Mighty Guides

The New CISO:
From Technology to Business-Focused Leadership

25 CISOs Share Expert Advice on
How to Make it in the "C-Suite"

SPONSORED BY:

FORTINET®

TABLE OF CONTENTS

INTRODUCTION

In recent years, the chief information security officer (CISO) has emerged as a new position among executive ranks. This development is not surprising: Information is the fuel that drives businesses operationally and strategically, and securing that information has become critical in ensuring solid business performance.

Just as the chief financial officer role emerged in the 1980s and the chief information officer position came into its own in the early 2000s, we are now in a period of role definition for the CISO. What exactly is the CISO supposed to do? And what skills does a CISO need to have? Newly minted CISOs are not the only ones asking those questions. CISOs experience some of the shortest tenures of anyone on the executive team.

We decided to look more deeply into the question of what it takes for a CISO to not only succeed in the enterprise but also have a positive impact on the business. With the generous support of Fortinet, we contacted 25 CISOs and asked the following question:

What advice can you offer a new CISO to help transition from technology-focused leadership to business-focused leadership?

In many ways, the answers provided by our experts reflect the still-emerging character of the CISO. The line between strategic and operational responsibilities of this position is clearer for some than others. That is partly a reflection of the different roles security plays in different businesses, and where the CISO falls in the reporting structure. However, the experts broadly agree that today's CISO must have a good understanding of both the business and technical implications of security strategy.

I found the answers to this question fascinating. I'm sure the advice contained in this e-book will help CISOs succeed in their role and provide insights into how effective cybersecurity strategy strengthens business performance.

All the best,
David Rogelberg
Publisher

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

© 2016 Mighty Guides, Inc. I 62 Nassau Drive I Great Neck, NY 11021 I 516-360-2622 I www.mightyguides.com

MARC OTHERSEN

CISO
Hess Corporation

Marc Othersen, CISO for Hess Corporation, a global energy exploration and production company, has more than 9 years' experience managing information security programs for companies, including Hess, LyondellBasell, and META Security Group, and more than 11 years' experience establishing and transforming information protection programs for Fortune 500 companies as a practice leader with organizations, including PwC, Ernst & Young, and Deloitte & Touche. He has performed analysis of information security trends, markets, and vendors as an industry analyst for Forrester Research.

Marc Othersen has three key pieces of advice for the young CISO who hopes to remain successful for decades to come:

- **Follow the money.** For Othersen, following the money means either getting your master of business administration (MBA) degree or attaining its equivalent in raw business. "You have to understand how businesses work," Othersen declares. "Not just your business, but businesses in general." Everything a CISO does must tie back to a business-function context, he says. Therefore, having a CISO grounded in business methods, balance sheets, and communications pathways is crucial. It might be unnecessary to go back to school—many books and online education programs teach those skills. "But you most certainly should know what an MBA program would teach," he says.
- **Understand risk management.** Once you understand business holistically, you can begin understanding the specific risk implications of critical IT system breakdowns, intellectual property thefts, and cyberattacks to your own business. Ground yourself in the discipline of risk management, and align yourself to the goals of enterprise-wide risk management. "What the CISO brings to the table is a specific perspective on risk areas that belong in the cyber world." If you master that idea, you can speak knowledgeably in the language of executives and help them to understand how your work helps them meet their objectives and protect the business.

KEY LESSONS

1 **To be truly effective, a CISO needs holistic, MBA-level business knowledge.**

2 **A CISO is a business leader who must have a seat at the table when enterprise-level decisions get made.**

> *"What the CISO brings to the table is a specific perspective on risk areas that belong in the cyber world."*

- **Learn soft skills.** There is a common thread to Othersen's advice. "It all has to do with communication—clear, concise communication," he observes. That means becoming deeply knowledgeable about such matters as threat intelligence—you cannot communicate what you do not understand, he says. But it also means developing a capacity to speak about threats without generating panic or being dismissed as a doomsayer. After all, most threats never materialize. He sharpened his own soft skills by joining numerous industry advisory boards and various committees within his own company. It has meant taking on additional tasks and responsibilities, but it has also put him in a position to watch and learn from other skillful communicators. "Being able to look through somebody else's eyes and understand their side of the conversation is part of those softer skills," Othersen states.

> "It all has to do with communication—clear, concise communication."

Othersen's eyes were opened to these lessons several years back when a company he was working with engaged in an asset divestiture. Not realizing there were cybersecurity risks involved, business leaders left Othersen out of the conversation. Being a little greener at the time, he did not insert himself into the discussion. That was a mistake, he says.

The company invited bids for purchase of its assets. What executives failed to understand—and would have learned had Othersen been at the table—is that several prospective buyers had previously been cyberespionage targets and represented a security risk. "Of course, then we were targeted and attacked," Othersen notes.

Executives also failed to understand internal threats. When a group of employees learned they were part of a divestiture, the less scrupulous among them began copying and uploading directories of confidential contacts to take with them. Othersen could have restricted access to sensitive intellectual property assets ahead of time had he been involved in the sale. "There were failings on multiple parts," he says. "Definitely on my part for not pushing harder for integration at the executive level."

Cyber is not fundamentally a technology issue, Othersen emphasizes. "It is an enterprise-risk issue and it needs to be addressed at the top as an enterprise risk," he says. "That is one of the big lessons that I got out of a lot of these battle scars."

He learned yet one more lesson that he feels he can pass on. He now knows that as a CISO he is a business leader who must be at the table when big decisions get made—just like the company's general counsel or chief financial officer. "If you can't get comfortable with that idea, then you are not going to survive as a modern CISO," he warns. "Because that is the role that needs to be filled."

WILLIS MARTI

CISO
Texas A&M University

Willis Marti is CISO for Texas A&M University. He previously served as director of networking and information security at Texas A&M while also teaching senior-level courses in networking and information security in the Computer Science Department. In addition to holding a master's degree in computer engineering from Stanford University, Marti served as a commissioned officer in the Air Defense Artillery and went on to contribute in the private sector at companies such as TRW, Martin-Marietta, and Sytek.

Website

Willis Marti believes that a good CISO should exhibit leadership in dealing with people. "Things are changing so rapidly that just being technically qualified doesn't make for a CISO," says Marti. A CISO is no longer an individual contributor once they reach that level within the organization; he or she must lead and direct other people's individual contributions. In making the transition from geek to leader, the key is to continuously develop leadership and people skills.

Demonstrating the ability to think and communicate with a focus on business needs is critical to success. When making the transition to CISO, it's important to realize that, "When you're selling yourself, it's not as a super geek. It's as someone who wants to relate to other people and their needs," explains Marti.

Doing so begins with understanding the challenges your business colleagues face. What are their desires and priorities? If a CISO talks to marketing professionals about restricting the availability of information flowing out of the organization, for example, such a statement may be viewed negatively or considered an obstacle to success. "You need to explain the problem to them in their terms because you're not going to convince them of your point of view. You have to relate the problem using a point that affects them," Marti advises.

KEY LESSONS

1 **A CISO needs to have a keen understanding of the challenges and priorities your business colleagues face.**

2 **A strong understanding of how the business handles finance and cost-justifies projects is essential for a senior leadership role.**

> *"When you're selling yourself, it's not as a super geek. It's as someone who wants to relate to other people and their needs."*

Upon reaching a senior level, it's imperative to understand how the organization handles finance, as well as the methods used to cost-justify projects. A CISO needs to know the budgetary limitations within the organization. No one has an infinite budget, and that budget has to be divided among different types of projects—both people projects and hardware- and software-oriented projects.

Ultimately, the CISO has to demonstrate that the resources required for proper information security are more important to the organization's success than other items. That requires an in-depth understanding of what the organization does, not just the technology employed to support it. "Bankers are not there for security, they're there to make money or to loan money or to manage it. At a university, they're there to get people to graduate. Or to get grants. You need to realize your position in the hierarchy and how your work supports the organization's mission," Marti says.

A CISO will also have to be prepared to have his or her proposals rejected at some point. In the end, the job requires presenting one's best judgment along with making the best case possible, but it's the chief executive officer (CEO) who will decide. "If you want to stay in the organization, that's the way it's going to be," says Marti. "The CEO might make a bad decision, and then you have to live with it. You have to be able to tell them I don't agree and this is why." For that reason, it's important to have a strong relationship with the people above you in the organization. A CISO will need to be mentally prepared to be overruled at some point, because it will inevitably happen at one time or another in one's tenure.

By developing the ability to lead people, communicate in business terms, and make a strong case for information security as a company priority, a CISO can make the critical transition from geek to leader. It takes continuous work and personal development during the course of a career, but it is an invaluable and necessary step for future success.

> "You need to realize your position in the hierarchy and how your work supports the organization's mission."

TO LEAD AS A CISO, HAVE THE IMPORTANT CONVERSATIONS

REED WILSON

CISO
Nu Skin

Reed Wilson is CISO and global infrastructure architect at Nu Skin, a billion-dollar direct sales company with offices in more than 50 countries. Focused on security, he directs security and infrastructure for Nu Skin, and consults with many governmental agencies and enterprises. He centers on what he terms "technology translation" and visibility into information's security at rest and on the fly. Wilson is a CISSP and holds many security-focused certifications.

Website

It's not easy to identify the exact moment at which a CISO has transitioned from technology geek to business leader. "There's no way I can point back and say this one event or this one seminar or discussion actually made me more business-focused and able to communicate with the business," says Reed Wilson. For CISOs aiming to develop these skills, he recommends dedicating the time to build personal relationships.

