90 DAYS A CISO'S JOURNEY TO IMPACT

VOL II

Forward by
Jeremiah Grossman

HOW TO DRIVE SUCCESS

Sponsored by SentinelOne

Table of Contents

CISO Intro

by Jeremiah Grossman

Chief. Information. Security. Officer. The person in charge of protecting an organization's information assets. The job title sounds so simple, even straight forward, and once upon a time it might have even been an accurate description of the role.

It used to be enough to make sure all patches were up to date, network firewalls were in place, intrusion detection set-up, anti-virus installed, and everything on the network properly configured, locked down, and hardened. Being a CISO was primarily technical in nature, but times have changed. Realistically, the only thing uncharged about the CISO job is the title.

Today, the responsibilities and skill-set required of a contemporary CISO have become much broader, all encompassing, and far more critical to the smooth running of the business. CISOs often require familiarity with new and highly sophisticated technologies such as Software Defined Networking, DevOps, Serverless, Containerization, IoT, Virtualization, Machine Learning, and Next-Gen everything in order to protect them. Not to mention The Cloud and all of its many facets. Then there is an ever expanding attack surface created by an explosive number of

new users, more data, and more devices needing to be safeguarded. The threats to the enterprise posed by organized cyber-crime, nation-state actors, and even hacktivists are very real and an ever present way of life — 24x7x365. Then many CISOs have to interact not only with their internal teams on technical matters, but also with the board of directors, journalists, regulators, politicians, customers, vendors, and partners on a wide variety of business level issues. The role of a CISO is certainly not for the faint of heart, but the multifaceted demands of the role are also why many find it so attractive.

Perhaps the best part of being a CISO job is change. Every day there is something different going on. The business is developing new products and services with new technologies, the attack techniques the bad guys are employing to hack them are advancing, and at any moment the job might kick in to a higher gear should an incident spring up expectedly. If you're not learning and teaching every day, you and your team will quickly fall behind. That's simply the nature of Information Security in general.

The major drawback is that a CISO's contributions are always difficult to quantify and justify in the ultimate language of business — dollars and cents. This is especially true when through skill and hard work, you have everything under control, nothing unexpected has happened, and your value is questioned. There never seems to be a 'win' condition; you're only noticed when failure strikes. If things do go wrong, such as a breach, then you're to

blame as the designated “chief scapegoat officer”. And of course everyone around wants to tell you how to do your job. There will always be others trying to convince you of what’s most important and how what your doing isn’t enough. “Just buy this point solution.”

I’m not here for that. I’m here to share some thoughts about ideas for how to think about the role of a CISO, it’s place of importance in the larger world, and what personality traits make for the most successful candidates.

Bruce Schneier once said, “You can feel secure even though you’re not, and you can be secure even though you don’t feel it.” When it comes to being a CISO, we have to keep both of these in mind. The people we serve want to feel secure, and when they do, that’s of tremendous value to them. People need to feel that there is someone they trust that’s protecting them, and should things go wrong, that person will also handle it well. Trust is what the feeling of being secure basically comes down to. At the same time, much of what CISOs do will never been known, understood, or appreciated outside of their peer group, the people that actually make things secure. In many respects, security people exist behind the scenes; they are the world’s silent protectors.

One of my favorite movie quotes ever is in Sneakers (1992), where Cosmo says, “The world isn’t run by weapons anymore, or energy, or money, it’s run by little ones and zeroes, little bits of data. It’s all just electrons.” How

profound. If you think about it, those who work in Information Security are collectively responsible for protecting the world's most sensitive information, it's biggest secrets, entire economies, and often even the life and liberty of the billions of people connected to the Internet. CISOs, the appointed leaders, represent the tip of the spear and the unsung heroes they rely on every day. While face down in spreadsheets, locked up in meeting rooms, and pouring over complex reports, let's not lose sight of the larger mission and what we're really here to do. To protect people. The protect the business. To protect the Internet.

Acknowledgments

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 Jenifer 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

Where do you start, especially with a job as broad as CISO? That's the question this book aims to address. The goal is to give you a clearer idea of what your first 90 days in a CISO role should look like. Every industry, every company and every CISO role is different, so we can't give you a guide on what you should be doing each day. However, we can give you a sense of direction.

