Heidrick & Struggles

Does your security chief have board-level commercial savvy?

The chief information-security officer has emerged as an important C-suite role, and a hard one to fill—particularly in Europe.

You are a newly appointed board member of a leading multinational company based in Europe. You've been warned that an unseen adversary is attempting to gain access to the company's most sensitive information. A minor incursion could damage the bottom line; a serious breach could kill the business and destroy the professional credibility of your leadership. Then you hear that a main production facility has been shut down by the chief information-security officer (CISO), a colleague whom you have never met. Within an hour, you and the rest of the board are patched in to a conference call with the CEO and the CISO.

In the heat of such a moment, who is tasked with ensuring that the board makes the best strategic decisions on issues of cybersecurity and corporate risk? What qualities and capabilities should you seek in a CISO—an individual entrusted to make unilateral decisions that affect commercial outcomes? We will address these questions in this paper.

Where does the CISO fit into the C-suite?

The leadership roles of the chairman and CEO are well understood and formulated. Yet as corporations have embraced digital transformation, the C-suite has expanded to include the chief technology officer (CTO), chief information officer (CIO), and, increasingly, chief operational-risk officer (CORO).

CISOs are the latest addition to this cohort. They are sector agnostic and have a broad commission. They can report in different directions, depending on the structure of the business: to the CEO, the chief operating officer (COO), the CIO, or, increasingly in larger organizations, the chief risk officer (CRO) or the CORO. In Europe, we are seeing more CISOs report to the head of legal or the general counsel. Whatever the company hierarchy is, the CISO needs to have an authoritative voice, with his or her views and recommendations heard and discussed at the board level.

What does the CISO's job entail?

"In the past 18 months, there has been more change in the IT and security world than I have seen in more than 20 years—and I don't see that pace slowing down," says Greg Day, the regional chief security officer for Europe, Middle East, and Africa at Palo Alto Networks, a network-security company.

According to the McKinsey Global Institute, by 2025 there could be 25 billion to 50 billion devices hooked up to the Internet of Things.[1] Yet perfect, unbreakable security simply does not exist, so firms must work to marginalize the risks.

"More and more, I see CEOs and board members wanting to understand the problem, but that means we have to talk to them about it in a language that they understand. This will make them better informed and able to collaborate on key decisions," says Day.

A CISO is a necessary appointment because cyber risk is a daily aspect of doing business, and he or she can help ensure that board members (who are generally in the latter half of their careers and did not grow up with this technology) fulfill their responsibilities. Directors who fail to assume responsibility for cybersecurity may find themselves individually liable for lapses.[2]

Damian Walsh, a partner in Heidrick & Struggles' London office and a nonexecutive director of an infrastructure firm, has ringside knowledge of how a board views the security threats: "A board's responsibility is very broad; there are a range of issues to deal with. On security, it is about the board's level of heightened awareness. Many organizations are being attacked relentlessly from different quarters: from financial scamming; from ransomware, where a malicious group will attempt to shut down files or systems for money; and from major attacks aimed at disrupting day-to-day business. This is the scale and magnitude—and boards have no choice but to protect their systems."

Cyber attacks continue to escalate in frequency, severity, and impact, with 69% of respondents relying on cloud-based security services to protect sensitive data, according to a PwC survey.[3] More than 300 million pieces of malware, 10 million pieces of ransomware, and 2 million botnets—where an attacker can take control of your system—were devised and deployed in 2014.[4] Peer-to-peer file sharing poses myriad risks. Though it is impossible for one individual, no matter how smart, to keep on top of every aspect of security, the CISO must filter through this noise to concentrate on specific dangers that have an immediate and direct commercial impact on the business. And there is much more to this role.

"The technical aspect of a CISO's role is simply one part of a much broader mandate that includes everything from alliances and relationship management of regulatory and intelligence agencies to advising the company's own leadership team and board," says Adam Vaughan, a partner in Heidrick & Struggles' London office.

> "It is an old view that information security is simply about building up the walls of a citadel to prevent external attackers from penetrating the defenses. Modern information security is as much about considering the behaviors and unintended operational risks within an organization; true CISOs focus on culture and process to address security in a more sophisticated manner."

[1] See *The Internet of Things: Mapping the value beyond the hype*, McKinsey Global Institute, June 2015, mckinsey.com.

[2] See Luis A. Aguilar, "Boards of directors, corporate governance and cyber-risks: Sharpening the focus," speech at Cyber Risks and the Boardroom Conference, New York Stock Exchange, New York, NY, June 10, 2014, sec.gov.

[3] See *Turnaround and Transformation in Cybersecurity: Key Findings from The Global State of Information Security Survey 2016*, PwC, 2015, pwc.com.

[4] See *Internet Security Threat Report*, Symantec, 2015, Volume 20, symantec.com.