"One thing I do is take a stroll for anywhere from five minutes to an hour," he says. "I have zero agenda, no idea that I have to meet with this person and talk about this particular project or this particular issue." Seemingly minor chats with the colleagues he's run into on these strolls have created opportunities for partnerships on a project or better cooperation from his colleagues on implementing security controls into a new product that they plan to launch.

KEY LESSONS

1 **Transitioning to a business leadership role requires building personal trust with colleagues.**

2 **Important security issues are more likely to come up in informal conversations than they are in formal meetings.**

Trust is the key ingredient for these important dialogues to happen, and building trust takes time. "It's this idea of being able to talk to people and being able to make sure that they trust you. They can come to you and say, 'Hey, I'm having this problem, or I see this as a hurdle,' and they can talk about it instead of trying to hide it or minimize it or checklist it to make it go away," explains Wilson.

> *"They can come to you and say, 'Hey, I'm having this problem, or I see this as a hurdle,' and they can talk about it."*

TO LEAD AS A CISO, HAVE THE IMPORTANT CONVERSATIONS

Developing a high level of personal trust is critical for anyone in the CISO role, and it can increase his or her leadership standing within the organization. It also provides a safe environment for important conversations about business issues that might not otherwise take place. In one seemingly casual chat, Wilson discovered that a business executive with whom he worked had a pressing security concern that needed his partnership. “It came out through 10 minutes of discussion that she was worried about a project manager that was handling a new project,” he says. “This led to more discussions in which we got to the bottom of her concerns. The real issue was the fact that they were worried about a project timeline to the degree that the timeline was in tension with our checklists for taking security precautions and addressing application vulnerabilities.”

It’s important for CISOs to note that most of these open, frank conversations about critical issues do not take place in formal meetings. It can be difficult for people to speak up and make themselves vulnerable when they are in a room with a group of their colleagues. As a result, the frank and open exchanges that are needed might not take place, even at the meetings where they are explicitly listed as the agenda items for discussion. “I’ve certainly found that when talking one-on-one with people, we’ve had far better communication about security needs. Those issues have then been able to make their way into our plans and our goals. If we were sitting in a formal meeting, it’s likely that only half of these issues would come out,” says Wilson.

By making it a priority to build relationships within the business, a CISO will ultimately be more effective in protecting the organization from security threats that might otherwise be left unmentioned. Building the personal trust and confidence required to carry out a CISO’s role takes time and patience, but it is well worth the effort.

> “I've certainly found that when talking one-on-one with people, we've had far better communication about security needs.”

SUZIE SMIBERT

Global CISO
Finning International

Breaking the typical CISO mold, Suzie Smibert is making a mark in the global information security community as an innovative and benchmark-setting information security executive. As the global CISO for Finning International, Smibert is responsible for enterprise information security and risk and compliance management for Finning in the Americas, the United Kingdom, and Ireland. Working with senior leadership, Smibert provides security leadership, vision, and experience. Before Finning, she was the global information security manager for Agrium with responsibilities spanning four continents.

Twitter I Website

Becoming a business leader begins with having humility and letting go of being the smartest technical person in the room, advises Suzie Smibert. "The technical background is what got you to be a CISO. What will make you successful as a CISO is your business acumen," she says. If you know you have a gap in your understanding of the business, start by finding a mentor. She suggests consulting the risk office, the chief financial officer (CFO), and the corporate secretary, who can assist in a few key ways.

If your organization has a risk officer, they can offer valuable guidance. "When you're trying to present to either your board or your senior executives, run that presentation through your internal coach and have them critique it," Smibert advises. "Be open to their feedback in how you could best adjust it so that your audience will understand your key points, and you can be confident that your content is aligned with the business objectives."

Risk officers are also well positioned to educate the CISO on how the company manages issues of risk as a whole. "A risk in the supply chain is no different than a risk in IT," explains Smibert. "We have to mitigate similar things and the risk tolerance to our leaders is the same".

KEY LESSONS

1 **To build the business skills required of a CISO, consult the risk officer, CFO, and board secretary for coaching and guidance.**

2 **At the CISO level, particularly when presenting to the board, executive presence is essential for effective leadership.**

> *"The technical background is what got you to be a CISO. What will make you successful as a CISO is your business acumen."*

"If a CFO or a chief operating officer (COO) is really risk-averse in the supply chain or transport management operation, there's a good chance he will be risk-averse in IT as well. So understanding that will help you navigate." Partnering with a risk officer can assist the CISO in better understanding how the business operates in regards to risk.

In addition, a CISO must have a strong command of finance. "Every business decision boils down to a number: return on investment, cash flow, and so on," says Smibert. "You need to understand that, and who better to teach you than the CFO?" Because IT often reports to the CFO, consulting them for coaching or mentoring is a great opportunity to develop that knowledge. If your ultimate career goals lie beyond the CISO role, perhaps as a chief risk officer, COO, or even a CEO, Smibert recommends pursuing a master of business administration (MBA) degree or an executive MBA, which can be invaluable in building the executive-level business acumen required for those positions.

When working on your skills in engaging with the board, reach out to the corporate secretary. If you need to get to know your board better, get face time with them, or get feedback on your presentation, the corporate secretary can advise you on the right approach. "The corporate secretary knows the board members, their likes and dislikes, and likely some personal things about them that will help you accelerate building your relationship with them," Smibert says. This guidance will allow you to be more relevant and effective when communicating with the board.

When presenting to executive leadership or the board, executive presence is key. A CISO who cannot articulate what they are trying to achieve and the purpose behind it will not succeed. "Sometimes we only get five minutes on the board or two minutes in passing with the CEO," says Smibert, "You need to be able to inspire confidence the minute you walk into the room." A perfect way to develop those skills is by pursuing public speaking opportunities through industry working groups and committees, where you can refine your presentation skills before a group of your peers.

> "When you're trying to present to either your board or your senior executives, run that presentation through your internal coach and have them critique it."

Advises Smibert, “It’s stressful—you have to prepare for it—but it will teach you or force you to learn the skill of reading a room, having a proper cadence when you talk, proper elocution, and how to explain your idea in simple terms that will be easily understood by your audience.”

Building the skill sets required of a CEO takes time and tenacity, but most of all it requires a sense of curiosity about the business and a desire to better understand what it is trying to achieve. By closely partnering with business colleagues who have deep knowledge of the organization’s approach to risk, its methods for handling finance, and the people who serve on its board, a CISO can refine these abilities and become a true leader who consistently delivers value to the company.

EVEN THE BODYGUARD NEEDS TO KNOW THE BUSINESS

KEVIN LYNN MCLAUGHLIN

Deputy CISO
Stryker

Dr. Kevin L. McLaughlin, a U.S. Army veteran who proudly served for 11 years, has compiled more than 35 years of law enforcement, corporate, and cybersecurity experience. McLaughlin has been involved in cyber investigations, SWAT, and anti-terrorism activities as well as executive management for cybersecurity teams. McLaughlin has briefed corporate boards of directors on cybersecurity, created information security programs, conducted information security strategic planning, designed information security solutions, investigated more than 700 cyber cases, and handled numerous cyber incidents.

Twitter | Website

Dr. Kevin L. McLaughlin is a tough-talking former police officer and Special Agent turned deputy CISO. He chafes a bit at the way his job is sometimes perceived as executive-level, and he should therefore act more like a polished executive. "You hired me to be a bodyguard, not speak your language," he says. "Do you really care if I sound like a Harvard graduate?"

At Stryker, McLaughlin has the luxury of approaching his job that way. His CISO is Alissa Johnson, a former deputy CIO for the Obama White House. She is a legitimately polished business executive, he says, leaving him free to perform his chosen role as the cybersecurity bodyguard who keeps the bad guys at bay. "Having both those tools makes us a really good team," he observes.

McLaughlin's career experience includes a seven-year stint as CISO at the University of Cincinnati, so he understands the CISO role. His point is that you don't have to become fluent in the polished phraseology of a Wharton master of business administration to do his job. You do, however, need to understand how cybersecurity affects the bottom line. Toward that end, he offers a tip: Set aside two to three hours a week to read business books. If you want to tap into how your bosses think, find out what books they are reading. "I think you should be well versed in business," he says. "You have to educate yourself in that realm."

KEY LESSONS

1. **The CISO does not necessarily need to think or act like a polished executive, but understanding the business is an imperative.**

2. **When framing communications with executives, use terms and analogies that reflect their personal experience.**

> *"You can't make assumptions that people have the same frame of reference."*

Sponsored by: FORTINET

He has another piece of advice to the incoming CISO struggling to make the transition to a business-focused leadership role.

"Understand that people don't know what you know." He illustrates: "If I say, 'Oh, man, ransomware is really bad,' to executives, they don't even know what ransomware is in many cases," he says. "You can't make assumptions that people have the same frame of reference." He likes to frame conversations with senior leaders to reflect their personal experiences. Using analogies, he notes, is an effective tactic.

"They're easy for people to understand," McLaughlin says. "When I am talking to executives about why they don't have to protect everything, I use the analogy of protecting a house. I might live on five acres, but I don't protect all five acres. I protect what is important." He learned this strategy the hard way. Years ago, as a young CISO, McLaughlin reported to a chief information officer (CIO) who had a deep business background. He assumed they both were technically minded, so he would be understood if he framed a budget request through the prism of ITIL best practices. Not so much. "I was talking about configuration and change management," he recalls. "I just missed him completely on how I was framing it."

He saved the day by getting to know more about the CIO. He read the CIO's blog posts, took his direct reports out to lunch, talked to his students, and researched him on LinkedIn. "Then when I went back, I framed the conversation more within his life experiences so he understood what I was talking about," McLaughlin recalls. He got his budget request approved.