The first 90 days of a new CISO's work can, roughly, be split into three. The first 30 days will be about getting the lay of the land and learning what you can about your new organization. The second 30 days are a useful time to put together your strategy and plan how you will go forward. And the final 30 days are the time to start executing your plan and trying to demonstrate some quick wins.

For a CISO who is new to the role, that will require a lot of learning. Carrying this out successfully requires effective communication. One thing we heard from every CISO

we spoke to for this book was that communication skills are vital. The majority of CISOs still come from a technology background, rather than a business background, and IT has a reputation for struggling with communication across the enterprise. That is a problem that new CISOs will have to solve. With user action being the dominant cause of breaches, good communication is essential.

Finally, effective CISOs need to be good managers, not only of their teams but also of themselves. Several of those we spoke to acknowledged that the breadth and complexity of the CISO role had initially been overwhelming and they had at first found themselves caught up in detail. Being effective means learning to find a balance between delegating when necessary and, when appropriate, being hands-on.

We hope that by the time you finish this book you will have gained some useful insights into how to fulfill your role. One idea that you will find coming up time and again is the notion of balance. The CISO's job is about balancing risks, balancing expectations and balancing needs. Like any balancing act, it is one that takes practice to perfect. For those about to undertake it, suggestions will no doubt be welcome.

There are plenty of ideas here, all of them recommended by some of the leaders in their field, with years of experience in the world of cybersecurity. We would like to thank all of them for giving their time and sharing their expertise to help bring this book to life. We are confident that it will help to make your first 90 days a smoother experience.

1. Learning

As described in the introduction, the first 30 days are the time for a new CISO to get the lay of the land. You need to learn about your new organization, its goals and its challenges. You need to be aware of any recent attacks it has faced and how they were dealt with. You will want to assess the current security situation and take a view as to how it might be progressed. You will be meeting key staff throughout the company and everyday users to find out what their view of security is and to establish buy-in for your efforts. Finally, it is important to acknowledge that learning continues beyond the first 30 days, and to put in place plans for continuing to learn as you make progress.

For a CISO, the learning process begins even before getting the job. As part of your research for the job interview, you will likely have done some due diligence by reading the company's website and news. In a way, the less you

find in the news, the better. If the company has been making headlines, it could be because it has fallen victim to an attack. Perhaps the fall-out from that is the reason why there is a vacancy at the CISO role?

Learn what you can about any recent attacks the company has suffered and how it responded. You might also find news stories explaining the company's goals or reports on new additions to, or departures from, the board. All of this can help you to form a picture of the company you will be joining.

However, it is possible to dig much deeper than that. As Alex Burinskiy says: "I talked to a company a while back and I pulled enough research on them that I knew roughly what level of patching their servers were at, so I had an idea of what their landscape looked like."

At the interview or shortly after taking the job, you should have established the budget available and how supportive the organization will be towards your efforts. This information will be crucial as your plans take shape.

Assess the situation

Once you have properly taken on your new role, the first task is to assess the state of the organization's security efforts. This entails first determining the organization's cybersecurity estate and existing risk. What are the organization's critical assets and who you are trying to protect them from? Once that is established, you can examine the cur-

rent protective measures and look for gaps. Each organization is unique: some will have thorough and well-managed security plans, in which case your priority will be looking for ways to improve them and keep them effective; others will have chaotic or poorly managed systems and you will need to do a significant amount of remedial work simply to get them fit for purpose.

Martin Littmann gives the following example: "Imagine an organization has historically believed that if you protect the perimeter - and as long as you are protecting the perimeter - then you are doing a great job but they have effectively done nothing within the perimeter to understand their insider threat. Or an organization may have strong firewalls, malware defenses and all that kind of stuff but they have VPNs and other connections to partners and other organizations. My question would be, have they looked at each of those other network connections to know that whoever is protecting the edge of those networks is not allowing traversal of malicious traffic into my network?"

Determining which situation you are in is a matter of spending the first few days of your new role asking a series of questions. How is the existing program validated? What benchmarks are available for measuring its success? What third parties does the organization rely on to share, store or process data? What security tools does it use and what else is available from the vendors to maximize their effectiveness?

Often, a fresh pair of eyes is all that is needed to see flaws in a system. Much as organizations like to plan and follow strategies, things often progress in an ad hoc fashion. A se-

curity tool is put in place and then a new vulnerability is found, which this tool does not address, so another tool is added. Over time the two tools might start to overlap, so that having both becomes unnecessary, or they might diverge, leaving vulnerabilities uncovered. A new CISO has a good opportunity to evaluate systems that have been altered over time and determine whether they can be rebuilt more efficiently.

