90 DAYS A CISO'S JOURNEY TO IMPACT

DEFINE YOUR ROLE

Sponsored by SentinelOne™

Table of Contents

Acknowledgments

To produce this ebook, I had the privilege of interviewing top CISOs and security leaders from a wide range of industries, with collective experience spanning two centuries. Even after 15 years of building security products, I learned a lot from their answers.

The inherent conflicts in the role of the CISO were dominant themes in all the interviews. As a C-Level executive, the CISO needs to understand the business and contribute to its growth, so that it can be successful. As the top executive responsible for the security state of the enterprise, the CISO must stay current with the security risks. To some extent, the CISO is an enabler and the bridge between risks and business needs. They must recognize the unique challenges the business faces and offer a secure alternative that suits the business needs.

On behalf of SentinelOne, I would like to thank the CISOs listed below for sharing their time and expertise for this book.

Migo Kedem,
Senior Director of Products & Marketing
SentinelOne

Pete Nicoletti,
Chief Information Security Officer (CISO) and Cloud Security Industry Leader

Pete is a Strategic Advisor for Cybraics, and on the Board of Directors or Advisory Board for a number of companies. He has previously been CISO at Hertz global and at Virtustream (a Dell company), and VP of Security Engineering at Terremark/Verizon. Pete has been a South Florida trailblazer with a wireless ISP, a network engineering firm and a CRM telephony company. He has 31 years of progressive responsibility in the deployment, marketing, sales, product development, engineering design, project implementation and operation of IT, IaaS/SaaS/PaaS, cloud, data center operations, the entire spectrum of security technologies, compliance frameworks and Managed Security Service Provider services and operations. In 2017, Pete was selected as a "Top 100 Global Chief Security Officers" by Hot Topics Magazine. His cloud security deployments and designs have been rated by Gartner as #1 and #2 in the world and he literally "wrote the book" on secure cloud reference designs, "Building the Infrastructure

for Cloud Security: A Solutions View", published in Intel Press.Pete is a former president of the South Florida ISSA and started the Chili cook-off and Hack for the Flag Contest still going strong! Pete enjoys mentoring security professionals and some of his prodigies have had great success! He lives in the Keys with his wife Jennifer and has 3 kids, two away at college spending his retirement money.

Chris Carney,
IT Security Operations Manager, Meredith Corporation

Chris is an accomplished Information Security leader with over 20 years of experience in IT and Information Security.

With an MBA degree and as a Certified Information Security Manager, Chris is uniquely talented at translating the technical security strategy needs for companies to align with the business goals and objectives.

He has worked in a variety of industries including financial services, healthcare, entrepreneurial start-ups and marketing/media. Follow him at https://www.linkedin.com/in/carneychris/

Kevin L. Emert
(CISSP CRISC)

Kevin served as Vice President/Chief Information Security Officer (CISO) for Scripps Networks Interactive (SNI: HGTV, DIY Network, Food Network, Cooking Channel, Travel Channel, Great American Country, TVN S.A. (Poland)) from July 2015 until it was acquired by Discovery Communications in July 2018.He has 27 years of experience in IT, with the last 19 focused on building and executing successful strategic cybersecurity and risk management programs. Prior to joining SNI, Kevin served as Vice President/ Deputy CISO at BOK Financial, a $30B financial services organization headquartered in Tulsa, Oklahoma. He was a driving force behind the company's transformation into a strategic player and provider of secure financial services in nine Midwest states.

Before that, Kevin was Manager, Global Information Security for ACI Worldwide, an organization of over 5,000 employees across 40 international locations. There he significantly decreased the company's risk by developing

and executing a successful global cybersecurity program focused on Compliance, Governance, Operations and Risk Management. He was previously the first Information Security Officer (ISO) and Corporate Security Officer (CSO) for Home Federal Bank of East Tennessee, and has held security leadership and technical roles at Sword & Shield Enterprise Security, UT Medical Center and United Parcel Service. Mr. Emert pursued a Bachelor of Science degree in Mathematics while a student-athlete at the University of Tennessee.

Lester Godsey,
Chief Information Security Officer (CISO), City of Mesa, AZ.

With over 24 years of public-sector IT experience, Lester has presented at the local, state and national level on topics ranging from telecommunications to project management to cybersecurity. Lester has taught at the collegiate level for over 10 years in the areas of cybersecurity, technology and project management.

A published author, he holds a BA in Music and an MS in Technology from Arizona State University. He is also PMP and CISM certified.

His passions are centered around both cybersecurity and data analytics, specifically about the synergy between the two disciplines and how they help get real cybersecurity work done.

Alex Burinskiy,
Lead Security Engineer

Alex's responsibilities include security operations, incident response and security infrastructure.

He has a strong proven background of managing enterprise threat levels, architecting security infrastructure, and creating security programs to defend corporate infrastructure. He holds an MS in Information Systems and Management from Minot State University. During his free time, he enjoys exploring the world and flying airplanes around the northeast.

Les Correia, *Director, Global Information Security — Architecture, Engineering and Operations, Estee Lauder*

Les's responsibilities include providing security-related functional support and advisory, consulting and engagement support for architecture, engineering, design, audit, governance and operations.

Recently appointed to serve on the Rutgers Cybersecurity Advisory Board, Les is an accredited subject matter expert in information security, risk management, ITIL, Six Sigma, business continuity and disaster recovery. Prior to joining Estee Lauder, he held senior/advisory roles providing thought leadership at AT&T, Lucent, INS (now BT Professional services), Vis.align/Forte, Mannai, Digital and numerous other organizations in the US, Canada, Qatar, Germany, Brazil, and India.

