire candidates who are intellectually curious, good communicators, and logical problem solvers. • Deprioritize traditionally favored technical skills and expertise.
	Hire women, and create a supportive culture	• Address gender biases and other staffing prejudices, whether purposeful or accidental. • Connect recruiting efforts to conferences that cater to women in security. • Create a culture that places, trains, and promotes staff into technical and/or management positions regardless of gender.
	Empower your team	• Give your staff face time in front of key meetings and audiences. • Provide cover for your staff so they're comfortable enforcing rules without retribution. • Place team members on customer-facing projects or other innovation linked to revenue.

1. Spend More Time Explaining Why Security Matters, To Gain Essential Buy-In

Historically, executives often ignored security or became numb to it. As an Asia-Pacific government agency CISO explained, “People get tired of hearing about security. CISOs need to keep on going anyway and to keep on doing what needs to be done.” Today, a larger and more diverse set of stakeholders is starting to ask questions about your program, and you’re likely to be reaching out for more help from people in legal, privacy, marketing, finance, and other roles who don’t think about information security on a regular basis. In these cases, how you explain your efforts and priorities makes all the difference.

- **Use stories before metrics.** Even if security leaders are gifted presenters, security won’t make sense to board members and other executives without real-life examples. The CISO of a $3 billion international manufacturing firm said that he explains risk scenarios — such as theft of intellectual property — using his colleagues as characters in the story to make it more real for them. Similarly, the CISO of a $500 million US retail chain said that he picks a few key executives he needs to be on his side and maps out the effects a security breach would have on their lines of business.

- **Tie every security effort to a defined business objective.** It may sound obvious, but it’s a point few CISOs have fully embraced: Information security exists only to help the firm meet its performance goals and objectives, whether those are to improve customer satisfaction, harness new technologies for growth, protect shareholder value, or maintain regulatory standing. As the CISO of a US healthcare organization explained, “We are in healthcare first, infosec second.” To illustrate the point, he described his best day at work: In response to physicians’ concerns about screens locking too quickly, he made passwords stronger and timeouts less frequent, which immediately improved their ability to treat patients.

- **Communicate with the board, don’t just report to them.** When first asked to present during a board meeting, many CISOs try to pack as many flashy metrics into their 5 minutes as possible — but these speedy recitations can cause directors to zone out and enter what one CISO called “iPhone prayer.”[13] In contrast, superstar CISOs speak a language that the board understands: money. The CISO of a global manufacturing company told us that he puts a dollar amount to every cyber risk so that the board knows how much a disaster might cost them. Meanwhile, the CISO of a major US financial services company says his team created a cyber risk index to measure risk, but they threw out complex charts and spreadsheets that no one understood.

2. Expand Your Knowledge Of The Company’s Technology Touchpoints

While security leaders keep hearing that they need to prioritize business knowledge over their legacy technical skills, that advice is imprecise. Specifically, superstar CISOs don’t necessarily need to have started out in the security operations center, but they must have the technical depth to understand the security implications of technology innovation going on around them:

- **Get involved in product development.** As companies engage customers through mobile apps, smart devices, and other digital products, they will need to build confidence with customers by securing those products, not just customer data.[14] This is a common trend among smart-device makers and other manufacturing firms, but there is evidence of the trend elsewhere. Forrester interviewed a CISO of a marketing services firm who has experience in product management and meets with product marketing and product management frequently. And the CISO of a large health provider helped develop an online prescription service with biometric authentication and a secure patient kiosk in physical locations, both increasing security of medical information and improving customer service.

- **Map your digital ecosystem.** Third-party compliance has become a nightmare for firms in most industries, and the complex technical integration between companies engaging with customers digitally is just beginning.[15] It's critical that you understand how your digital partners will interact with your sensitive customer data, how they will authenticate users, and how they will authorize transactions.[16] The head of group security for a global food and beverage company is exploring integration of data with partners' mobile apps, IoT devices, and wearables. He adds that the ecosystems around intelligent agents like Amazon's Echo and Microsoft's Cortana will soon require a lot of his team's attention.

- **Anticipate the technical road map.** Security leaders who don't want to reclaim their former "Department of No" badges — which should include you — must anticipate road map shifts and have solutions ready. Superstar CISOs invest time, energy, and resources based on how their company plans to adopt technology rather than scrambling to react to current adoption. The CISO of a US healthcare organization told Forrester that when executive colleagues started talking about big data and analytics, he sent team members to Hadoop security training, so he had a trained expert when the business was ready to start its new project. The CISO of a major financial services firm said that he anticipates new technology requests and prepares several options for security controls for them to choose from, increasing their speed and agility to move forward with the project.

3. Prioritize Growth Potential Over Technical Experience

Security leaders everywhere are citing a lack of staff and unavailability of security employees with the right skills as major challenges for their business.[17] However, many of these security leaders are also the ones using outdated, inaccurate, and ineffective hiring practices. The talent that you find at hackathons will be extremely limiting and not diverse. True superstar CISOs know that security talent comes in many forms apart from the typical computer science background. To stack their security team with the best talent, superstar CISOs take a new approach to staffing:

- **Go green, prioritizing investment in raw talent.** Currently, interviews with security job candidates are based on traditional biases toward technical skills. This means that security hires are often more likely to be knowledgeable, but not necessarily the right fit to support digital transformations. Instead, hire candidates — even directly out of undergrad programs or high school — that are intellectually curious, strong communicators, logical problem solvers, and genuinely interested in the field. A cybersecurity CEO told us that she's restructured her interview process entirely to focus on drive and future potential instead of searching for candidates that have 10 years of experience, no people skills, and unrealistic salary demands. The CISO of a major financial services firm explained, "We're using new tools that very few of us are already trained on, hence we're looking out for recruits with nontraditional tech skills."