What information sources are available to you, to help plan your security roadmap? Are there internal reports covering the areas that matter, and if not, how can you go about setting them up? What information did your predecessor leave behind? You might not want to follow your predecessor's path, but their reports and evaluations are still useful.

Consider is a full risk assessment for the organization. You will be doing these regularly anyway and starting one as soon as possible will give you a solid benchmark. It will identify the relevant threats in detail, determine your exposure and propose solutions. A risk assessment can also serve as powerful evidence for future spending on staff and security tools.

"I did a 90-day and then 180-day gap assessment," says Clint Lawson, CISO at MidFirst Bank. "This is a high-level gap assessment, it's not way down in the trenches. I used an ISO 27000 framework but there are several different frameworks out there, such as NIST, or, for a cloud-focused company, one from the Cloud Security Alliance (CSA).

"Once you choose a framework and go through the process, you'll have a sense of your strengths and weakness-

es. Then you can formulate your plan and present it to the board so that they know where you want to go and, hopefully, will provide sponsorship."

At the end of this process, you should have the framework of your strategic roadmap, which will help you to guide the organization, keeping in mind its existing risk appetite, available tools and the budget for new tools and solutions.

Meet the people

While you are assessing your defenses, you will be meeting your team and getting a sense of their skills and experience. However, you should make time to sit down with each team member individually, so that you can assess them properly. These are the people who will be, not only the ones carrying out your plan, but also the people who will project your security vision throughout the organization. Which staff members will immediately be able to help you to make an impact? Which ones might need more training to bring them up to the necessary level?

If this is your first CISO role, then it is possible that it is your first experience of managing a team of this size. We will look at managing yourself and your team in more detail in Chapter Three, but you should be mindful of your own managerial strengths and weaknesses while assessing your team. Which skills can you help to develop in your team? What areas might you need to deal with

through training and development?

Part of this process is about telling your team how you want things to function. Explain your management style and your vision for the team but ask for their feedback too. How do they work best? What do they think their KPIs - and those of the team - should be? Where do they think they need training? Soliciting feedback - even if you don't act on all of it - is likely to motivate them and build loyalty.

This last point is especially important in the security industry, where skilled workers are scarce and expensive. In the 2017 ClubCISO Maturity Report, three-quarters of respondents (73 percent) said they were having difficulty attracting or retaining good security staff either all the time or frequently[1].

As well as your own team, you need to devote plenty of time to meeting people across the company. Communicating effectively with them is examined more fully in Chapter Two. As part of your information gathering approach, you need to meet senior executives. What is their view of security and how can you raise awareness of what you are trying to achieve? For some CISOs, this 'political' aspect of the job makes them uncomfortable. However, having executive support for your program is essential, so you need to accept this part of the job. A 2016 Deloitte report warned that most CISOs "have to invest a lot of time to get buy-in and support for security initiatives"[2].

1 https://www.clubciso.org/wp-content/uploads/2017/07/Are-you-having-difficulty-attracting-or-retaining-good-information-security-staff.jpg

2 https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html#endnote-sup-8

Of course, you need to spend time meeting people across the business, at all levels and from all departments. This will naturally tend to lead you to talking to managers but try to meet other staff too. Understanding the goals and working practices of people across the business is vital to developing a security program that helps them to achieve their goals, without putting obstacles in their way.

"All users are different and they think about security in different ways," says Chris Carney, of the Meredith Corporation. "If you take some of our younger generation, Millennials, they're used to being able to control, customize and make things work in the way that suits them. Then we have other users working in the organization that are comfortable with not necessarily wanting to control and change their devices and applications. So, being able to be flexible with that and understand the user's perspective definitely helps."

Finally, don't neglect the opportunity to meet with vendors and analysts. Many CISOs avoid this because they consider it a waste of time but it can be useful, particularly in your early days with an organization. These meetings are a valuable source of market intelligence and insight. At the very least, you should aim to meet with the vendors of the products and tools your organization uses. Find out whether there are features that you are not fully exploiting, or processes that you could be running more effectively. Inevitably, if you plan to add new tools to your company's suite, or change existing ones, you will need to spend some time talking to new vendors - again, this is a good opportunity to get new perspectives on the challeng-

es you face and to learn more about potential solutions.