Les has a strong record of client satisfaction references from high-visibility corporations. He utilizes international cultural exposure and bilingual fluency to leverage worldwide business and partnerships

Previous roles have encompassed systems analysis, pro-

gramming, systems/network integration, project/engagement support, IT strategy assessments, service/methodology development, security practice startup, and business to technical alignment reviews.

He continues to broaden his knowledge, pursuing forums, exhaustive certifications, professional development, and training in the field including CISSP, CISM, CISA, CBCP, CIPP, GCFA, NSA-IAM/IEM, CCSK, COBIT, ITIL Expert, Six Sigma Green belt, PMP etc.

He holds an MSc in cybersecurity from NYU's Tandon School of Engineering. He also holds several advanced credits/Graduate certificates - MBA essentials, cybersecurity, Telecommunications and Software Development.

During his free time, Les participates in various Security Hacker/Law Enforcement/User forums while also enjoying flying manned and unmanned aircraft, motor racing, and mountain climbing. He is also part of US Coast Guard Auxiliary Flotilla 014-12-07.

Clint Lawson
(CISSP, MCITP, MCSA, CEH), Chief Information Security Officer (CISO), MidFirst Bank

Clint is a security executive with 20 years of experience ranging from start-ups to global organizations. He is currently the CISO of MidFirst Bank.Previously he was the Director of Threat Intelligence and Cyber Operations at Hertz as well as holding previous security rolls at Johnson Controls International, Hewlett Packard Enterprise (EDS), and York International.

Clint's current focus is developing quantitatively informed cybersecurity strategies, delivering measurable risk metrics, and building agile security teams.

Martin Littmann,
Chief Technology and Information Security Officer (CTO & CISO), Kelsey-Seybold Clinic

Martin is responsible for IT Architecture & Strategy, Infrastructure, Network and Information Security.

He holds a Bachelor of Science in Geology and began his career as a geothermal exploration geologist, later transitioning into information technology development and architecture roles.Martin has over 30 years of global business experience spanning healthcare, energy, manufacturing and consulting. He has served in roles across the IT spectrum including application development and delivery, infrastructure, information security, and customer service.

Over the last 15 years, Martin has been heavily focused on Critical Infrastructure and Information and cybersecurity.

Jake Curtis,
Chief Information Security Officer (CISO), for a large global operating German media company

Jake has been educated and working in the broad field of IT since 2002 in different positions.Since late 2014, he has specialized in information security management, while still practicing “hands-on” technical stuff.

Introduction

"I have a whole set of hacking books and hacking movies and me and my buddies get together all the time and say our stories are way better," says Pete Nicoletti, Chief Data Officer at Cybraics and former CISO at Hertz. "I made a service where we would go way beyond the vulnerability scan or pen test; We would actually physically break into a building and then, from the site, typically break into the network and show you where you're vulnerable - so not only your physical security systems but also your network and internet facing security system.

"We would write very comprehensive reports; we were 100 percent successful in breaking into buildings and acquiring crown jewel information. We did banks; we did very large companies. I've come in through skylights, as well as walking behind people in turnstiles... you name it. I've invented lockpicks to break certain types of locks that

there wasn't a lock pick for. Pretty crazy stuff."

Few CISOs can draw on a background as colorful as Mr. Nicoletti's. Though the cybersecurity world can seem like a Hollywood script at times, when it concerns state-sponsored espionage or gangsters running drug empires through the 'dark web', most of the day-to-day is about patching vulnerabilities, painstakingly seeking out security gaps and reiterating the same basic security advice to your colleagues. The target is perfection, even if perfection can never actually be achieved.

The fundamental questions every CISO must ask are what you are trying to protect, who you need to protect it from and the tools with which you can do so. It sounds simple but this is a challenge that is growing more complex with the growth of cloud computing, the Internet of Things and other technologies that blur the edges of the estate and open up more avenues for attack.

To be a success, a CISO needs to address these questions on a strategic and a tactical level, balancing day-to-day security with long-term projects that will ensure that the organization is well positioned to handle future threats. How that plays out in practice will depend to a large extent on the structure of your organization. Increasingly, CISOs are being positioned within the organization to report to the CEO, though many report to the Chief Security Officer, Chief Information Officer or another executive.

Ultimately, as a C-Suite position, this is a job that requires a long-term view and that means developing a robust strategy. And yet, the strategy also needs to be flexible enough to deal with circumstances that change quickly. This isn't

contradictory. The end goal of the strategy remains but the most effective CISO will have a plan B in mind and will not be afraid to pivot when it becomes clear that plan A isn't working. Even so, there are quick wins that any CISO can target in their first 90 days, which will help to build their standing within the organization and ensure that they hit the ground running. Examples of some of those quick wins are included within.

We would like to thanks all of the leading CISOs who gave their time and shared their expertise with us to help bring this book to life. We are sure that you will find plenty of useful tips within, though we cannot offer any advice on how to abseil into a building through the skylight.

1. The cybersecurity estate

The first question with any kind of security is: what are you trying to protect? Whether it's a building, a VIP or an apartment, what you are protecting will define a lot of your actions. Next, you need to know who or what you are trying to protect them from - kidnappers, robbers or trespassers, for example. And finally, you have to know what tools are at your disposal - alarms, guard dogs, cameras and so on.