> "When I am talking to executives about why they don't have to protect everything, I use the analogy of protecting a house."

EVEN THE BODYGUARD NEEDS TO KNOW THE BUSINESS

When making a formal presentation to senior leadership, McLaughlin suggests creating a short list of bullet points ahead of time and sticking to them. Include these items:

- Where are we?
- How are we doing?
- What do we still need to do?
- Where do we need help from executives?

If there is time, walk them through your most recent accomplishments. But gauge the room, McLaughlin cautions. Executives might not be interested in listening to you applaud yourself. “Really,” McLaughlin remarks, “they want to know that their money is well spent, what you are doing with it and—oh, by the way—are you done, or do you still need more help?” If you fail to provide that focus, he warns, “You are just giving a briefing for the sake of giving a briefing. And there is not a whole lot of value in that.”

CISOS MUST UNDERSTAND THEIR POSITION IN THE HIERARCHY

PHIL FERRARO

Cybersecurity Consultant and Global CISO
Phillip J Ferraro LLC

Phillip Ferraro currently is an advisor to C-suite executives and board-level directors. He previously served 15 years as a global CISO in Fortune 500 organizations and the U.S. federal government. He provides extensive and demonstrated knowledge on cybersecurity risk management, develops and implements world-class cybersecurity programs designed to protect and defend against the world's most sophisticated attackers, and ensures compliance with multiple regulatory standards.

Website

Phil Ferraro provides security consulting to many kinds of organizations. From his perspective, the CISO must understand where they are situated in the organization, and they need to understand their relationship to the chief information officer (CIO). The CISO and CIO have different roles. A CIO is responsible for the operation and maintenance of the network, systems, applications, communications systems, and a broad spectrum of technology in the enterprise. People within the CIO reporting structure might implement security technology such as firewalls and other security tools, along with other technology solutions for the business, but the IT team is not typically a security organization.

A CISO is responsible for ensuring that the actual level of cyber risk in the enterprise is aligned with the risk appetite of the business, which is defined by the board and executive leadership. The CISO's team is responsible for mapping out the security strategy and making sure that all systems and security solutions are configured correctly to deliver the appropriate security posture for the business. "Another way of looking at it is the CIO reporting structure is the implementer, and the CISO reporting structure are the auditors," says Ferraro. "Ideally you want those functions separated."

Organizations handle this differently, with some having the CISO report to the CIO. That can work if the CIO really gets security. However, if the CIO doesn't get security, this setup will make the CISO's job a lot more difficult. Ferraro says, "In any organization, the CISO and CIO will need to work closely together."

KEY LESSONS

1 **The CISO must understand where they are situated in the organization, and they need to understand their relationship to the CIO.**

2 **The CISO must be able to show the business impact of a risk as well as the business impact of actions that would minimize that risk.**

> *"In any organization, the CISO and CIO will need to work closely together."*

CISOS MUST UNDERSTAND THEIR POSITION IN THE HIERARCHY

Ideally, the CISO will be a peer in the C-suite, because to do the job well, the CISO needs to educate the C-suite about seeing cyber risk as business risk. The CISO must be able to show the business impact of a risk as well as the business impact of actions that would minimize that risk. The effective CISO will act as a business leader who enables the organization to be as innovative, creative, and productive as possible while operating within tolerances defined by that organization's risk appetite, which is set by the board and executive leadership. It is difficult for the CISO to accomplish these things if he or she is buried in the organization and does not have a high level of visibility.

Ferraro has found there are typically three types of CISOs:

- Those who are technical and came up from the technical side of IT. These CISOs are good at what they do, but they lack people and executive management skills. They have difficulty communicating in terms of business risk and impact on shareholder value, which are things the board and C-suite care about.
- Those who are good in executive presentations. They look good, they sound good, and they speak the language, but they don't truly understand how the technical nuances can affect the business.
- Those who have a deep technical understanding and excel at executive program management. These are the rock stars. They have it all.

To be an effective CISO in the C-suite, you must be the third type. This CISO needs to be able to walk into a board meeting and give a concise, 15-minute executive presentation, in a language the board understands. This CISO can then walk out of that meeting, take off the tie and jacket, sit down with a room full of IT engineers, and actively participate in the technical discussion. It takes time to develop these skills. Ferraro says, "Like any other career, it takes experience, education, having good mentors, and networking in the right groups."

> "Like any other career, it takes experience, education, having good mentors, and networking in the right groups."

RICHARD RUSHING

CISO
Motorola Mobility, LLC

As CISO for Motorola Mobility, LLC, Richard Rushing participates in corporate, community, private, and government security councils and working groups setting standards, policies, and solutions to security issues. He has developed an international team to tackle the emerging threats of mobile devices, targeted attacks, and cyber crime. He has developed and deployed practices and tools to protect intellectual property across the worldwide enterprise. An in-demand international speaker on information security, Rushing has presented at many leading security conferences and seminars.

Twitter | Blog

It matters little whether you are a new outside recruit or are being promoted from within the company after 20 years of service. Any new CISO can fall into the trap of strategic misalignment with the business, cautions Motorola Mobility CISO Richard Rushing. Avoid getting caught up in information security's technical aspects, Rushing advises. You might wind up arguing about the technical merits of a next-gen firewall procurement for hours before executives who are reluctant to open their purse for yet one more piece of nice-to-have technology. "The stick is in the mud and you've lost it," he notes. "You're not moving anything forward."

There is another way. "Go back and say that this next-generation firewall replaces these other six things that we have other boxes for—which saves us $100,000 in two years' time," Rushing suggests. "If you had that conversation, they'd go, 'OK!'"

KEY LESSONS

1 **As a CISO, it is important to identify what drives the business, and place all emphasis there.**

2 **The good news is that the path to progress is open; hackers have taught executives that solid information security is crucial.**

Here is Rushing's advice for a young CISO transitioning to a business focus:

- **Understand your business' emphasis.** The new CISO must identify what drives the business, and place all emphasis there. Sell your services to the business the same way every other department does—by focusing on savings and costs, he says. A shortcut to gaining insight into your particular company's business emphasis is to read through presentations that were given to leadership in the past.

> *"One of the most important functions of the CISO is marketing their organization to the rest of the business."*

"Everything that has a dollar symbol on it. Guess what? You've got to have a dollar symbol on it as well," Rushing emphasizes. "This is not something you are going to get coached on. It's kind of expected: Match our template."

- **Become a marketer.** If you argue that you need $1 million to move the cybersecurity needle from a 2.4 to a 3.5 rating on the maturity scale, you probably are not making your best possible case. CISOs need to be more than just masters of information security, Rushing says. They must become masters of messaging. "One of the most important functions of the CISO is marketing their organization to the rest of the business," he says. Communicate clearly and tirelessly the importance of the services you oversee, he urges. "I don't necessarily have to go broke moving the dial if I can get buy-in," he says.
- **Seek out friends and peers.** If you are being promoted from within, chances are you already know the key senior directors or vice presidents from long-term experience. "But if you don't," Rushing advises, "you need to pay a visit to them and understand their problems, issues, and concerns." Unfamiliarity may not breed contempt, but it could breed apathy. "Executives can't engage you if they don't know you," Rushing states. "No one is going to pick up a phone that has a magic button that says, 'Call CISO.'"

Rushing feels that the time he has taken to develop those relationships has paid off handsomely. "If there is a problem, my CEO is in my office or calling me on the phone," Rushing says. "He couldn't care less where I am reporting to—if he has a problem, I'm going to get a phone call or he is going to be waiting in my office wanting answers. And that is perfectly fine with me." He has a simple term for relationship building: "We call it getting a seat at the table."

> "Executives can't engage you if they don't know you. No one is going to pick up a phone that has a magic button that says, 'Call CISO.'"

The good news is that in your role as CISO, part of your job has been done for you—by the bad guys hacking into your corporate peers' systems. Most executives now understand that information security, at some level at least, is needed, Rushing states. That makes this "a golden age of security," he says. "We have now acknowledged the problems and everybody is trying to fix them."

It will never be easy, but at least the path to progress is open, Rushing says. "You can do things that make impacts to the business," Rushing notes. "And you can see those impacts easily."

FORGE RELATIONSHIPS, FOCUS ON PRIORITIES, AND ESTABLISH CREDIBILITY

SAM MASIELLO

CISO
TeleTech

Sam Masiello has been working with email and messaging and fighting Internet pollution for more than 25 years. As the CISO at TeleTech, Masiello is responsible for PCI, SOX, and SSAE compliance initiatives. He also oversees the protection of employee, consumer, and customer data for all clients, including many Fortune 500 companies. Before TeleTech, he led the international application security team at Groupon where he was responsible for the security of web and mobile e-commerce applications and PCI compliance initiatives.

Twitter

Sam Masiello says things have changed for CISOs over the past few years. "There's been a pretty significant, fundamental paradigm shift as it comes to the requirements of CISOs over even the past five or six years. I would say the CISO role is fairly new overall because companies are really starting to take security seriously," he says, "and the requirement of CISOs is to be not just the technical backroom guy who knows how to protect the network but also the guy integrated with the business."

Masiello, CISO at TeleTech, says it's not necessary for CISOs to have a master of business administration, but they are required to have some business acumen. Three elements of business savvy are particularly important: forge relationships, focus on priority issues, and establish credibility.

"One of the first things you need to make sure you're doing is forging relationships with all your key stakeholders internally," he says, and that doesn't mean just the people on the security team. Masiello suggests forging relationships with the leaders of other departments outside of IT and even with vendors. "You want to make sure that they realize you are there to partner with them."