Analysts can also be useful figures to get to know because they will help you to benchmark your organization's approach within the sector. They are, of course, in the business of gathering information that they can sell to clients, so be careful what you share. However, used wisely, these are valuable contacts.

Keep learning

The learning process continues beyond 30 days, so use this time to lay the groundwork. First, strive to learn everything you can about the business and, if it's new to you, the sector in which it operates. With all of the above to handle, it can be difficult to accomplish this in the first 30 days, but you should be able to get a broad picture of how the company operates, its strategic goals and its challenges, such as regulation, competition and disruption. According to research by Digital Guardian, 59 percent of CISOs have a technology background, compared with just eight percent who have a business background[3]. Filling in the blanks in your business knowledge is an important task.

Secondly, consider finding yourself a mentor. The role of CISO is broad, complex and stressful. Having someone with experience that you can go to for support or advice can prove invaluable in terms of your professional devel-

3 https://digitalguardian.com/blog/anatomy-ciso-breakdown-todays-top-security-leaders-infographic

opment and effectiveness. Another way to find support and share expertise is to look for meet-ups in your area. These provide a good opportunity to learn what others are doing and what is working for them. Sometimes it will help to validate your ideas and at other times it will challenge them.

A useful way to keep up with conversation in your sector is to find relevant blogs, reports and other information sources. LinkedIn, Medium and various blogging sites are often good sources of discussion and expertise, which can help to shape your thinking or just keep you up to date with topical discussions.

Finally, make sure you put yourself out there by writing blog posts or speaking at conferences and industry events. Gathering your thoughts for publication or a presentation can be a useful exercise in itself, but making yourself visible within the community is another way to ensure that you keep learning. Many technology specialists who make the step up to CISO, do not prioritize this 'public relations' part of the job but it is a habit shared by many of the most successful CISOs.

KEY QUESTIONS

1. *What is the state of the company?*

2. *What is its security situation and where are the gaps?*

3. *Who are the people in your team and your organization?*

4. *How can you ensure that you keep learning?*

2. Communication

Effective communication can be the difference between success and failure as a CISO because the whole organization - from the board to the most junior staff member - needs to understand good security practice. Much of your success in executing your security strategy will depend on how effectively you establish communication within the organization.

If you have followed the suggestions in the previous chapter then you will understand the role security has played in the organization. As CISO, your task will be markedly different if the organization has, for example, a very clear, mature approach to security. In that case, communication will be less about education and more about ensuring effectiveness. On the other hand, if you are taking on the CISO role at a company that has not had a coordinated security plan, then your role will be much more one of evangelism.

Your learning phase will also have given you an un-

derstanding of the compliance architecture driving the business and the sector as a whole. Certain sectors, such as financial services, have stricter regulatory obligations and therefore the companies in these sectors are typically more sophisticated in their compliance processes. In other businesses, the notion of compliance itself is a new one and part of the CISOs role will be ensuring that the need for compliance and security is adequately communicated.

The support of the board will be crucial to your success. The CISOs we spoke to for this book were unanimous in their belief that every board understands the need for strong security and compliance policies. They have seen plenty of companies hit newspaper front pages after security breaches and they have no desire to be next. However, this does not always look the same in practice. Different boards have different appetites for security and compliance. Your relationship with the board will depend to a large extent on how much their appetite matches your goals. The closer the fit, the better.

"I am fortunate to have a CTO who came from a very security-focused company, so I have a really strong supporter on the board," says Jake Curtis, CISO of a large international media company. "Mainstream media reporting on data breaches and other security and data privacy topics has made C-level executives very aware of the issues, at least here in Europe."

If the board does not have as much of an appetite for security as you would like, then your job is again one of evangelism. A crucial consideration is how knowledgeable they are. Even one person on the board who is well versed

in security and technology will be a useful ally. A board that is entirely lacking in security literacy will of course require more education and evangelism.