Cybersecurity is no different, except that the answers to those questions are sometimes unclear. If you are protecting a building then the physical limits of that building are obvious but that isn't the case when it comes to the building's cybersecurity. Even the tools at your disposal can be a little unclear - does tool A protect us from threats 1 and 2 or only from threat 1? Do we even have a tool for threat 3?

When it comes to assessing the cybersecurity estate,

therefore, the first questions are very basic. Can you define your network's boundaries? You can't protect something if you don't know it's there. Do you know about every device on the network, not just the ones that are being used regularly? Is there a forgotten computer that somehow is still connected? Next, do you know what all those devices are doing? The realm of 'shadow IT', where staff members find their own solution to a problem without informing IT and end up using an insecure application, is one problem here.

That brings us to the users. Do you know who they all are? They aren't always employees - there's the client who is given access to the network because it's the most efficient way to give them the data they need and the child who uses Mum's laptop to play games. It's hard to get visibility of all these users but it needs to be done. Finally, do you know what they are all doing? This includes, as mentioned above, the shadow IT apps, the games, the dubious websites they shouldn't be visiting on a work computer and so on.

"What's interesting about these questions," says Kevin Emert, CISO of Scripps Networks, "is that they are not security questions. They are IT practice questions." Having answers to them is vital to an organization's cybersecurity posture but the CISO needs to work with others to establish them. From the outset, we can see that the role of a CISO is collaborative and will involve a degree of negotiation.

Of course, there are degrees of protection, too. To go back to the building example, you will probably allow anyone to enter the lobby but might require anyone going beyond that point - to the elevators, say - to have a pass. Other areas

of the building will require people to have a pass and know the key code to enter certain rooms, for example. Key staff will have a secretary who will screen visitors, and so on.

The equivalent in a cybersecurity situation would be to determine the 'Crown Jewels', the things that you absolutely must protect. In some businesses, these are so vital, for example, the designs for a new generation of military aircraft, that they are never on the network at all. Most organizations, however, will be happy simply to put extra security around the really important data.

Companies with more mature cybersecurity operations will be able to answer the above questions more readily. For others, more work may be involved. In either case, the next step in assessing the cybersecurity estate is to, in the words of Lester Godsey, CISO for the City of Mesa, ensure that you "eat your vegetables". That is, to take care of the basic cybersecurity tasks.

Mr. Godsey says the expression covers questions like "how mature is your vulnerability management effort? Do you have adequate protections for all your endpoints? Are you collecting data about your environment? How often are you patching? It sounds simplistic but until you at least have the wheels in motion on that you can't go further. You need to eat your vegetables first."

Threat analysis

The above gives us some starting points for answering that first question: what is it you are trying to protect? The next issue, when assessing the cybersecurity estate, is to establish who you are trying to protect it from. What are the threats you face? Most of these are tangible and many are straightforward - viruses, phishing attacks and other threats that can be predicted and defended against.

Outside of the straightforward threats, the most common source of insecurity is the users themselves. According to the Netwrix 2018 Cloud Security Report, almost 58 percent of organizations that had a security incident in 2017 blamed it on insiders[1]. Often this is simply a problem of awareness; users don't realize that what they are doing is a security risk or they have forgotten in the rush to get the job done. In some cases, they are aware of the risk but ignore it for the sake of convenience. Finally, many users dismiss the risk because they assume they are not a target; it's easy for a user to think that the data they handle is not important enough or their role in the company not high profile enough but this isn't the case. One significant risk is that a user's credentials could be stolen to allow an attacker to enter the system.

That means that a proper assessment of the cybersecurity estate will consider the level of awareness users have, how often this awareness is reinforced or supplemented through training and how frequently a problem arises be-

1 https://blog.netwrix.com/2018/01/23/cloud-security-risks-and-concerns-in-2018/

cause of user behavior. The CISOs we spoke to for this book generally argued that the best training makes the issue personal. Users need to understand that everyone is a potential target and that they should take certain measures, both in their professional lives and their personal lives. Like the organization itself, users must eat their vegetables.

Another kind of insider threat is the malicious actor. This could be a user with a grudge against a colleague or the company, or someone stealing data for personal gain. As Martin Littmann, CTO and CISO at Kelsey-Seybold, put it: "We know that internal threats are some of our greatest threats because, if I'm doing a good job of protecting access to my network and everything else, then the best way for somebody to take advantage of me is to be my friend."

At the other end of the scale from user threats, are those from nation states or attackers backed by nation states. In most cases these are targeted at certain types of company - those in defense, finance or critical infrastructure, for example. However, there is some evidence that nation states are happy to support cyber criminals simply for the disruption they cause to rival nations. As with users, the key to protecting your organization is understanding what the goal of these attackers is. If it's industrial espionage then you have to make sure that company secrets are treated as crown jewels and protected accordingly.

Part of the reason that defining the boundaries of the network has become so difficult in recent years is the rise of the Internet of Things (IoT) and the move to cloud services. Though both of them increase risk, neither one is going anywhere. Indeed, they are going to be used much more.

The IoT raises the possibility of attackers gaining access to the network through a connected vending machine, an air quality monitor or some other device that could easily be installed without much thought given to network security. It seems convenient that the vending machine can monitor stock levels and automatically order replacements and it is - so long as the method for doing so is secure.

The picture is further complicated when users bring in their own IoT devices, which are connected to the network or used to handle company data. The IT department often doesn't know these devices exist, much less what they are used for.