KEY LESSONS

1 A CISO needs to have a level of business acumen, which includes the ability to forge relationships across the C-suite.

2 Establish a level of credibility that points not only to technological expertise but also to a desire to see the whole business improve and succeed.

> *"The requirement of CISOs is to be not just the technical backroom guy who knows how to protect the network but also the guy integrated with the business."*

In addition to getting feedback from those stakeholders, he adds, “Make sure that you’re communicating a compelling future vision of where security needs to go. That means establishing that baseline, understanding where the company is at today, and creating a compelling vision of where you need to go. You’re not just maintaining status quo but showing the business that you have a strategy of where you need to be going from a security perspective.”

The next step, according to Masiello, is to focus on a subset of priority issues. For the CISO who is just entering the organization, focus on the first 100 days. “Establish a baseline. Identify areas where you need to establish long-term plans, but also identify things in the organization that could potentially get you some quick wins—easy things to fix because those are the things that you want to report up to management and the board. Even though those may be small wins, they’re wins nonetheless and they show that you are serious about advancing the program forward and not just spinning in that same hamster wheel.”

These efforts all lead to establishing credibility with the board, Masiello says. “One of the things that you absolutely need to do, not only within management, but within the organizational structure, is establish the credibility that you are not only the subject matter expert but also someone that comes in that wants to make a difference in the company. Someone who really wants to confirm to the company that you are doing everything you can to ensure all the company’s assets are protected, your clients’ assets are protected, and your partners’ assets are protected. Being able to establish those quick wins, that baseline, and that vision all go into establishing that credibility. For a new CISO, those are things that are fairly crucial to make sure that you get right.”

> “One of the first things you need to make sure you're doing is forging relationships with all your key stakeholders internally.”

BRANDON DUNLAP

Global CISO
Black & Veatch

With more than 20 years' information security experience, Brandon Dunlap has managed risk in many organizations and industries. As the global CISO for Black & Veatch, he is developing a program to support operations and clients in more than 100 countries to deliver critical human infrastructure projects. Previously, he has run information security operations for a Fortune 200 utility, been a security product entrepreneur, and served as director of product management at a large security software company.

Twitter | Website

If a CISO from a technology background wants to build business acumen, he or she should begin by learning about the business: how it makes money, how it operates, and its strategic direction for the future. "In my own organization," says Brandon Dunlap, "we actually have internal training programs, taught by finance and accounting staff, where anyone from any function or component of the business can take business literacy classes." Another option is to develop those business skills by taking a more formal education path in business accounting and finance, such as pursuing an MBA or other such program. Advises Dunlap, "That would pay huge dividends down the road in being able to speak more clearly the language of your business, which will help you break that technologist mold."

A CISO can also adopt a hands-on approach to developing business expertise. By taking the initiative and speaking with colleagues across the enterprise to understand what they are trying to achieve in their work, the impact that the security program has on that work, and any pain points they may have, you can build the knowledge as well as the personal relationships necessary to remove obstacles and bring value to the business.

KEY LESSONS

1 **A CISO can build business expertise by pursuing formal training opportunities as well as building strong partnerships within the organization.**

2 **To develop business leadership, it is important to align your work with the strategic direction of the business and support the goals of the company.**

> *"That would pay huge dividends down the road in being able to speak more clearly the language of your business, which will help you break that technologist mold."*

"That helps build trust with your user community. I've found successfully doing that will cause you to be drawn into the conversations as opposed to trying to inject yourself into them later," says Dunlap.

It's occasionally said that CISOs don't have a seat at the table, but Dunlap believes there is more than one way to become a part of important conversations happening at the company. CISOs might have the boardroom table in mind, but there are multiple tables available. "If you take the time to cultivate relationships outside of IT," he recommends, "you'll get invited to the dinner party, shall we say, at those other tables. I've been invited to different business units just to give a 30-minute presentation on how they can protect the intellectual property of our customers. And it's because I had those relationships that I got invited there."

If you've been with an organization for some time and have just been promoted into the CISO role, you likely already know who's who and should focus on introducing yourself to them in your new role. Dunlap advises, "Get out there and explain your new role to some of the folks, and ask, 'How can I help your business unit?'" By framing the conversation in terms of specific business outcomes you can deliver, you can create strong working partnerships that will help you succeed as a CISO.

> "Get out there and explain your new role to some of the folks, and ask, 'How can I help your business unit?'"

If you're new to the organization, Dunlap advises considering a different strategy that, he notes, some people may consider a bit risky. He says, "Send an email to the administrator who works for a business unit's leadership, and ask them, 'How did the previous CISO do? How can I do better? Where can I help you?'" If you take a customer-centric approach, chances are good that the vice president will point you to specific people in the division you can talk with, creating opportunities to forge the essential relationships you need to get started. "They can open doors for you," Dunlap explains, "and in that regard, allow you to build your professional network inside the organization."

CISO LEADERSHIP REQUIRES A CLEAR FOCUS ON BUSINESS OUTCOMES

As a CISO, aligning your work with the strategic direction of the business will make you a more effective risk manager. Dunlap's organization, which expects to experience rapid growth in the coming years, is placing a priority on talent management. He says, "There are ways that we can start to enable that and to create a workplace where security is transparent and easy for the users. By enabling Bring Your Own Device (BYOD) policies as well as some other low-friction technologies, we now become an enviable place to work." Those initiatives deliver a clear business benefit to the human resources function while underpinning the company's strategic plan going forward, offering security benefits as well.

A CISO who wants to develop business expertise can do so in several ways: by pursuing formal training opportunities within and outside the organization, by proactively seeking opportunities to deliver value for business units within the company, and by strengthening relationships that will lead to a better partnership on security initiatives. By taking special care to frame conversations using a customer-centric approach that focuses on business outcomes, a CISO can develop from a technology professional into a business leader.

MATTHEW ARCHIBALD

Vice President, CISO
Silver Spring Networks

At Silver Spring Networks, Matthew Archibald is responsible for enterprise information security and risk management across a network of corporate programs, including customer engagement and trust relationships, corporate culture of information safety, privacy and data protection, information asset management, regulatory compliance, IT continuity and recovery, operations standards, and awareness. In addition, Archibald acts in collaboration with the product manager for security technologies to drive new capabilities to market.

Website

Matthew Archibald remembers when he began thinking like a business leader. At the time he was asking his employer to consider a $15 million data-security deployment involving extensive global employee training and some new technology investment. During an executive meeting to discuss that project, a litigation attorney spoke up. "'I am only going to spend on average half a million dollars a year in litigation—so why would I spend $15 million on security?'" Archibald heard the attorney ask. "'The risk is not necessarily high enough.'"

Archibald's reaction: "That's a good argument." He realized it also is the way that businesses think. Painful though it was for the veteran technologist, Archibald admitted that CISOs must think that way, as well. "It is important at least to be knowledgeable about the implications of what you are doing," he says. "You have to take into account, what is the chief executive officer thinking about? What is the chief technology officer thinking about?"

CISOs tend to concentrate on IT investments that help identify and defeat system breaches and data exfiltration, Archibald notes.

KEY LESSONS

1 You must become knowledgeable about the business implications of what you are doing as a CISO. You have to take into account what the chief executive officer and chief technology officer are thinking about.

2 If you take the extra step of aiding in product development, you might be rewarded with less pushback when it comes time to make your budget requests.

> *"I am only going to spend on average half a million dollars a year in litigation—so why would I spend $15 million on security?"*

"Then they collect evidence for months to try and go prosecute somebody—in China," he states wryly. "You are rarely going to be successful at that." Thinking that way, Archibald contends, you might miss simpler opportunities to help the business, for example, by offering new, security-minded workflows that protect high-value information. In cybersecurity, he contends that technology is a secondary mechanism. "Everything else is driving people to change habits," he says.

One manifestation of a chronically tech-centric attitude, he warns, is wastefulness. "In this kind of odd world that CISOs live in, there is a notion that best practices call for two of each kind of technology," he observes. "So if one has a potential blind spot, it gets offset by another that likely won't have the same blind spot." He sees that as a foolhardy way to invest in IT.

Archibald eliminated about 40 percent of redundant cybersecurity technologies when he took his present job, saving roughly $500,000 a year. The move could marginally increase risk, but from a business perspective, it makes sense, he contends. "The number of times you might miss something is so small compared with the billions of packets that go across the network," he notes.

By now, Archibald is so locked into business thinking that he has become involved in product development at Silver Spring Networks. He says more CISOs around Silicon Valley are doing likewise, though it remains generally atypical. For Archibald, the payoff has been big. "If I can find a way to help the business tackle a problem related to external-facing needs," he states, "then when I want to make a change internally that might add a little bit of overhead, the pushback is much lower."

> "The biggest gap relative to the position of a CISO has everything to do with people and little to do with technology."

Archibald's advice? "Forget about technology," he urges. All technology does is help you make sure people are doing what they are supposed to do. "The biggest gap relative to the position of a CISO has everything to do with people and little to do with technology," he insists.

If, as a CISO, you still see yourself primarily as a technology player, it is time to do an about-face, Archibald argues. Become a business enabler first, a cybersecurity architect second. "As a CISO," he says, "you are actually much more valuable in terms of what you deliver back."

RICHARD TIMBOL

Information Systems Security Manager and CISO
Top 10 Global Law Firm

Richard Timbol is a cybersecurity and compliance professional with more than 25 years of experience. His early career was as an enterprise network engineer in the pharma, financial, health care, and retail industries. He has led teams and departments in information security, network engineering, messaging, and end point support. He has also served on the New York State eHealth Information Privacy and Security Collaborative and on several security advisory boards, including the Threat Intelligence Committee for the LS-ISAO.