How far does a CISO's reach extend in the business?

Just how far does the CISO's reach extend within the business? We have found that a vigilant CISO can—and will—close down a strategic business process without recourse from the CEO. Day recounts a case where a CISO had to shut down a significant section of the production environment of a major global corporation after a cyberattack. The CISO had never met the board, but within 30 minutes he was called on the carpet to explain the issue.

According to Day, "The board asked why the system had been shut down and asked for it to be brought back online. The CISO replied that the software embedded in a system had been compromised by an attack and that there could be critical consequences for customers. He wasn't giving them tech speak. He translated the problem into their commercial language."

The CISO understood the business. He knew that the affected production facility was not running at capacity and, if the software incursion was sorted out quickly, that it could recover the capacity loss. This is not an isolated example and it highlights the commercial significance of the position.

"Anything that is going to jeopardize the business is going to harm shareholder value and stakeholder interest," says Walsh. "From a board's perspective, they need to know that management has understood the issue and is addressing it. It is up to the CISO to deal with this correctly."

This view is reinforced by Gavin Colman, a fellow Heidrick & Struggles partner in London, who points to a drive from the top down: "The chairman and CEO are aware that something big is happening here; they have witnessed serious breaches at their competitors, and the regulators are on their shoulder. They don't want anything detrimental to impact their organization. The question they must keep repeating is, 'Are we secure?'"

Why does a CISO need to collaborate outside the company?

The CISO must communicate effectively with the board, but the job extends well beyond this internal function.

“While open dialogue with the board is the key to effectiveness and relative success internally, the relationships a CISO develops externally—including alliances with competitors in similar markets—can be the difference between good and great,” says Vaughan.

Thus, an effective CISO in the United Kingdom should become part of a collaborative defensive community—including INTERPOL, Scotland Yard, the Ministry of Defence, Government Communications Headquarters (GCHQ), and specialist industry bodies—that can share information and protect businesses and other entities against sophisticated attacks.

“Utilizing these partnerships with governmental and intelligence networks can prove to be powerful in identifying early warning systems for both state-backed and criminal attacks,” explains Vaughan.

The CISO also needs the emotional-intelligence skills to be an influencer and a persuader at the board level, at the senior-management level, and in this external peer community. It is unlikely to be a position for an introverted technology expert, no matter how intelligent he or she may be.

Where can you find the talent?

The CISO job is incredibly difficult to fill. There are not enough globally qualified candidates—and there is a serious paucity of talent in Europe.

“The pace of this change means that the talent is struggling to keep up,” says Vaughan. “Candidates grow their careers in one specialized area related to information security. But the top role requires knowledge of five or six areas, so finding talent with the requisite breadth of experience is extremely difficult.”

In many cases, the new breed is emerging from the intelligence-service community, including high-level candidates from the Ministry of Defence, MI5, MI6, or GCHQ—though we stop short of hiring away James Bond. There is also a cohort coming from the global mobile- and telecom-infrastructure sector, and network security in hardware and software firms. As specialists in a widely applicable field, these candidates can move across sectors easily. However, many potential CISOs fall short on strategic commercial experience and lack knowledge in working collaboratively with external bodies.

The ideal, well-rounded CISO emerging more recently from the United States (especially Silicon Valley) has polished leadership skills and is attuned to people’s behavioral patterns and values. However, European organizations often struggle to convince these prime professionals to move to London, Paris, Amsterdam, or Berlin. Wooing the best candidates from California is made particularly difficult by a perception of increased terrorism threats across the pond, as well as considerations such as housing, quality schools for their children, and pay scales.

“There is a tiny pool of qualified people, and they are in big demand,” says Walsh.

Compensation reflects this reality in California, where a CISO in a top Silicon Valley outfit can command up to $2 million a year, plus benefits and bonuses. In Europe, this compensation depends on the sector, with C-suite technology officers in major financial firms earning substantial amounts.

Given these obstacles to hiring a single individual, some companies split the role among two or even three people. (For more, see “Four mistakes to avoid when hiring your next security chief,” on heidrick.com.) Other companies employ specialist consultants to undertake strategic projects. These professionals put the right metrics and processes in place and then hand them over to an operational, in-house team.

What drives a CISO?

While salary is a motivator, it is not necessarily the main incentive for taking on the role of CISO. Typically, CISOs are driven by the opportunity to make a significant mark in their field, perhaps by setting the standards in a new industry. Such individuals are resilient, unafraid to argue their case and undeterred by rebuffs.

"After the dot-com boom, technical experts often fell below the radar of senior business people," explains Colman.

"That reality has been changing significantly. Most sectors are now genuinely underpinned by technology. Companies have chunky and meaningful revenues streams supported by technology—and this revenue is potentially under threat."