The other consideration that will affect your ability to communicate is the corporate structure. The position of the CISO within the organization between companies. According to 2018 research by PwC, 40 percent of CISOs report directly to the chief executive[4]. Roughly a quarter (27 percent) report to board directors, a similar proportion report to the chief information officer (24 percent), while 17 percent report to the chief security officer and 15 percent to the chief privacy officer. These numbers add up to more than 100 percent, suggesting that some of those surveyed report to more than one part of the business. Interestingly, a 2017 report by Ponemon found that 50 percent of CISOs report to the CIO[5]. The discrepancy is likely an indication of the extent to which reporting structures vary.

Having assessed the lines of communication upwards, it is important to assess those going down through the organization. What is the support for security across the business? Is it typically viewed as an IT responsibility or do staff understand that security is everyone's responsibility? As above, the answer to this question will determine how challenging your job will be and whether you need to begin by laying the groundwork for better security.

At this point, you should have a view on the organiza-

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

5 https://interact.f5.com/rs/653-SMC-783/images/RPRT-SEC-1167223548-global-ciso-benchmarkUPDATED.pdf

tion's security stance and that of its sector; you should know your position in the hierarchy and how receptive the board is, and you should have a sense of how security is viewed throughout the business. Finally, you must grasp the business goals of the organization, not only so that you can be effective but also so you can shape your communication strategy accordingly. Find out the capital projects planned for the next 12 months, and examine any other plans the company has in place. These will be areas where you can make an immediate impact.

Play to your strengths

Once you have gathered the information above, you can make decisions about your communications strategy. Do you need to be a security evangelist, an educator or a facilitator? The answer is likely to be a combination of all three, so you will need to determine which roles you need to play, when and with whom. As Martin Littmann explains: "Security is not an IT function. It's not a goal to be achieved. It is a 'lifestyle change' for the corporation. Any lifestyle change has to be adapted to the audience that has to make that change." He adds that an effective CISO can help to bring about this change in formal meetings, email updates and informal face-to-face conversations. All of these techniques play a role, so a good CISO needs to work on their communication skills in a variety of settings.

Play to your strengths: if you know that you are a good

communicator in formal settings and less comfortable in informal ones, then make formal meetings your foundation. If the reverse is true, then create opportunities for more informal chats.

"People tend to discount the political aspects of living within a corporation," says Mr. Littmann, "and there are politics everywhere. In some cases they are big and in others they are small but you have to learn what those politics are and decide what give-and-take is necessary to accomplish your goals."

It's also easy to overlook communication skills as part of the CISO's toolkit. Having 'security chops' (as one CISO described it) is important, but the role is a people role, not just a technology one. Give serious thought to whether you need communications skills training before stepping up to the CISO role.

You need a good working relationship with the CEO and the board, of course, but there are other key relationships to build to be most effective as a CISO. First, build relationships with the IT leadership. Even if you don't report to IT, a good relationship matters because they are the team who will implement the tools you need to function, ensure that your programs run smoothly and so on.

Similarly, you should cultivate good relationships with the chief financial officer and the compliance officer (if there is one). ROI and payback are often intangible in security, which is why the field is often viewed as just a cost center. However, the ultimate payback is the absence of front-page newspaper headlines about the business. Most executives understand that, but the longer the company

goes without a public breach, the easier it is to get complacent. That's why the CISO needs to build relationships and provide constant feedback on what they are doing and why, as well as emphasizing the value.

Alex Burinskiy says: "The way that I've actually run this is by managing the relationship over the long-term and slowly bringing everyone up to speed. Once we have a good relationship, I can say 'Hey, you know, we're missing this component and we need to get it up and running' - and those teams will be ready to implement it as part of the roadmap before we hit any issues."

He gives the example of rolling-out anti-virus software, which is something that affects most of the business. You need to ensure that desktop users across the organization can continue to work and not be confused by new options or messaging. On the server side, you want everything to be able to run at full speed, without the server teams being hindered. And finally, for most businesses, you will want your customers to be able to access the data as they need it.

Burinskiy says: "You will be working with them very closely in the testing phases to make sure that everything goes as smoothly as possible and you want their buy-in. You might not always agree with their opinions and you can always decide to ignore their opinions but you at least want to get buy-in because it ends up helping you to create that win at the end."

Listen closely

The point about working closely with users is a significant one. All the CISOs we spoke to emphasized the importance of listening to your colleagues and their issues. You can only begin to protect them by truly understanding what they are trying to do. Through listening closely, you may discover that how people describe their jobs is, in fact, different from how they carry them out. Work to establish yourself as a trusted resource for the teams in your organization, be involved in decision making so that you can flag possible security concerns before they become an issue, and help to keep the security operation ahead of the curve.