Twitter

Richard Timbol often encounters CISO colleagues who rose to senior management with minimal information security knowledge. "That's dangerous because they don't understand the strategies they're crafting," Timbol says. "They're very ivory tower."

At conferences, he says, CISOs who were talented technologists early in their careers often approach him, feeling a bit lost. "Their questions are always, 'How do I convince my board to fund this project?'" he says. "Or, 'Why am I not getting the empowerment I need?'"

Both types of CISOs have the same problem: They fail to merge field knowledge with business savvy to develop and communicate a sound security strategy. They often end up marginalized. "Your empowerment is only as good as what you can convey," Timbol states.

Many CISOs compensate either by causing panic or becoming passive, Timbol observes. Here is what he recommends they should do:

- **Understand the business.** Lack of deep business awareness minimizes many CISOs, according to Timbol. "They try to talk the same language across the board and regardless of what vertical they are in, instead of learning the business," he says. Knowing how your business makes money will help you understand what you are protecting, he says. "If you don't do that," he remarks, "your security program is going to be more ivory tower than reality. You will not be able to relate your strategy."

KEY LESSONS

1 **Many CISOs are disempowered by an inability to combine security awareness with deep understanding of the business.**

2 **It can be advantageous to move slowly and develop liaison relationships throughout the business before introducing any new security initiatives.**

> *"Your empowerment is only as good as what you can convey."*

- **Develop a strategy.** Formulate a one- to two-year roadmap to security maturity, Timbol recommends. "Be able to convey that in a clear and concise way," he adds. "Include specific milestones and items you can measure success against." When your plan includes the deployment of any new information security technologies, state succinctly to leadership why that investment is needed. "Always tie it into the business," Timbol remarks.
- **Sell the vision.** With a strategy in place, selling the vision becomes easier, but it requires taking proactive steps. "Publicize successes," Timbol suggests. "When it is all quiet, that is a success—it means your strategy is working correctly." Ideally, every conversation with leadership should describe some new successful step toward security maturity. Timbol fosters that conversation with a monthly security report card. "We look at all of the attacks that we stopped from different vectors," Timbol states. "I put that out. Why not publicize that and say, 'This is the value we are getting'?"

Timbol learned these lessons early. He remembers how a CISO predecessor at a previous job worked hard to establish a raft of cybersecurity policies, but still failed in the job. That CISO was not good at explaining his policy rationale, according to Timbol. Some of his mandates—requiring color-coded badges to access various areas of the building, for example—rankled employees accustomed to a casual environment. Some policies were clearly canned ideas culled from texts and not tailored to the business. That CISO disempowered himself, Timbol contends. "There were things he wanted to do that made a lot of sense," he remarks. "But leadership didn't fund them. They already were tuned out."

> "Publicize successes. When it is all quiet, that is a success—it means your strategy is working correctly."

Timbol then took over, but he didn't rush into anything. "I realized that to become a security liaison to the business, I had to show that I understood the business," Timbol recounts. He spent several months building relationships throughout the business and studying his company and its vertical. Initially, he offered no security reforms. That approach, he thinks, won the day. "I think that was a pivotal moment for me," he recalls.

For Timbol, the twin morals of his story are: Understand the organization and make a concerted effort to know your peers. "Don't be afraid to be gregarious," he says. "Talk things out with the business. Understand and listen to what people have to say about what they are trying to achieve. Don't try to force a square peg into a round hole, but work in conjunction. It's all about teamwork."

CISOS MUST MIND-MELD WITH THE BUSINESS

LORNA KOPPEL

Director of Information Security, CISO
Tufts University

As CISO for Tufts University, Lorna Koppel's key responsibilities include assessing and managing the security risks to the university and the overall operating security for their diverse environment, including development and implementation of security policies, data stewardship and compliance activities, technology and architecture standards, and operational detection and response activities. Previously, Koppel held various security and leadership positions at Iron Mountain, Kohler, BT Infonet Services Corporation, CSC, MESO, Inc., and the USAF.

Website

There are many things a business needs to do to be successful—and only one of those is to contain information security risk. Lorna Koppel, CISO for Tufts University, advises CISOs to understand that and piggyback on those business priorities in their efforts to prevent security risks from derailing the business.

CISOs need to sync their goals with those of the business. Koppel's insight underscores her recommendations to new CISOs trying to become more effective, business-focused leaders:

- **Undergo a mind shift.** The CISO needs to enable the business, not simply protect it, Koppel states. "I have seen a lot of security programs where people try to fix all these security holes," she adds. "They see them as a horrible risk—meanwhile the business is focused on a completely different area." The CISO is almost forced to adopt what she calls a "quasi-split personality." Even as you work out and respond to business objectives, you must also run a cybersecurity program. "You are still going to do most of what you would have done, if you were running a straight technology program," Koppel remarks. "But your first focus is on enabling the business. So rethink it from that perspective."

KEY LESSONS

1 **The CISO's focus must be on enabling the business, not simply protecting it.**

2 **IT-centric CISOs must adapt to the needs of business—not vice versa.**

> *"You are still going to do most of what you would have done, if you were running a straight technology program, but your first focus is on enabling the business."*

- **Be prepared to let go.** CISOs promoted from IT positions often think their job is to prevent all risks and close all security gaps. Koppel was once among them. "Even today," she admits, "it is hard for me to not want to do that. But that is not my priority, and it can't be the priority." The business can't afford to maintain a hypervigilant security posture, she adds. The good news is that when you are seen sacrificing your own security preferences in favor of key business priorities, you will begin to earn the respect of the C-suite.
- **Open your ears and hear.** CISOs must actively seek out the resources and intelligence needed to protect the business. "Pay attention to the discussions that are going on around you." Koppel says, "What are the strategic plans for the company? What are its highest priority projects?" Those answers will not be offered to you, she warns. "Other business leaders don't seek out the IT security leader and hand them information. There is an assumption that you already know this stuff. So you have to realize that and speak up."

In Koppel's observation, technologists can be slightly introverted. What they love to talk about is technology. Business leaders typically do not. So younger CISOs sometimes get frustrated when dealing with executives and managers who lack their own level of technical knowledge and interest, she notes. That lack of tech-engagement can easily be misinterpreted, she cautions. "I have even seen people get hostile," Koppel says. "They think the other person is trying to derail them or undermine their success. In reality, it is often just communication style and different approach."

A change the CISO can easily make, she suggests, is attending and more fully participating in business meetings. That will help you key in on the various C-suite communication styles, she says. But the benefit will extend well beyond that. "You can build an unofficial understanding of the organization's level of risk tolerance," she states. "You need this to better prioritize what risks you should fix or work on, and what issues you can decide not to address."

> "You can build an unofficial understanding of the organization's level of risk tolerance. You need this to better prioritize what risks you should fix or work on."

The bottom line is this: IT-centric CISOs must adapt to the needs of business—not vice versa. When you fail to adjust, you make an already difficult job harder, she adds. "If you can't communicate on their terms, leadership will see you just as an IT security leader," she contends. "They will think you don't get it. Nor do you get that seat at the table."

GENADY VISHNEVETSKY

CISO
Stewart Information Services Corporation

Genady Vishnevetsky, CISO for Stewart Information Services Corporation, is an established leader with experience building successful security programs to protect the enterprise against emerging threats. Vishnevetsky leads the security, governance, and compliance programs for a major real estate financial services company. In his past role as the vice president of security and information security officer at Paymetric, Vishnevetsky built the cybersecurity, governance, and compliance programs for the fifth-largest payment processor of card-not-present electronic payments systems in the United States.

Website

Genady Vishnevetsky, CISO for Stewart Information Services Corporation, says his most important piece of advice for new CISOs is to not be a traffic cop. "It is not uncommon, especially for a technologist from the business security field, to come into this position as a traffic cop," he says. "Security has traditionally been perceived as a defensive mechanism. You really have to learn to be a business enabler. There are many ways that security can allow businesses to function and can work with the business and contribute to the bottom line. That's what a technologist needs to learn."

The switch from traffic cop to business enabler isn't an easy one to make. Vishnevetsky suggests that it begins with making allies by meeting with the leaders within the organization to establish an understanding of how the new CISO can help them be more successful. "Understand how to be an enabler. Security can be perceived as hard, but it has to support the business and it has to support the profit and loss statement. It has to help the business to grow because if you're an obstacle—if you're the traffic cop and you're saying no all the time—you won't be there for a long time because the business won't tolerate it," he says.

KEY LESSONS

1 **The most important thing for a new CISO to remember is that their job is to enable the business, not to always be the person saying no in the name of security.**

2 **Education is a role the CISO is also tasked with. It's important that the CISO spend time educating both the board and employees on how to be more secure.**

> *"Security has traditionally been perceived as a defensive mechanism. You really have to learn to be a business enabler."*

"What I normally tell my peers," Vishnevetsky says, "is it's not my job to tell the business to do or not to do certain things. It's my job to identify the risk and present to my executive team or to a board the risk to a business from a certain initiative and help them to make a decision. I'm not the one who's making decisions. My role is to be an educator."

Vishnevetsky says that part of educating the board is to make recommendations on helping them expand their knowledge of security requirements within their industry. For example, the National Association of Corporate Directors produces publications about cybersecurity and cyber risk. He recommends those to the members of the C-suite. "The board is held responsible at many levels from the Securities and Exchange Commission and the government," he says. "When I talk to the board, I recommend them to get familiar with those security principles. Because ultimately, they are held liable for accepting risk they shouldn't accept or not being aware of a certain risk to the business. That's on the board."