Cloud computing

Cloud computing, meanwhile, blurs the boundaries of the cybersecurity estate. It can be hard to know where your data is. Many companies report that the largest cloud providers offer very limited scope for specifying where data is stored. Companies that have been assured that their data will not leave a certain jurisdiction, for example, the EU, report finding that when the network suffers an unexpected outage, their data has been sent elsewhere.

Even if this does happen, the data is still the responsibility of the company that it belongs to, not the cloud provider. That puts pressure on organizations to consider every eventuality with regards to where their data is held and processed. Once you add shadow IT to the mix, the risks

increase. Many IT and security professionals have stories about businesses that have contacted a cloud company about using its services only to be told that their company already has several accounts through shadow IT.

So far, the questions we have considered have definite answers. It might take time to find every device on your network but those devices can be counted and a meaningful answer reached. However, a significant element of the cybersecurity world is intangible. Intangible threats can be things that you might never know, such as how many times a particular password has been stolen or previously unknown attack vectors.

As one of our interviewees put it: "We are constantly in the business of looking for types of threats that we don't know about yet." This means more than just looking for an attack that you didn't know was coming; the modern CISO has to have a plan for dealing with an attack using a method that they did not previously know about. It's like being in charge of defending a medieval castle and suddenly finding that you are under attack by paratroopers.

Ransomware, a form of attack that has been rising in recent years, appears to have been usurped by crypto mining malware - a new growth industry for attackers. As of May 2018, the Coinhive crypto miner is thought to be the most prevalent malware, having affected 22 percent of organizations worldwide[2]. Meanwhile, more and more organizations are seeing 'fillers' attack techniques - that is, attacks that do not use malicious executables. The Ponemon Insti-

2 https://www.nasdaq.com/press-release/mays-most-wanted-malware-cryptomining-malware-digs-into-nearly-40-of-organizations-globally-20180607-00604

tute reports that 77 percent of successful attacks in 2017 used fileless techniques[3].

Summary

The technology world moves quickly. Today's attack methods and threats will continue to evolve and will look different five years from now. However, so will the cybersecurity landscape of the organization. CISOs should expect cloud penetration to have reached a point where it makes less and less sense to talk of a perimeter. Alex Burinskiy, lead security engineer at Cengage, says: "Is perimeter security going to be gone in five years? No. Is it the beginnings of the end for perimeter security? Probably." Alongside these changes, CISOs are confident that they will be able to draw on more tools.

In five years everything might have changed. And yet everything will remain broadly the same. Securing the enterprise will still be about those same fundamentals: What do you want to protect? Who are you protecting it from? And what tools do you have at your disposal?

3 https://www.barkly.com/ponemon-2018-endpoint-security-statistics-trends

KEY QUESTIONS

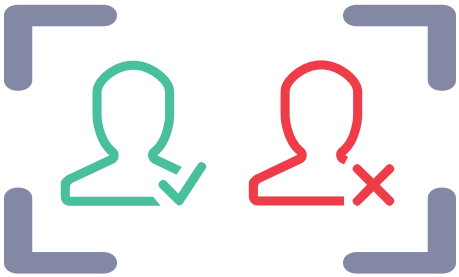
1. *Where are the boundaries of the cybersecurity estate?*

2. *What are you trying to protect - and who from?*

3. *What are the intangible threats?*

4. *Are you keeping an eye on the future?*

2. The role of the CISO



The position of CISO remains a relatively new one in the corporate world. Fewer than half of companies had a security executive in 2006 but by 2011 this had risen to 80 percent of businesses. Not all of these will have the title of CISO, so they are unlikely to be C-suite executives. Even for those who are designated CISO, their position within the org chart varies from one organization to another. According to PwC's 2018 Global State of Information Security Survey, 40 percent of CISOs and other security executives report directly to the chief executive, a quarter (27 percent) report to other board members and a similar proportion report to the chief information officer. Others report to the chief security officer (17 percent) or the chief privacy officer (15 percent)[4].

There are pros and cons to all of these reporting lines. Though there has been a trend towards CISOs reporting to

4 https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

the CEO, a report in Security Roundtable in May 2018 noted that this is not always desirable because of the CEO's limited bandwidth[5]. "The greater number of principles who directly report to the CEO reduces the executive's ability to focus on strategy and organizational leadership," lawyer Steve Berlin said.

The structure of your organization will have an effect on how your role works in practice, which makes it impossible for this chapter to be too specific. However, broadly speaking, the CISO will always be the person who has responsibility for the information security strategy of the entire organization. That means being responsible for the staff who manage information security, managing vendors of third-party information security products, acting as an 'evangelist' and educator on information security across the business and, in many cases, liaising with regulators and law enforcement organizations as necessary.

Don't be 'Dr. No'

The CISO is often seen as the organizational blocker, much like the IT department, telling people they can't do things and forcing them through unwieldy processes in the name of compliance. The CISO will point out that these steps are necessary and in the interests of the company, protecting its business - and everyone's jobs. This often

5 https://www.securityroundtable.org/whats-the-best-reporting-structure-for-the-ciso/

cuts no ice, however, and it is easy to find yourself in a position where colleagues just want to work around you. The result is a growth in shadow IT and the adoption of risky processes - often ones that the CISO is not aware of.

This can be avoided, however. A significant task for a new CISO is undertaking a bit of a PR exercise. You need to shape how the organization sees you and explain how you want to work with them. As with so much in life, first impressions count.