- **Hire women, and foster a culture that supports them.** The industry is not suffering from a staffing or skills shortage as much as from ingrained sexism and a massive gender disparity that will continue to plague the industry until security leaders restructure their recruiting efforts.[18] It's not necessarily malicious, but that's irrelevant; unconscious bias is unavoidable, but one of the biggest mistakes security leaders can make is to assume they and their organizations are above it. Superstar CISOs know that in order to improve their organization and the industry overall, it's crucial that they actively recruit more women and place them in technical roles. One CISO we spoke with said that she focuses her recruiting efforts on conferences like Women In Security And Privacy, Grace Hopper, and the Executive Women's Forum, which attract thousands of qualified women attendees.

- **Empower your team with the spotlight and your support.** Too often, people with strong security and risk skills don't stick around very long. To combat this challenge, the CISO of a large travel and leisure company described how superstar security leaders have to trust their team members enough to get in front of other execs and give their honest input. On top of that, she also makes sure to provide a safe zone so that they're comfortable saying no to projects or initiatives that introduce too much risk, without fear of retribution.

Recommendations

Realize Superstar CISOs Are Master Tacticians, Not Stage Stars

Every CISO has heard that their job success depends on supreme presentation skills, business acumen, technical prowess, charisma, and other grand character traits. However, it's clear that savvy, thoughtful tactics distinguish the best CISOs more than any star quality. They need to have courage enough to take a stand on critical issues, with personal resilience to keep fighting through inevitable setbacks. So don't model yourself on the singer onstage but on the master conductor in the pit — out of sight, but integral in every scene. For example, instead of trying to develop more charisma to carry you through tough conversations, reach out to relevant teams with the offer to streamline difficult policies, strengthen the security of an upcoming product, or review the controls of an ecosystem partner. Being a valued partner will ultimately make those tough conversations easier.

Endnotes

[1] Source: Forrester Analytics Consumer Technographics® Global Online Benchmark Survey (Part 1), 2018.

[2] Source: "Vendor and Third-Party Management," FFIEC IT Examination Handbook InfoBase (http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk-management/operational-risk/vendor-and-third-party-management.aspx) and "Business Associates," HHS.gov (https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html).

[3] The internet of things (IoT) has evolved beyond a hyped buzzword into commercially available technologies that can significantly improve customer outcomes and deliver business benefits. However, the interlinked set of hardware, software, and ubiquitous connectivity of the IoT ecosystem creates new security challenges and exacerbates legacy security problems. See the Forrester report "The IoT Attack Surface Transcends The Digital-Physical Divide."

[4] Source: Glenn McDonald, "Strange and scary IoT hacks," Network World, July 3, 2018 (https://www.networkworld.com/article/3285968/internet-of-things/strange-and-scary-iot-hacks.html#slide3).

[5] Source: Alison DeNisco Rayome, "As IoT attacks increase 600% in one year, businesses need to up their security," TechRepublic, March 21, 2018 (https://www.techrepublic.com/article/as-iot-attacks-increase-600-in-one-year-businesses-need-to-up-their-security/).

[6] See the Forrester report "Best Practices: Recruiting And Retaining Women In Cybersecurity."

[7] See the Forrester report "Best Practices: Recruiting And Retaining Women In Cybersecurity."

[8] See the Forrester report "Best Practices: Recruiting And Retaining Women In Cybersecurity."

[9] See the Forrester report "US Tech Market Outlook For 2016 And 2017: Cloud And Business Caution Will Slow Growth."

[10] Source: Forrester Analytics Global Business Technographics Data And Analytics Survey, 2018.

[11] Source: Forrester Analytics Global Business Technographics Marketing Survey, 2018.

[12] When we asked global security decision makers which activities would be the top priorities for them and their team over the next 12 months, just 16% chose "embedding security into our organization's end products or services," and 15% chose "developing secure customer-facing mobile and web applications." Source: Forrester Analytics Global Business Technographics Security Survey, 2018.

[13] Your ability to communicate can mean the difference between success and failure in many aspects of your professional life, and it becomes even more important when trying to get the attention of an executive board. Now that information security has become an essential part of risk management across many organizations, chief information security officers (CISOs) must effectively present their case to boards and C-level executives in order to articulate risk posture, explain strategy, or garner more budget. See the Forrester report "The CISO's Handbook — Presenting To The Board."

[14] See the Forrester report "Secure Applications At The Speed Of DevOps."

[15] While sales, marketing, and other business functions have advanced tools and techniques to make the most of data across digital channels (including social, mobile, and web), risk functions have no such luck. Stuck with legacy systems and outdated frameworks, risk professionals struggle to keep up with the vast amounts of available data they need to identify and mitigate risks taking place within and outside of their organizations. Forrester describes key strategies to help you build digital risk insight that improves how you detect and manage risk and how you support strategic business priorities. See the Forrester report "Build Digital Risk Insight."

[16] See the Forrester report "Vendor Landscape: Supplier Risk And Performance Management."

[17] See the Forrester report "Best Practices: Recruiting And Retaining Women In Cybersecurity."

[18] See the Forrester report "Best Practices: Recruiting And Retaining Women In Cybersecurity."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO

B2B Marketing

B2C Marketing

Customer Experience

Customer Insights

eBusiness & Channel Strategy

Technology Management Professionals

CIO

Application Development & Delivery

Enterprise Architecture

Infrastructure & Operations

› Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

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.