In addition to educating the board, Vishnevetsky recommends a change in tactics from defending or preventing to detecting. "You can't address everything. The bad guys will always be ahead of the curve. We're always playing a game of cat and mouse and unfortunately, the security professionals are the mice," he explains. "By focusing on enabling the capabilities to detect the adversary as quickly as possible, it can and will reduce risk significantly. It takes time for an adversary to penetrate your defenses and move laterally to find and then steal the golden jewels. The sooner you find the adversary and contain them, the greater your chances that you will not be breached. You will find the adversary. You will be compromised but you will not lose valuable data. In short, my advice is to switch from defense to detect. Defense and prevention mechanisms are still good; you still need to catch the low-hanging fruit. But don't spend a lot of effort there and don't focus on defending your environment using standard detection and intruder response."

> "It's my job to identify the risk and present to my executive team or to a board the risk to a business from a certain initiative and help them to make a decision."

JONATHAN CHOW

Senior Vice President, CISO
Live Nation Entertainment

Jonathan Chow is senior vice president and CISO for Live Nation Entertainment, where he is responsible for the implementation and monitoring of the enterprise-wide information security program. He is a popular speaker and has received several awards, including the Premier 100 IT Leaders by *Computerworld*, the Information Security Executive of the Year People's Choice Award from the T.E.N. Executive Leadership Program, and Global CISO Top 10 Breakaway Leaders by Evanta.

Twitter

Early in his cybersecurity career, Jonathan Chow worked for the NBC television network. One evening, just as the *Nightly News* was about to air, a serious IT network intrusion was detected. "We were trying to approach the problem in a cautious, conservative manner so that we could do the right forensics, gather information, and study the problem," Chow recalls. He approached his boss to discuss his plan. "My chief information officer (CIO) really took that opportunity to remind me that this is a time-sensitive business," Chow recalls. "I'll never forget what he said: 'We can't show the 5 o'clock news at 6 o'clock.'"

Doing his job and getting to the root of the problem were important considerations, but not the only ones, Chow now understands. Redundancies were built into the system—the intrusion did not really threaten to scrub the broadcast. But tackling the problem the wrong way might. The lesson? "Don't forget that you are practicing your security craft within the business context."

KEY LESSONS

1 **A mismatch still exists between what many businesses expect from CISOs, and what CISOs who have come up from the IT department have experience with.**

2 **Building up executive presence is much more important for new CISOs than many in the field recognize.**

Chow is now senior vice president and CISO for Live Nation Entertainment, so he still lives by the same dictum—the show must go on. Still, he empathizes with young CISOs who have not had the benefit of his experience. "CISO" is a relatively new title, Chow notes. So a mismatch exists between what many businesses expect and what new CISOs come prepared to accomplish. Most come from the IT department and bring a lot of tech-centric assumptions into the new role, he observes.

> *"Don't forget that you are practicing your security craft within the business context."*

"Honestly, coming up through IT doesn't prepare you for being in the C-suite," Chow says. "There is a real disconnect."

We have actually seen this all before, Chow states. When the CIO title came into vogue years ago, people also were often recruited from IT. Many understood technology but not how businesses operate. The good news, Chow says, is that they muddled through. "As the CIO has gone through iterations of the job or gained years of experience, they learned how to become that business leader."

For Chow, the CISO's present situation brings to mind a big Thanksgiving gathering. "There is no kids table in the C-suite," he contends. Just like those kids, CISOs dealing with executives for the first time often don't know how to act, what to say, or whether they belong, Chow says. "If you don't," he adds, "then you won't." So how can you demonstrate maturity enough to earn your seat at the big table? Here are Chow's tips:

- **Learn your business.** To become successful, Chow urges young CISOs to master business context. "Otherwise, it is just a science experiment," he states. The technological tenets of security—antivirus, firewalls, penetration testing—probably won't change much over time. "What changes is how you apply the technology, and what you do with the results of what you find," he says. "That is business-context sensitive."
- **Communicate in business terms.** The C-suite speaks of risks, not vulnerabilities. Adapt to that, Chow advises. "Many CISOs will kind of dive into code and run through specific exploits and vulnerabilities," he observes. "That's not that useful when you are talking to your fellow members of the C-suite or to the board of directors. They want to know the business impact."
- **Leave Henny Penny in the barn.** The CISO must become adept at delivering bad news, Chow states. "Rarely are you going to have tons of good news to share," says Chow. Do not be an alarmist; instead, learn to address crises calmly and confidently. "You can't be that fire-and-brimstone preacher saying we're all going to hell," Chow asserts. "Become judicious about what and how you communicate."

> "Acting like you belong, standing like you belong, and talking like you belong will help you belong."

For Chow, the moral of the story is that building up executive presence is much more important for young CISOs than many in the field recognize. "Acting like you belong, standing like you belong, and talking like you belong will help you belong," he insists. "That will help you gain acceptance."

PRASANNA RAMAKRISHNAN

Vice President, Information Risk Management
Career Education Corporation

Prasanna Ramakrishnan is vice president of IT risk management at Career Education Corporation, where he is responsible for managing the strategy and operations for IT security policy, risk management, logical access, security operations and engineering, compliance and change control, and business continuity. Previously, Ramakrishnan was the director of IT risk management at ULTA Salon, Cosmetics & Fragrance, leading all IT security and risk management activities while guiding the retail organization through all compliance challenges.

When a CISO makes the transition to a business leadership role, Prasanna Ramakrishnan advises, it might be a good idea to consider changing the reporting structure within the organization. The CISO has traditionally reported to a chief information officer (CIO) or chief technology officer, and as a result is often viewed as a technology-focused security function. Mature companies, however, are moving toward making this role report to a chief executive officer or chief risk officer. "This reporting change not only creates the perception that the CISO is an enterprise-level function but also provides the strategic direction this role requires. This will help in the transition to an enterprise-level focus," Ramakrishnan notes.

CISOs are knowledgeable about controlling weaknesses and the risks and threats they bring to the environment. "When we talk from the control perspective," he says, "it always comes across as a finger-pointing exercise. That does not help resolve the problem." Rather, when mistakes are identified, it's a great opportunity to not only teach the person the right way to avoid making those mistakes in the future but also help them understand the risks that exist in the organization.

KEY LESSONS

1 **When security-related mistakes are identified, CISOs should use that opportunity to help staff understand the risks.**

2 **Although some technology questions can have a yes or no answer, security questions are frequently more complex and require meaningful discussion.**

> *"You are successful in a security role when people come to you and tell you their problem hoping that you will resolve the problem, not fearing that you will victimize them."*

"My boss once told me that you will know you are successful in a security role when people come to you and tell you their problem hoping that you will resolve the problem, not fearing that you will victimize them," says Ramakrishnan.

It is critical for a CISO to build positive, open relationships with the staff to successfully transition into a business or enterprise-level leadership role, because that's how most enterprise-level risk management decisions are made. "Technology risk management decisions appear to be black and white," explains Ramakrishnan, "whereas the truth is that all risk management decisions are in a grey area where dialogs and conversations about what is right and what is wrong lead to a decision."

He once reported to an operationally oriented CIO who would sometimes ask him yes or no questions that appeared to be framed from a black-and-white perspective—for example, "Can we enable this feature?" At that earlier stage in his career, Ramakrishnan would say yes or no right away to please his boss, only to realize later on that he didn't fully understand the question.

With the benefit of experience, he now feels that risk management decisions cannot be made in a vacuum. "Most of the time security questions cannot be meaningfully answered with a single word," Ramakrishnan says. Proper risk management requires considering a lot of information, ideally high-quality information if it is available, to make the best recommendation.

> "I try to come across as somebody who is willing to serve in a consultative role."

Now, when asked such types of questions, he does not immediately say yes or no. "My answer is to ask, 'What is the background? Why are we doing this? Can you give me some history?' I try to come across as somebody who is willing to serve in a consultative role." By using this approach, he and his colleagues can surface the information needed to fully answer the question and arrive at the best decision.

By taking a service-oriented approach and considering a reporting relationship change so that it is better aligned with the business, according to Ramakrishnan, the CISO will be able to access quality information to make a better risk management decision. As a result, that person will be able to substantially improve his or her risk management skills and truly become a leader within the organization.

DAVID MACLEOD

VP of Corporate Information Technology & CISO
Welltok

David MacLeod, Ph.D., FHIMSS, CISSP, CHS-III, and CISM, has been CISO for a large, multistate Blue Cross and Blue Shield organization; chaired the BCBCA Association Information Security Advisory Group; was CISO for a Medicare data center; and was appointed by Secretaries Thompson and Ridge to advise HHS and DHS on information protection and assurance in the health care and public health sectors as a part of the National Infrastructure Protection Plan and the federally sponsored Information Sharing and Analysis Centers.

Website

To develop the business leadership skills required of a CISO, says David MacLeod, it's important to become adept at explaining security issues in business terms so that the business case for your initiative can be clearly understood by decision-makers within the company. To that end, he adds, using analogies can be quite helpful in getting your point across.

One security analogy MacLeod likes to use is that of a bank vault. "Consider the risk of having a bank that has no vault to put its money in versus the risk of a bank that has a vault that is rated at 24 hours," he says. "Bank vaults are rated for how long they can sustain an attack by a skilled safecracker. By thinking about how long your bank vault might have to withstand an attack, you might be able to better decide what type of a vault you want to buy, right?"

If security teams are passing by to check on the vault every hour, a 24-hour vault is probably more than adequate. But if the bank plans to close on a Friday night and there will be nobody on the premises again until Tuesday morning because of a bank holiday, that constitutes the longest period of time during which the vault could be vulnerable to an attack.