“I used to say that I’m not a no-CISO, I’m a know-CISO. So I ‘know’, rather than say ‘no’,” says Pete Nicoletti. “I would tell people that although security is always viewed as something that’s going to slow down or stop a process, my goal is to lubricate business and to speed it up, as well as to make it more secure.”

Mr. Nicoletti said that ways to do that include removing complexity that increases risk and introducing tools that make processes happen faster and more easily. He says: “I realized that business has to get done and I can't be the one to shut things down without offering a solution that frankly makes it better and that's typically what I did.”

Sometimes the CISO might think an idea is too risky and that the most sensible option is to say no. Even in this case it is still possible to explain the risks and indicate that you advise strongly against a particular course of action. This allows the business to take responsibility for the decision and, in drawing on your advice, they are working with you to reach a solution, rather than simply being told no. This changes the dynamic of the relationship; some people instinctively reject being told no, particularly by someone

who is not their boss, but by working with them you are more likely to win them over to your point of view.

"My goal is not to be a blocker but to help facilitate the conversation," says Lester Godsey. He adds: "I genuinely think that most people want to do the right thing." He says that he believes most of the unnecessary risks taken in the organization are taken because of ignorance, rather than a disregard for risk. That means that, for the bulk of your colleagues, simply educating them about risks they are taking will help to cut down on poor decisions.

Jake Curtis, CISO of a large international media company, emphasizes the importance of being flexible. He says: "Our security policy might have super-specific rules about passwords but the stakeholders may need to quickly implement a prototype without being able to implement that policy completely. The classic approach would be to tell them to stop immediately because they haven't met the requirements. However, we're more likely to acknowledge that we're dealing with intelligent people and they know the risk is minimal. They just need a running prototype and they can take care of the password issue in a later step. Typically, we'll find a pragmatic way forward. We want to make sure that security is not considered to be an impediment."

It can be useful for the CISO to go beyond facilitating decision making and become the company evangelist and educator for security best practice. Mr. Nicoletti argues that security measures should always be incentivized with a 'carrot' and not a 'stick'. When people feel that if they make a mistake they could be publicly shamed for it or, worse, receive disciplinary action, they are much more likely to

try to hide their mistakes and cover up any decisions that backfire. On the other hand, staff who are incentivized to report errors, perhaps through the possibility of a bonus or a public acknowledgment of their good judgment, will be an asset when it comes to improving security.

So, for example, in a 'blame' culture a staff member who clicks on a link in a phishing email might try to hide what they've done, exposing the company to a risk of a breach. In a 'reward' culture, that person is more likely to come forward - admitting their mistake but knowing that they can play a role in good security by bringing it to the attention of the CISO's team.

Of course, even in a reward culture, there will still be times when someone is deemed to have acted with negligence or malice and the company will want to discipline them. The point is not to absolve people of responsibility for their actions, but to put in place a framework that ensures that risk is minimized and breaches are spotted early.

Moreover, there will be times when you do have to say no. Chris Carney, of the Meredith Corporation, says: "We're both trying to make the business successful and I would make sure that whoever I'm dealing with has a clear understanding of how my decision will help that. Of course, they're going to have their own view. If it comes down to a decision point where it's my call against theirs on the way things should go, then it's a question of who is ultimately accountable. If it's something that impacts the security of the enterprise and the organization, then I pretty much have to tell them that it has to be this way."

Take an enterprise view

The security demands of an organization are complex enough but they cannot be the sole focus of the CISO's time and attention. Mr. Godsey says: "If you are a CISO and your only focus is on the cybersecurity aspect, then in my opinion, you fail that as a CISO; because there's a C in front of your title for a reason. And so you need to have an enterprise view with regards to how security fits in the bigger picture of what the organization's goals are."

This broadens the above need to facilitate the conversation; it's not just about facilitating the conversation around decisions where risk is specifically identified but around decision making for the business as a whole and being the person who ensures that risk is constantly considered.

Learning to operate at this level for the first time can be challenging, especially since the bulk of CISOs come from a technology background, rather than a business background. At the C-Suite level, business language is the *lingua franca*, and however much the CISO needs their colleagues to understand technological considerations, those conversations have to happen in business language. One CISO, who works for a major global manufacturer, said that one of his earliest realizations on becoming CISO was that "I had to learn how to talk the language".

This means the cognitive load of taking on the CISO role can be enormous: it requires a level of technology expertise and management skill that might be greater than the individual has had to deal with before, and it also demands a knowledge of overall business and the specific sector in

which the company operates. This is a lot to get to grips with and is unlikely to be manageable in the first 90 days. Indeed, that CISO says that it can take six months to get to grips with a new sector. He adds that this is a problem any time a CISO changes sectors - there will be a period of time devoted to adjusting to the new model. That's unavoidable if the CISO is to reach their potential.

He adds: "If I'm the CISO of a hospital and then go to another one, and another one, I know already all the pitfalls. However, it's a different kind of role being a CISO in health and a CISO in manufacturing or a CISO of a financial institution. I do think you really need to learn about the business but I don't think a CISO needs to be the expert on the business - that would be unrealistic."

Gaining that knowledge means getting onto the 'factory floor' and meeting people. Of course, the company probably has numerous PowerPoint presentations about how it does business, but there is no substitute for getting this information first hand and that means meeting the people who are carrying out the business tasks. This can be a two-way exchange of information because while you are meeting them to learn how they work, you can also use this time to evangelize about security and explain your own ways of working. One reason why this technique is so effective is that people in the business will appreciate that you are taking the time to listen to them and, therefore, are more likely to make the effort to reciprocate.