While leadership approaches vary, what is not up for debate is that leadership is essential. The CISO has to be the visible leader of security within the organization, not a back-office figure that staff never meet.

In its 2018 Global CISO Report, ServiceNow identified 'Security Response Leaders' - those who stood out within the organization for their security capabilities[6]. The report said that the main qualities that set these individuals apart from others are: they are more focused on automation, especially for strategic tasks; they are tightly integrated with the rest of the business, especially IT; they say that a strong relationship with IT is crucial to their success; they see security as a core goal for the entire company.

Leadership styles vary, so the best way to lead the security efforts in your organization will be the one that you

6 https://www.servicenow.com/content/dam/servicenow/documents/whitepapers/wp-ciso-globalstudy.pdf

are able to implement most effectively. For example, Mr. Littmann says: "The most effective leaders are oftentimes the greatest servants. The reality is that if I am doing the right thing, if I am exuding confidence, if I'm exuding competence then that will be seen. If I listen to people and what their issues are and try to map it to what I'm trying to accomplish then they might end up making the decision I wanted them to make. When they get the win of being able to make the decision and I'm the one who is executing it anyway, then I'm a winner as well."

In a role that requires working across functions and developing relationships with those higher up the organizational chain, as well as lower down, you need to adopt a communications and leadership strategy that focuses on creating win-win scenarios.

KEY QUESTIONS

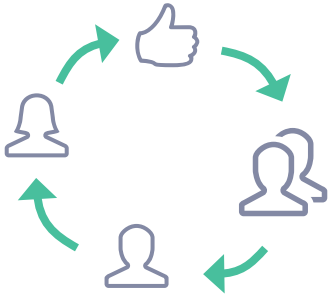
1. *What role has security typically played in the organization?*

2. *What is the support for security at board level - and elsewhere?*

3. *What is your communications strategy?*

4. *What is your leadership style?*

3. Managing your team (and yourself)



Assess your needs and your resources

As CISO, you will be taking over a cybersecurity team of some form. It's possible that you will be joining a company that has not had a dedicated cybersecurity team and therefore your first job will be to create one, but most companies have some staff in security roles. In many cases, you will find yourself taking over a mature team. Whether you find yourself at one of these extremes or somewhere in between, early in your first 90 days you must begin to take stock. Determine what the company's security needs are, how many people will be needed to service those needs and then look at the people you have available. You can find more information on this part of the process in Chapter One.

There is no ideal size for a security team. Among CISOs that we spoke to, a rough estimate of 10 to 15 people for a company of 5,000 was suggested, but this is by no means a

firm rule. Some small businesses could be very significant targets and therefore need a large team, while there are large businesses whose threats are mostly indirect and so a small team will suffice.

How you assess the talents of your team depends to an extent on your personal style. Some people will feel that they can tell during an interview whether a person is right for a role on their team and so sitting down with each staff member might be enough. Even so, you will also want to look at past appraisals for your team, if available, as well as any other information about their job performance.

Accreditations and qualifications tell you something about a person's capabilities, but most of those we spoke to cautioned against relying on them. They don't tell you how well a person has carried out their role, nor do they give you much understanding of other necessary skills that they may or may not have. For example, cybersecurity staff need to understand their customers and, for some, they will need to be able to work well in a supervisory capacity.

Finally, all of the above has to be done with the needs of the organization in mind. It might be that you have been recruited to move the cybersecurity operation in a new direction, in which case the existing team may not be right for the future, even if they have done an excellent job in the past. You need to consider whether, as well as having the right mix of skills, you also have the right emphasis on skills throughout your team.

Hiring

The growth in demand for cybersecurity expertise in recent years has rapidly exceeded the number of qualified workers available. New entrants into the job market rarely come with all the skills they need, and it takes time to train them. For some roles, experience is vital and that takes time to acquire. What's more, there are many job vacancies open at a given time, making this both a supply and a demand problem.

The ISACA's 2018 State of Cybersecurity report said that just over half of organizations are able to fill vacant posts within six months, while a third (32 percent) of companies take longer or cannot be filled at all[7]. Meanwhile, a 2017 survey by Dark Reading found that organizations were struggling to find recruits with technical experience and people skills (52 percent) and also having difficulty finding people with experience in their sector (52 percent)[8].