KEY LESSONS

1 **A CISO must communicate security risks using easy-to-understand language. Analogies can be particularly effective for this purpose.**

2 **As business leaders, CISOs must effectively partner with the CEO and board. As security leaders, CISOs must provide clear technical direction to their team.**

> *"Every one of the other C-levels is expected to be a good businessperson first. Their expertise happens to be in a particular area, and the same is true of the CISO."*

In that case, a bank would want to purchase a vault that's rated at 96 hours or more, paying a significantly higher price for the added security safeguards that come with it.

Explaining security decisions in these terms is a terrific way to help business partners understand the risks around security and privacy, says MacLeod. Conversely, "The worst way to communicate security risks is to try and scare people. Saying that your company could be hacked, that it could be the next Home Depot or the next Anthem, for example, is not the way to go. The best way is to put it in terms they understand and explain it in good, sound business sense."

Other C-level executives have long been expected to demonstrate strong business acumen in addition to expertise in their field of specialty. "When the executive team gets together, you expect the chief financial officer to come to the table as a good business person but one who brings skills particular to finance," says MacLeod. "Every one of the other C-levels is expected to be a good businessperson first. Their expertise happens to be in a particular area, and the same is true of the CISO."

A CISO that does not understand the business and cannot think like a businessperson won't be able to grasp, much less articulate, the breadth of risk that the business faces. MacLeod, for example, has spent most of his career as a health care CISO. He says, "If I don't understand the business model and how health care works, I'm not going to have a clue about which threats might present themselves."

MacLeod feels that today's CISOs must acknowledge that they inhabit a dual role. "I use the mythological god Janus, the two-faced god looking both ways, as an analogy. As a CISO, you have to have one face that's looking out to the business, to the board, to your other C-level executives and explaining things in a manner that they understand, but at the same time, you have to have a face that is more inwardly focused toward security operations and the technical operations of the organization, and be able to articulate to them how to do the job that needs to be done," he explains.

> "If I don't understand the business model and how health care works, I'm not going to have a clue about which threats might present themselves."

THE DUAL ROLE OF THE CISO: BUSINESS LEADER, SECURITY LEADER

As much as a CISO must bring strong business skills to the table today to be effective in the position, it is still important to maintain strong technical knowledge as well. By being able to speak to the technical team in terms that they understand and give clear direction about the technology and the controls that are to be put in place, while being able to conduct thoughtful and deliberate risk management discussions with business partners and the board, a CISO can ensure future career and business success.

THE CISO NEEDS TO BE PART OF THE BUSINESS DISCUSSION

SCOTT SINGER

Chief Security & Information Officer and CISO
PaR Systems, Inc.

Scott Singer is the CISO for PaR Systems, Inc., an industrial automation company. Before PaR, Singer spent 16 years with Medtronic in various leadership positions, including European infrastructure manager and division CIO. In his last two years at Medtronic, Scott led the global security function. As a Navy Reservist, Captain Singer is the Navy Emergency Preparedness Liaison Officer (NEPLO) for the state of Minnesota. Before being promoted to NEPLO, he was executive officer of a Pacific Fleet cybersecurity unit.

Twitter I Website I Blog

As someone who wears both the chief information officer (CIO) and CISO hats at PaR Systems, a company that develops industrial automation systems, Scott Singer has an interesting perspective on the CISO role. “Being a CISO only, especially at a large enterprise with tens of thousands of employees, can be challenging,” says Singer. Part of it has to do with where the CISO actually fits in the organization. Not all companies view their CISOs as true players in the C-suite. Singer says, “I’m fortunate in that I have both CIO and CISO responsibilities, which makes it easier to bring CISO issues to the table.”

It’s important to recognize that at the end of the day, the CISO is a strategic business role, not a strictly technology role. “You must understand the business issues and be a part of the business discussions,” Singer says. This means understanding not only the technology but also the business implications of technical issues, and being able to explain those business implications in terms that are meaningful in the executive suite.

CISOs need to understand their role in helping the business meet its objectives. For example, businesses’ ability to win contracts is becoming increasingly dependent on successfully proving to customers that as a partner or service provider, they represent a low security risk. “Large aerospace companies will run a rigorous security audit before doing business with you,” Singer says. This approach is becoming increasingly common in any business relationship involving access to computer systems where a breach can cause serious, costly problems. “The CISO has a role to play in making business happen,” says Singer.

KEY LESSONS

1 **The CISO needs to understand and be able to navigate executive-suite politics.**

2 **It’s important to recognize that at the end of the day, the CISO is a strategic business role, not a strictly technical role.**

> *“You must understand the business issues and be a part of the business discussions.”*

He cites an example of understanding how to navigate complex international data security regulations so that it becomes possible to participate in a project. Singer's company has engineering facilities in both the United States and the United Kingdom. Ideally, these engineering teams want to share data on one system.

In the United States, there are certain categories of data that a U.K. person cannot view without a license. Likewise, there is restricted data in the United Kingdom that a U.S. person can't look at without a license. However, if you work with the Ministry of Defence in the United Kingdom, or you work with certain U.S. government agencies, and you can prove that you have strong controls within your organization, you can share that data between those organizations in certain situations. Singer says, "It comes back to the CISO understanding leverage points and competitive advantage points, and providing solutions so that the business can achieve its goals."

The CISO needs to understand and be able to navigate executive-suite politics. This ability is important because attacks and breaches happen. The CISO does not want to become a sacrificial lamb to an attitude that says, "Well, we fired the CISO—that takes care of that problem." Like any other executive-level player, it is useful to have allies in the boardroom. Ultimately, the CISO needs to be technically competent but also able to see and perform in a business context. "The CISO needs to be seen by other executives in the company as a business partner," says Singer.

> "It comes back to the CISO understanding leverage points and competitive advantage points, and providing solutions so that the business can achieve its goals."

NATHAN RAJEN

Public Information Officer and CISO
Key Safety Systems, Inc.

As PIO of Key Safety Systems (KSS), Nathan Rajen is implementing technology-driven transformation to help KSS innovate and deliver superior safety systems to automotive manufacturers. He also serves as the CISO, successfully navigating the company through VDA/ ISO 27001 global security audits. Before KSS, Rajen founded Abacusoft, LLC, a strategic advisory consulting firm focused on manufacturing and industry. As senior director with Siemens IT Solutions (later acquired by Atos), Rajen led the Americas Consulting Services for Manufacturing and PLM Industry Solutions.

Twitter | Website | Blog

Information security can add value only if the CISO understands business process context. That is the opinion of Nathan Rajen, CISO and process information officer for global automotive supplier Key Safety Systems. With that idea as backdrop, he offers two bits of advice to the CISO who hopes to become a more business-focused leader:

- **Assess your vertical.** Study and report back to leadership on the regulations and compliance standards that apply to your industry. What are competitors doing? What assets might be considered competitive advantages, if defended properly? What new security compliance standards might differentiate your company in the marketplace? Learn all you can about the expanded ecosystem of customers, partners, and suppliers, Rajen urges, "That is where most of the security regulations are put in place." The board will not object, he contends. "When presented in the right context, they will understand that this is their business."
- **Assess the company culture.** Rajen suggests assessing the company's cybersecurity stance and determining whether the culture is proactive or reactive. In proactive organizations, he observes, security leadership often has decision-making influence with senior management.

KEY LESSONS

1 **Information security can add business value only if the CISO understands the business process context.**

2 **To position security as a strategic advantage, learn your company's and vertical's regulatory, statutory, and operational challenges.**

> *"You are going after millions of dollars of business with this customer and something as simple as corporate security could jeopardize this opportunity."*

> "You can approach security through traditional consultative approaches," he states. Reactive organizations, however, tend to view IT as a cost center. They typically need a "trigger event" to jolt them into genuine security awareness. "If the organization is reactive—to put it bluntly—you need to put the fear of God into management for them to really take security seriously," he emphasizes.

Rajen was promoted to his current job after working with Key as a consultant. Before he took over, he says, the IT security posture was fairly reactive. "I needed to figure out how we raise awareness because the thought process around security was non-existent," he contends.

Around that time, Key applied for preferred status with a European original equipment manufacturer (OEM). The OEM requires suppliers to achieve Level 3 to Level 4 compliance with the ISO 27001 information security standard. However, Rajen's internal audit revealed that Key was somewhere between Level 1 and Level 2. He had his trigger. "You are going after millions of dollars of business with this customer and something as simple as corporate security could jeopardize this opportunity," Rajen recalls telling the board. "Let's make the right kinds of investments to close the loop and address this." Board members agreed. Key made the investments and its preferred-supplier status with the OEM was secured.

Rajen's takeaway message is that, to make a strategic difference, the CISO must offer more than a strong background in technology and security protocols. "You are expected to bring those to the table," he asserts. "The difference maker is how you go beyond those basics."

Comprehensively build relationships within the business, he urges. Educate yourself on your company's and vertical's regulatory, statutory, and operational challenges. "Position security and related initiatives as a strategic advantage," Rajen advises. "That is really how you can make a difference."

> "Position security and related initiatives as a strategic advantage. That is really how you can make a difference."

OMKHAR ARASARATNAM

Chief Technology Officer of CISO, and Global Head of Strategy, Architecture and Engineering
Deutsche Bank

With almost 20 years' IT experience and a long history of leading global, multibillion-dollar programs, Omkhar Arasaratnam is a cybersecurity and technical risk management executive who helps organizations realize business goals while effectively managing risk and compliance. At Deutsche Bank, Arasaratnam is the CTO of CISO, leading CISO strategy, architecture, and engineering. Arasaratnam is an "old geek" who has contributed to the Linux kernel, helped maintain Gentoo Linux, holds several patents, and has contributed to ISO/IEC 27001:2013.