The more you understand about the business, the better an idea you will have of where the threats are. Different sectors face different threats and different types of busi-

ness have different types of information to protect. This is partly why information security knowledge is not entirely transferable - though the basic principles remain the same, trying to protect industrial secrets from nation-state espionage is a different task to protecting customer data from thieves seeking credit card data.

The daily routine

How you carry out your role on a daily basis will depend on many factors, including the size of your department (and the size of the company), the maturity of your security infrastructure, the frequency with which your organization is targeted and your personal working style.

Many of the CISOs we spoke to warned of the dangers of being too hands-on. There's a tendency to want to play a role in everything, especially if you have stepped up to CISO from a junior role that was more focused on carrying out tasks. The shift to the CISO role is often a matter of shifting from a tactical role to a strategic one. Too much focus on detail means less time to look at the big picture and think strategically.

Just as it is easy for a CISO to spend all day poring over the minutiae of the information security program, so it is possible to get locked into an endless series of strategy meetings. This is the opposite problem, where the CISO is so focused on strategy that they have no idea what's happening day-to-day. Balance is key and some kind of routine

might be necessary to help achieve it. Perhaps one day is set aside as free from meetings and this could be the day that you check-in with your team members to make sure you're aware of the important details? Others prefer to block meetings during certain times of day, though this can sometimes be difficult to enforce.

Nevertheless, there will be an element of routine tasks to the job. Some CISOs told us they like to start the day by catching up on security news and news from within their company's sector, just to get a sense of what is going on. Others prefer to start by 'checking the fences' - looking at the defenses they have in place and making sure that everything is working as planned.

A portion of each day will also be devoted to response, whether to minor incidents that perhaps need to be met with a slightly tweaked approach or more significant incidents that need action before they become a crisis. If an actual crisis occurs then daily routine will have already gone out of the window and you should be implementing a well-practiced response plan.

Other ongoing tasks include reviewing new technology and tools to determine whether they can form a useful part of your arsenal. Overlapping this is the need for vendor management. CISOs we spoke to agreed that talking to vendors is useful but they warned that the time spent has to be controlled. CISOs who shut themselves away from vendors entirely are denying themselves a useful source of intelligence and the chance to sense-check their processes and plans. At the other extreme, CISOs who make themselves too available will struggle to get anything done. There

needs to be a healthy balance. Some CISOs suggest that a vendor management policy be set early so that it can be followed exclusively.

It should be clear by now that a CISO has numerous responsibilities and needs a range of skills. When you first start as a CISO, you will have gaps in those skills. That's unavoidable, but try to be aware of where those gaps are and take steps to deal with them. In the long term, that might be some form of training combined with, in the short term, hiring someone who is strong in that area. For example, if you are weak in project management then make your first hire an experienced and well-organized project manager.

Finally, don't be afraid to delegate. This is an extension of the point above about not getting too caught up in either detail or strategy. We will discuss team building in more detail in Chapter Six but the key point is that when you have in place the team you want, trust them to get on with the job. This will allow you to focus on your priorities.

Summary

As we mentioned in the introduction to this chapter, your role as CISO will be determined to a great extent by where the role sits in the org chart. However, it will also be shaped by how you carry out the role. The more active or passive you are, the more your stance is proactive or defensive, the more you dictate to staff or educate them - all these things will determine how the organization perceives you, how much autonomy they grant you and how your role combines with the role of other C-suite executives and key staff members.

You can be seen as 'Dr. No', who prevents people from doing things, and therefore as an obstacle to be overcome, or you can make yourself a trusted partner, keen to help the business meet its goals but always with an awareness of risk. It is obvious from the way that distinction is phrased that every CISO we spoke to for this book advocated the latter approach.

KEY QUESTIONS

1. *Do you know where you, as CISO, sit within the org chart and what that means?*

2. *Are you going to be 'Dr. No' or 'Dr. Know'?*

3. *Do you understand the business well enough to really understand how risk affects you?*

4. *Are you able to balance the day-to-day efficiently alongside ongoing projects*

3. Strategy

In the previous chapters, we have looked at taking stock of the cybersecurity estate and the role you can expect to play as CISO. These are the tasks that will feed into how you develop your strategy for the organization. The next challenge is executing your strategy, including finding some of the quick wins that will help you to establish yourself and your team within the organization.

Remember that your strategy exists to further the goals of the organization. Les Correia says: "I would not decide on a strategy independently of the company strategy. The strategy would actually come from the company itself. If the goal is to go digital or to sell more widgets then I would develop a strategy that matches that."

Within that overall goal, there are still many variations of strategic approach. The path you take will be determined by the risk appetite or risk tolerance of the organization.

How much risk are the senior executives willing to take in pursuit of their goals? How much risk are they permitted to take, given regulatory or compliance constraints that might affect their operations? These will differ, not only from one company to another but also from one time to another; For example, if a competitor has just acknowledged a significant breach then the whole sector might become more cautious.

Risk appetite will vary within the organization, too. The legal department will always be more cautious than the creatives, for obvious reasons. In developing your strategy you will need to balance all these risk attitudes to make the organization as secure as possible, while also maximizing opportunity. Eliminating risk is neither possible, nor desirable - all business involves risk - but a good strategy is one that takes a considered view.