Lack of available talent drives up salary expectations, which is a challenge for smaller firms. Location is a factor, too. Capitals and major cities may be well supplied with talent, with fewer options in elsewhere.

Martin Littmann says that demand for cybersecurity professionals can attract "mercenary" people. He says: "I think you've got to craft your hiring process to mitigate for that factor. I'm going to hire people that are willing to

7 https://cybersecurity.isaca.org/state-of-cybersecurity?cid=pr_1222560&appeal=pr

8 http://www.informationweek.com/whitepaper/security-management-and-analytics/security-monitoring/surviving-the-it-security-skills-shortage/389923?gset=yes&-download=true

stay as long as I've been here."

The challenge is complicated by the fact that technical skills are not the only criteria for recruitment. As CISO you need to find someone who fits your way of working and the company's broader culture. As noted above, finding a cybersecurity expert with experience in your industry is difficult and that can have consequences in particularly complex sectors, such as those that are regulated.

How you approach hiring also depends on your style. Some CISOs will want to do everything themselves, others will prefer a more collaborative approach and want potential recruits to meet some of the team to see how they fit in. Alongside this, you will have to consider specific hiring practices within your company as mandated by the HR department. For example, some organizations have requirements that a certain number of minority candidates are interviewed. This is not always easy with a limited talent pool, but there are advantages to pursuing it. A homogeneous team can be homogeneous in its thinking; a team that better reflects the business and its customers can improve effectiveness and make for a fairer workplace.

Team building

"It's just like assembling a sports team," says Kevin Emert. "You can have all-stars on your soccer team but if they don't play together as a team, they're not going to win many games."

The lack of availability of talent makes it vital to retain your best people but, as Mr. Emert notes, that will only get you so far. Beyond that, you need to ensure that your talent can work together productively. Many aspects feed into this: your leadership style and how staff respond to it; the mix of personalities within the team; the skills make-up of the team - for example, is more than one person trying to lead on a particular aspect? If so, that will cause disruption; And finally, there are areas such as company culture. For example, if cybersecurity is not valued within the organization then the team will be less motivated.

You can affect all those factors, whether through clarifying the roles in the team, building relationships with staff or establishing the role of cybersecurity in the organization. You can consider a more explicit team building exercise, too, such as an away day. It can be tempting to shy away from active leadership if it doesn't come naturally to you, so find something that fits your style and lets you lead in a visible way

People need to feel valued in their work - that what they do every day is making a difference. They also want to feel challenged and engaged. This can be tricky to manage. Once people master a role, they can get bored and seek new challenges. It isn't always easy to fix that - sometimes there isn't a new challenge or a role with greater responsibility to promote someone into. Sometimes you need your best person to stay in the role for the good of the company. As CISO, your priority is the organization's needs but you must be aware of team morale and motivation. It will determine how effective your team is and how

likely you are to retain staff.

One way to work towards both goals is to have a development plan in place for all staff. This helps them to understand their career path, which will keep them motivated. They will know that you are regularly assessing their skills and performance. It will also help you to match your team's skills with your strategic plan. You will know, for example, that a key project for next year will have a staff member to manage it because you already have that person on a path that gives them the experience they need.

Lester Godsey says that he has a three-year plan for each staff member, which is reviewed annually. He adds: "I make it very clear to my staff that my goal is to meet the needs of the organization. If I'm doing my job well as a supervisor, then I should be able to align their personal development goals with those of the organization. If the two are ever in conflict, then the organization's needs come before the individual's but nine times out of ten I can align their personal goals with the organizational needs. And then that development plan helps drive building those skills and those areas of expertise."

Managing yourself

As a new CISO, managing your team is not the whole challenge. You must also manage your own time - and you will have more demands for your attention and more areas of responsibility than ever before. In this context, man-

aging your own time is not a trivial task.

Mr. Godsey says: “I don’t think brand new CISOs have a good grasp of what the strategic planning and foundational work of the job entails. Part of the problem is, when you're in that role, it's so big and wide, there are so many moving parts and there's no shortage of work. It's human nature not to know where to start.”