The best CISOs are motivated and passionate about their work, adds Colman:

"They are wrapped up in their subject, and their eyes light up when they talk about this—and very few other people's eyes do. They keep abreast of issues and ideas by networking with other CISOs. They have a resilience and a grittiness to keep coming back to a complex challenge."

Why must a CISO be commercially savvy?

"The very best CISOs are deeply commercial," says Vaughan. "They are as able to advise on the relationship between investment in risk negation and commercial opportunity as they are on the technical aspects of the role. They are automating process, digitizing protection, and changing culture and operational behaviors, while also advising the leadership team how to effectively enter or reenter difficult markets."

Colman reiterates that this is not purely a technology appointment; it has to be a fundamental business one. As with other C-suite positions, the role is about changing and managing people's attitudes—in this case, toward security risks. The effective CISO thus needs to be a polished and sophisticated communicator, able to influence both internal and external stakeholders. But there should be no illusions about this new breed; finding a robust and full-fledged CISO is a difficult task.

Interview: Greg Day, chief security officer, EMEA, Palo Alto Networks, talks about the evolution of the CISO position

Before becoming chief security officer (CSO) at Palo Alto Networks, Greg Day held a string of impressive positions: he spent more than 20 years with security company McAfee, where he was a malware researcher and consultant, joining the company via its acquisition of Dr. Solomon's, a provider of security-software solutions. He also served as EMEA CTO at two other security companies, Symantec and FireEye.

Day characterizes the cybersecurity challenge as a constantly shifting and complex game of three-dimensional chess.

"It's a matter of who can outsmart the other: the good or the bad guys," he says. "Historically, the good guys were awful at sharing information because sharing was a sign of weakness. Unfortunately, the criminals are very good at collaborating: they share source codes, ideas, and concepts and even sell lists and databases to each other."

Thankfully, this game of chess has—for now—shifted back in favor of the good guys. Lead practitioners, corporate businesses, government agencies, and trade groups are working collaboratively to neutralize the threats.

"What started as informal chats about threats has formalized," Day says. "These new collaborations demonstrate how it is in our interest to share intelligence about what we are seeing, because the quicker we hear about it, the quicker we can respond to it. The simple way to win is to outthink the criminals—and there are a lot more good guys out there than bad guys."

Confirming Vaughan's declaration that CISOs must build external collaborative networks in addition to tending to internal matters, Day says he spends two-thirds of his time as CISO on such external activities. Based in the United Kingdom, he currently sits on the UK National Crime Agency's steering committee, the CERT-UK/CiSP advisory team, and the vForum research community, having formerly held the position of vice chair of the techUK cybersecurity group. He has been part of the Council of Europe Convention on Cybercrime and has participated in a number of industry and advisory groups. These external connections are vital.

"As a chief security officer, my job is about helping the world understand cybersecurity, what it means, and what companies need to do, and then helping my company to understand how it needs to help to address these challenges," Day says.

Each firm must shape its own cyber strategy, and the sharing of information across the industry should be a relentless push to help strengthen companies' security positions.

Why is a CISO increasingly essential—and how is the role changing?

"The required skill sets are certainly changing," notes Day. "Most people working in security who reach the level of CIO, CTO, or CISO have traditionally been grassroots people from the computing industry."

Cybersecurity has historically been viewed as an industry populated by smart techies employed purely to keep the whole system up and running. But Day says that while industry certification through the Certified Information Systems Security Professional (CISSP) program has helped create a knowledge bank, it needs to keep up with current threats.

"In the past, the security team might warn of a risk, wanting time to sort out how to keep it all safe, but they were largely ignored by corporate leadership," he says. "Today that relationship is different, thanks to the many public instances where a security incident has led to dismissal of top brass and a drop in stock price. Suddenly, board members and senior executives want to understand what is going on. Still, a techie saying that the firewall doesn't have the right number of ports of protocols tends to confound a CEO. And the CEO can't make a business decision if he or she doesn't understand what the technical team is talking about."

As such, the CISO is a translator, as well as a security practitioner and a savvy, business-focused executive.

"The CISO still needs smart geeks or technical people working alongside him, but he needs to translate their demands and requests into business implications and then take those to the board and talk in the board's language," Day says.

While the language gap is slowly being resolved, the reporting structure is evolving too. The early leadership matrix had the CISO reporting to the CIO, who owned everything in the field of technology and security.

According to Day, this hierarchy exposed a flaw. The CIO's budget might be defined on the deployment of Windows 10, a new SaaS system, or a new customer database. The CISO would get between 10% and 20% of the CIO's budget. So the CISO's capabilities depended on the CIO's strategy and plans—and were therefore constrained by these budget implications.