Strategic objectives

One overriding part of your strategy, before we even consider specific objectives or cybersecurity programs, will be to establish yourself. There is an element of public relations to this, and it may not come naturally to every new CISO. However, it is important for building confidence in you, as CISO, in your cybersecurity program, and in your team. How you go about it will depend on the role of cybersecurity within your company and how it is viewed. You will need to work much harder in a company that has had no clear security strategy before, for example.

In the early phase of your time as CISO you will want to establish how you make decisions and run your department. Since security is so dependent on human behavior, the staff in your company need to have an idea of your approach. Will you govern security by edict or be collaborative? Will you tempt with the carrot or punish with the stick? Or a combination of both? This should be considered as part of your strategy from the outset because consistency early on will pay dividends later. For what it is worth, the CISOs we spoke to for this book unanimously favored managing security collaboratively and the carrot over the stick.

As with many parts of this book, it is impossible to give a detailed guide to how you should proceed. Every CISO role is different. However, you will want to define a small number of strategic objectives. Some of these should be short-term - so-called quick wins, which we will discuss below - and others will be long-term projects, either because they are less essential or simply because they need more time

and resource. How many strategic objectives you define will depend on your resources and how far into the future your plan looks.

For each strategic objective, outline the benefits to the business of carrying it out, the initiatives necessary to meet it and the projects planned for each initiative. In this example the 'objective' is the overall goal that you want to achieve - for example, preventing data loss - the 'initiative' is something specific that will move you towards the objective - for example, decreasing phishing incidents - and the 'project' will be a specific part of the initiative - for example, compulsory email security training.

Your own terminology might vary, of course. You should use language that makes sense to you and that fits with the communication style of your business. The important thing is that you define, in clear and precise language, what you intend to achieve and how you plan to achieve it. This will be a living document and we will discuss below the need to be willing to change plans when necessary, so do not be concerned about committing yourself in writing to something that might not come to fruition. If you like, add a note to this effect in the introduction to your plan.

Quick wins

A quick win or two early on can do wonders for establishing your reputation within your organization. Given the importance of quick wins, these should not be left to chance. Look for opportunities to create them so that you build momentum. Once again, where you look depends on the organization. Perhaps some obvious measures have not yet been employed or you might be in a situation where all the low-hanging fruit has been plucked by your predecessor. However, our CISOs offered a few pointers on where to look.

"An example of a generic quick win might be, do you have your patching up to date? We're seeing all these companies failing at patching; if you find that patching is a problem, then maybe the company doesn't have a good tight policy around it," says Clint Lawson, CISO at MidFirst Bank. "You need to implement a policy, ensure that it gets sponsorship and move towards it. Your initial gap assessment might also find that the company doesn't have a password policy, they're not filtering Internet traffic, or they don't have endpoint protection. These are all examples of quick wins that you might find in some companies and they're all important to address."

Email security was highlighted as a strong contender for a quick win, for a number of reasons. First, email touches everyone across the company so there are few better ways of making yourself welcome than tackling a spam or phishing problem. Second, it's the kind of project that can be completed within the first 90 days, giving you a solid

foundation as you move out of the honeymoon phase of your time as CISO. And third, it cuts down on problems that could easily develop into something more serious. Every CISO we spoke to emphasized that email remains a significant avenue of attack, even after staff members have had training about email security. Everyone receives so many emails that it takes only a momentary lapse in concentration to click on the wrong link.

Another quick win is establishing a vulnerability management program or a patch management program. Many organizations will have these in place, but if they don't then both are good tactical measures that can help the organization in the short term and lay the foundation for programs you might deploy in the long term.

Endpoint security is another area to consider. Many enterprises are still using legacy AV, which most users hate and consider a necessary evil. Legacy AV has a poor reputation because of its performance overhead, which users notice particularly during a scan or when copying large numbers of files, and its low efficacy against today's threats. According to a recent SANS study, although antivirus was the tool most commonly used to detect the initial vector of attack, only 47 percent of attacks were detected this way. In recent years, new technologies have been deployed to solve the same problem in different ways. For example, using machine learning to defend endpoints, or simplifying the architecture using cloud and automation.

Machine learning and automation provides a good opportunity for quick wins. Modern attackers know what defenses they are likely to face and have methods for evad-

ing them. Enterprises that do not implement automation in the discovery and, especially, remediation of attacks will be left behind. They are likely to be targeted regularly by common malware that can easily evade traditional defenses and cause damage, putting the CISO in constant firefighting mode. The underlying quick win of automation is time-saving. It does not eliminate the need for a professional workforce, but it will remove the need to keep them occupied with repetitive tasks and free them to do meaningful work.

No one wants the next data breach to happen in their backyard. However, it isn't possible to block every conceivable security hole proactively. As such, the best way to be proactive is allowing the latest technologies, like AI, to do the work for you. This doesn't mean chatbots. Those are a nice gimmick but this is about using automation to prevent and clean up malware attempts, rather than trying to get machines to understand conversation. There is also a subtle difference between implementing AI technologies to proactively prevent endpoint breaches and AI that will discover what happened after a breach. Being proactive means investing in a security layer for the last mile, with multiple layers of protection and visibility, including AI and automation.