One CISO, who works for a major global manufacturer, says: “I took managing my calendar way too slightly at the beginning. It's really what you need to start focusing on when you take a CISO role: what is important? Because you will be dragged into a lot of meetings from the beginning. You end up spending two or three hours on email and then four hours in meetings. There’s only an hour left to do actual work! I need to focus on certain things so I've started blocking out days. On Friday, for example, I have almost zero meetings.”

As mentioned above, CISO is a C-Suite role and that means taking an enterprise view of the business, which does not always come naturally. Mr. Godsey warns against simply focusing on operational tasks because the enterprise-level work is overwhelming. He says: “I would tell new CISOs: you're better off trying to do something, even if it winds up not working out the way you think it will, as opposed to being frozen in action, and just continuing to just do operational stuff. That's worse.”

It is important to stay open-minded as you settle into your new role. If you have changed companies, or even sectors, to become CISO then this is especially true. Don’t assume that the way that you have always done things is

either the only way or the desirable way. You will learn a lot about other ways of accomplishing tasks.

One CISO told us: “The other thing I had to learn, as a CISO, was to let things go. A CISO role has a lot of functions but you need to understand, whatever your background, that you might need to let things go and take a higher stance. For example, I had to learn not to put my fingers into operations anymore and to ask my Director of Operations to do that job.”

One major challenge of being CISO is to represent the cybersecurity team across the company. You need to be spending significant amounts of time building relationships, with the board, with department heads and with ordinary customers in the business. You need to ensure that you allow time for this in your diary. You also need to carve out time to meet with your team, to meet vendors and to be an active voice within the cybersecurity community.

Doing that will mean less time managing the daily tasks of your department. Delegate that work to your team and trust them to get the job done. Don’t be a ‘helicopter’, hovering above your team and watching them carry out every task.

Alex Burinskiy says: “If you hire great people, then let them do great work. If you don't trust them to do great work, then you probably shouldn't have hired them in the first place; you're kind of wasting your time by being a helicopter.”

KEY QUESTIONS

1. *What skills are available to you and do they match the organization's needs?*

2. *How easy will it be to hire talent to fill the gaps?*

3. *Can you keep your team engaged and motivated while still meeting your goals?*

4. *Are you able to manage your time efficiently and willing to delegate?*

4. Conclusion

A lot can happen in 90 days. It is certain that even after you have read this book and planned out your first 90 days as CISO, you will find that certain things refuse to go to plan. Nevertheless, we hope that this book will provide enough direction that you will be able to weather such storms with minimal disruption.

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

1. What is the state of the company?

Hopefully, your research at the interview stage will spare you any nasty surprises, but you need to learn everything you can about the company's security situation early in your first 90 days.

2. What is its security situation and where are the gaps?
No security system is flawless so identify the gaps and decide whether they are acceptable, given your objectives.

3. Who are the people in your team and your organization?
Your team will be vital to your success as CISO, while your colleagues in the wider organization are your customers. You need to get to know both groups.

4. How can you ensure that you keep learning?
Find ways to continue to learn on the job, not just from colleagues but from blogs and online news sources and from conferences and events.

5. What role has security typically played in the organization?
If you are coming into a culture that understands the need for cybersecurity then your role as a communicator will be significantly different than if you are joining a firm with little security experience.

6. What is the support for security at board level - and elsewhere?
The more support you can draw on, the easier your job will be. The question is whether you have to build support early or whether it is already in place.

7. What is your communications strategy?
The appropriate communications strategy will depend to a large extent on who you most need to reach and how open to your message you expect them to be.

8. What is your leadership style?
Do you need to be an evangelist, an educator or an enforcer? What you have learned about the organization will help you to determine how you will lead.

9. What skills are available to you and do they match the organization's needs?
If the organization is changing its security strategy then the staff you have available may not have the skills you need. You might also decide that your team will need new skills in the future.

10. How easy will it be to hire talent to fill the gaps?
Recruiting talent in IT security can be difficult and is affected by many factors including how much your company can afford to pay and what size population you can draw on.

11. Can you keep your team engaged and motivated while still meeting your goals?
Retaining staff is essential because recruitment is so challenging. Consider the kind of program you will put in place to allow your staff to progress.

12. Are you able to manage your time efficiently and willing to delegate?

Once you have your team in place, you need to trust them to get on with the job, while you deal with strategic concerns.

Shaping your answers to the above questions will give you a plan that will guide you through your first 90 days as CISO and, hopefully, set you on the path to success.

Good luck!