"This creates a conflict of interest," says Day. "The CIO is all about new technology and enabling the business, while the CISO is there to keep everything safe. The CISO might suggest that new technology poses a big risk to the business, while the CIO wants to make that resource available to the business. In this relationship, the CIO is always going to win."

Significant governance changes in the past 18 months have shaken up this dynamic. The *Governance of Cybersecurity: 2015 Report*, developed by the Georgia Tech Information Security Center (GTISC) and supported by Forbes, the Financial Services Roundtable (FSR), and Palo Alto Networks, revealed a shift in Europe, where more than 50% of CISOs are now reporting directly to the CEO, COO, CFO, or general counsel, rather than to the CIO.

"With companies expected to notify the board when there is any significant breach, the C-suite executives need to understand the consequences," says Day. "If a breach is made known to the public, there is a possibility of lawsuits. That all gets very costly and messy."

How does the CISO keep up to speed?

"The technology world is massively complex already and becoming more so," says Day. "There are millions of threats out there, and a typical business experiences more than 10,000 security events every month."

The CISO has to filter these down into the few that truly matter and take appropriate action to mitigate the impact.

"The CISO has to be very good at filtering," says Day. "You need to distill these vast numbers down into something meaningful. From an external perspective, it is about subscribing to a service or an organization that will give you only the threats relevant to your industry, sector, and geographical regions."

The CISO has to have smart and empowered people on his or her own team and the management and leadership skills to keep them motivated and on top of their game. In simple terms, there is no room for dropping their guard.

"The required skill sets are certainly changing," notes Day.

The chief information-security officer has emerged as an important C-suite role, and a hard one to fill—particularly in Europe.

The CISO has to have smart and empowered people on his or her own team and the management and leadership skills to keep them motivated and on top of their game. In simple terms, there is no room for dropping their guard.

while industry certification through the Certified Information Systems Security Professional (CISSP) program has helped create a knowledge bank, it needs to keep up with current threats

"The CISO has to be very good at filtering," says Day. "You need to distill these vast numbers down into something meaningful. From an external perspective, it is about subscribing to a service or an organization that will give you only the threats relevant to your industry, sector, and geographical regions."

About the Heidrick & Struggles' Contributors

London Office

Chris Bray is a partner and a member of the Global Technology & Services Practice.
cbray@heidrick.com

Gavin Colman is the regional managing partner for the Information & Technology Officers Practice in Europe and Africa.
gcolman@heidrick.com

Adam Vaughan is a partner and a member of the Financial Services Practice.
avaughan@heidrick.com

Damian Walsh is a partner and a member of the Industrial and CEO & Board practices.
dwalsh@heidrick.com

The team wishes to thank Greg Day of Palo Alto Networks for his contributions to this article.

HEIDRICK & STRUGGLES

CEO & Board Practice leaders

Global

Bonnie Gwin
New York
bgwin@heidrick.com

Jeff Sanders
New York
jsanders@heidrick.com

Europe and Africa

Will Moynahan
London
wmoynahan@heidrick.com

Asia Pacific

Fergus Kiel
Sydney
fkiel@heidrick.com

Graham Poston
Singapore
gposton@heidrick.com

Cybersecurity Practice leaders

Matt Aiello
Co-Leader
maiello@heidrick.com

Phil Schneidermeyer
Co-Leader
pschneidermeyer@heidrick.com

Information & Technology Officers Practice leaders

Katie Graham Shannon
Global Practice Managing Partner,
Regional Managing Partner, Americas
kshannon@heidrick.com

Gavin Colman
Regional Managing Partner, Europe and Africa
gcolman@heidrick.com

Financial Services Practice leaders

David Boehmer
Global Practice Managing Partner
dboehmer@heidrick.com

Jenni Hibbert
Practice Leader, UK
jhibbert@heidrick.com

Dan Ryan
Regional Managing Partner, US
dryan@heidrick.com

Frazer Wilson
Regional Managing Partner, Asia Pacific and Middle East
fwilson@heidrick.com

Global Technology & Services Practice leaders

Michael Cullen
Global Practice Managing Partner,
Regional Managing Partner, Americas
mcullen@heidrick.com

Tim Luedke
Regional Managing Partner, Europe and Africa
tluedke@heidrick.com

Hamish Shaw
Regional Managing Partner, Asia Pacific
hshaw@heidrick.com

Heidrick & Struggles

Heidrick & Struggles is the premier provider of senior-level executive search, culture shaping, and leadership consulting services. For more than 60 years we have focused on quality service and built strong relationships with clients and individuals worldwide. Today, Heidrick & Struggles' leadership experts operate from principal business centers globally.

www.heidrick.com

WE HELP OUR CLIENTS
CHANGE THE WORLD,
ONE LEADERSHIP TEAM
AT A TIME®

hs-00159