Finally, employee education is a strong contender for a quick win. Employees are the first line of defense in cybersecurity, so improving their understanding is immediately beneficial. Even if the company has security education plans in place, there is usually more that can be done because these programs are never really finished. They

also have the benefit of making you and your team visible throughout the company, which helps you to establish yourself. There are several ways to do this, from showing people how to be more secure in their work tasks, to helping them to apply security standards to their personal use of technology, and that good personal security will lead to better behavior at work. Some of the CISOs that we spoke to even mentioned writing regular security newsletters for distribution to the entire staff.

When plans go wrong

However well defined your plans are, you will find that they do not always run smoothly. In the first place, emergencies might arise. If your initial assessment of the company's cybersecurity landscape turns up a major vulnerability, for example, then your strategy will need to shift immediately to that. Worse, you may uncover signs of a breach and have to move into investigating and recovering from it.

These are rare exceptions, however. More likely, your plans will run into the common blockers that affect any organization. A 2017 study by Deloitte identified three common barriers to building "a more proactive and business-aligned security organization"[6]. First, leadership and resource shortcomings. This can encompass everything from a poorly defined or poorly funded security program

6 http://deloitte.wsj.com/riskandcompliance/2017/03/13/the-new-ciso-leading-the-strategic-security-organization/

to an IT director with a poor understanding of security strategy. Second, security that is inadequately aligned with the business, which most commonly means that the security team are seen as the 'blocking' department that prevents the rest of the business from being productive. And third, a poorly defined security organizational structure. This can mean that the CISO does not have the authority or position necessary within the hierarchy to direct meaningful change.

Ideally, if such barriers are present at your organization, you will identify them during the information gathering phases described in Chapters One and Two. If so, by the time you come to set out your strategy, they should either have been dealt with or you should be able to factor them into your planning. Removing these barriers will require support at board level, however. It is not something that the CISO will have the power to do by themselves.

Kevin Emert says he often compares strategic planning to driving from New York City to San Francisco. Your strategy is how you choose to travel; You could go by air or road, for example, and each of those choices would lead to other choices about the type of vehicle you use, and so on. He says: "Let's say you're driving and you get to Kansas and, all of a sudden, there's a road closure. You're going to have to take a different route. You still have the goal of getting to San Francisco, but now, due to problems outside your control, you're going to have to adjust your strategy."

Your cybersecurity strategy could meet similar roadblocks and preparing for those should be part of your strategy. Much of this is psychological. Avoid getting so wedded

to your strategy that you refuse to change or wait too long to change. Don't become convinced that pivoting means that you made bad decisions on your initial strategy. Trust that you made the best decisions at the time when you devised your original strategy and accept that the best decision to make now is to change your plan.

With that in mind, you should allow for a plan B. It doesn't necessarily need to go into your strategic plan, though it might. When confronted with circumstances that force you to change your strategic plan, the best response might be to bring forward something that was in the plan but not due to be worked on in the short term. On other occasions, it might be better to put a completely new program in place instead of whatever was in your initial plan. This will be a lot easier if you consider some of these outcomes in the first 90 days. For example, saying to yourself 'this is how I see my strategic plan working but if a breach were to happen then we would do this and this instead' or 'I plan to do this but a regulatory change affects this area of our business then I will start this program instead'.

Good planning means considering what happens when plans go awry.

KEY QUESTIONS

1. *Do you understand how risk appetite and risk tolerance balance in your organization?*

2. *Have you considered how your strategy will support your working style?*

3. *Have you assessed where the quick wins might be?*

4. *Do you have a plan B in place in case plan A fails?*

4. Conclusion

The CISO role is complex and covers a broad area. This book should have given you a sense of what the role looks like and how to approach it. The advice here can all be shaped to your particular circumstances.

In conclusion, let's recap the 12 questions that this book has asked you to consider.

1. Where are the boundaries of the cybersecurity estate?
This is becoming increasingly hard to grasp in an era of cloud computing and the Internet of Things but it is crucial to your security plans.

2. What are you trying to protect - and who from?
Every company has assets but they are different. Are you protecting corporate intellectual property from industrial espionage or customer data from thieves? What you are trying to protect will shape your approach to security.

3. What are the intangible threats?
These are the hardest to quantify but you need to consider where they might be.

4. Are you keeping an eye on the future?
New threats are arising all the time. You need to be sure that you can see what's on the horizon.

5. Do you know where you, as CISO, sit within the org chart and what that means?
Your place in the hierarchy will have a strong effect on what you can achieve and how quickly.

6. Are you going to be 'Dr. No' or 'Dr. Know'?
Our research strongly suggested that the latter is the best choice.

7. Do you understand the business well enough to really understand how risk affects you?
You have been hired for your technical expertise but being effective at your job will mean understanding how the business works.

8. Are you able to balance the day-to-day efficiently alongside ongoing projects?
Expect to find yourself beset by competing demands from the outset and make a plan for how you will deal with that.

9. Do you understand how risk appetite and risk tolerance balance in your organization?

Everything in business involves risk but companies have different views on how to balance it. Your strategy will have to fit within your company's risk appetite.

10. Have you considered how your strategy will support your working style?

Consider your working style - collaborative or individual, for example - and how your strategy will fit in with that.

11. Have you assessed where the quick wins might be?

Quick wins will be vital to establishing yourself in your new role and letting your colleagues know what you are capable of.

12. Do you have a plan B in place in case plan A fails?

Not everything will go according to plan. Try to consider what you would do if certain things go wrong.

Determining your answers to the questions above will help you to understand what the CISO role looks like for you and give you a headstart on the road to success.

Good luck!