Businesses are multifaceted, says Omkhar Arasaratnam. CISOs, he contends, tend to forget that. "We monolithically refer to everyone else outside of IT as 'the business,'" he states. "I think that is the first misstep that a lot of technologists make." The challenge—and the opportunity—is for the CISO to escape that us/them mindset and learn to communicate in ways that resonate across business constituencies, Arasaratnam says.

The operational risk officer, for instance, will understand a discussion about risk management much better than she might a presentation on technology management, Arasaratnam suggests. The chief financial officer (CFO), likewise, will better understand you if you speak in terms of balance sheets, income statements, and cash flow, rather than the number of indicators of compromise logged in a day.

What Arasaratnam and some like-minded peers have specifically advocated for several years, he says, is the framing of information security in business-risk terms. "That tends to marry quite well with most non-technology aspects of businesses," Arasaratnam indicates.

KEY LESSONS

1 **The CISO must escape the us/them mindset and learn to communicate in ways that resonate across constituencies.**

2 **Contextualizing information security so that non-tech-savvy leaders understand it is the best contribution a CISO can make.**

> *"We monolithically refer to everyone else outside of IT as 'the business.' I think that is the first misstep that a lot of technologists make."*

He explains. "If I go to our CFO and say, 'We have a potential issue that could result in a one-time loss of €1 billion, and therefore I want to put this €200,000 fix in place,' he will be much more amenable," Arasaratnam advises, "not only in terms of understanding but in terms of approving that particular solution."

Early on, Arasaratnam was himself purely a technologist. He contributed to the Linux open source operating system's kernel development and even worked for a time as an ethical hacker, intentionally cracking into systems under contract with IBM. He transitioned toward business-focused leadership after taking a job as chief security architect for TD Bank. The change was not entirely easy. "At IBM, I could always fall back on my technical laurels," Arasaratnam recalls. "Going into TD really forced me to think as a banker. That caused me to start morphing the manner in which I spoke about security."

Through trial and error, he discovered that framing presentations in risk-based terms was "extremely palatable" to his TD bosses. Banks make money off risk, after all, so they know it is not inherently bad. They correlate all the risks involved in a transaction and, based on their risk/reward analysis, decide whether to proceed, Arasaratnam notes. "Using a similar story line, but orienting it to security, has been successful for me," he states.

Of course, he adds, even formulating that analogy required him to educate himself thoroughly on how banking works and how various banking departments help to further that success. Every CISO needs to attain a similarly high degree of business acumen, he asserts.

With that understanding in place, the CISO can begin the transition to business orientation by learning to contextualize information security for non-technologists so that they can understand how cybersecurity affects them and the business. "That," Arasaratnam contends, "is the best thing that an up-and-coming leader can do."

> "Going into TD really forced me to think as a banker. That caused me to start morphing the manner in which I spoke about security."

GO GET THE PULSE OF THE BUSINESS

MARTIN MAZOR

Vice President, CISO
Meggitt PLC

Martin Mazor is a global leader in information security with more than 20 years of experience leading and developing successful information security programs. He is currently the vice president and CISO for Meggitt. Previously he was the global CISO for Ingram Micro where he led all aspects of information security including security operations, application and SAP security programs, architecture, administration, and IT compliance. Prior to Ingram Micro, Mazor was the global head of information security for the Fluor Corporation.

CISOs come in various types, according to Martin Mazor. Some are tech-centric, some gravitate toward frameworks and policies, while others—these tend to be younger—are geared toward integrating development and operations into their security processes. Mazor considers himself a hybrid. “You can be a little bit of everything, I think,” he says.

The commonality for them all, Mazor states, is a primary need to understand how the business works and how their CISO contributions can advance the overall business mission. With that in mind, Mazor offers two primary pieces of advice to the incoming CISO who is transitioning to a business-focused mindset:

- **Build relationships.** First, get to know your peers and their information security pain points, Mazor asserts. Build up relationships within your own department and with other members of the C-suite—preferably through face-to-face meetings. That is the quickest path toward understanding the business’ cyber-risk posture, Mazor says. Some CISOs will struggle here, he acknowledges, preferring penetration testing and intrusion detection reports to meet-and-greets. That must be overcome, he insists: “You’ve got to become an established partner of the business.”
- **Build a sensible risk model.** This task should be your next major focus, Mazor says. Your cyber-risk model must be attuned to your business’ particular drivers, and it must be reality-based. “It has to be a phased, graded approach with established baselines, risk models, risk postures, whatever works for the company,” he says.

KEY LESSONS

1 **Understand how the business works and how a CISO’s contributions can further the overall business mission.**

2 **The CISO’s duty is to move the organization beyond cookie-cutter approaches to cyber-risk management.**

> *“You've got to become an established partner of the business.”*

> Do not fall into the trap of trying to convince leadership that you can make their business 100 percent secure with just a few strategic investments. "No company can perform that," Mazor insists. "You cannot secure everything. Don't try."

Most companies have a low cybersecurity posture and many know it—which is why so many are hiring CISOs. They do not, however, necessarily understand how best to overcome it, Mazor says. "People start reading books and looking at all kinds of training," he notes. "Then they start cutting and pasting the different risk framework models." The CISO's duty is to move beyond the cookie cutter. That, Mazor adds, is why it is so imperative for young CISOs to develop meaningful relationships with the chief risk management officer, the chief information officer, the chief executive officer, and anyone else who might help generate "a security-thinking model" for cyber-risk management. "If CISOs are not doing that day one—or day two—they are not getting ahead," Mazor comments. "They are jumping in and looking at firewalls, and that is not where they need to be."

Communication skills, in short, are a core CISO skill, he says. Developing a knack for focused gregariousness might seem a tall order for some, he admits. Viewed another way, however, maybe not. "For a techie, it's like learning a new language—like Java coding," Mazor says. "It's the same kind of thing. Communications is a skill. If you don't have it, you can go learn it."

In the end, Mazor really is talking about the CISO taking to heart his or her role as a genuine business leader. Not just a glorified IT guy, he adds, but someone who belongs in the C-suite. "There is nothing unique about a CISO role," Mazor contends. "If you are going into leadership, the first thing you need to do is build the relationships, both internally and externally, with that shared-goals model. Go get the pulse of the business."

> "If you are going into leadership, the first thing you need to do is build the relationships, both internally and externally, with that shared-goals model."

A VETERAN CISO SURVIVES A HURRICANE

ROY MELLINGER

Vice President, IT Security, and CISO
Anthem, Inc.

Roy Mellinger is vice president of IT security and CISO at Anthem, overseeing a department of more than 300 information security and risk management professionals. Before joining Anthem, he served in executive security leadership positions for Sallie Mae, GE Capital, Heller Financial, Household International, Inc., and Spiegel. Mellinger is a CISSP, with advanced certifications in security architecture and information security management. He is on the board of directors for HITRUST, and the advisory board for the Lares Institute.

When companies endure major data breaches, someone generally gets fired. Often it is the CISO. For CISO Roy Mellinger, things did not play out like that. At Anthem, he endured one of the biggest breaches in history, yet kept his job. He thinks he knows why. "The reason why I still have my career and job," he states, "is because I did everything right." Perhaps more important, he adds, management knew he did everything right—because he kept them well informed all along the way. "All of the risks were laid out," Mellinger recounts. "When there were budget decisions, or projects, or implementation prioritizations, all of that was laid out. They had made informed decisions."

KEY LESSONS

1 **Being clear and transparent with leadership can help the CISO weather even the worst storms.**

2 **Security is not about technology; it is about people and process.**

As it happens, many of the security tools implemented post-breach were parts of projects and initiatives for which Mellinger had received prior approval. "Instead of a three-year timetable, we did them in nine months," he says, "because of the breach." Because he had always been transparent and realistic in his messaging to executives before the crisis, Mellinger contends, when it struck, they understood the reality of the situation. "I think that is a key takeaway for any new CISO," he says.

There is a catch. Although it is important to keep management informed, Mellinger suggests, you must inform them in the right way. Here are tips from Mellinger for doing so:

- **Nix the scare tactics.** Be viewed as a leader with a plan, not with a fire alarm. "You're the fixer," Mellinger remarks. "Communicate that we have some challenges, but the sky is not falling." You succeed at scaring executives only at the cost of credibility, he insists.

> *"You're the fixer. Communicate that we have some challenges, but the sky is not falling."*

After all, the CISO is not alone; every leader faces challenges. “As a CISO,” Mellinger declares, “you are an executive. You’re not a Big C, but you’re a C. So be prepared. That is what you’re getting paid for.”

- **Avoid geek speak.** Mellinger notes that every business function is represented in the C-suite. Yet when business presentations are made, everyone understands them because they get presented in common business terms. CISOs must follow that lead. Keep executive presentations rooted in language and experiences that they understand, he advises. Avoid tech jargon. “You have to really focus on business language to get your message across,” he cautions.
- **Picture = 1,000 words.** One of his mentors impressed Mellinger with a knack for boiling down complex presentations to a few PowerPoint slides, always including illustrations. Mellinger mimics that approach. Even his five-year security roadmap is represented in a few PowerPoint slides. “Every page has a framework—network security, data loss prevention, forensics, cybersecurity operations center operations, user administration,” he says. “And every one of those decks has pictures.” Mellinger’s advice: “Think high level and talk to the picture.”

Finally, he advises, remember that security is not a technology problem—it is a people and a process problem. “The tools help you achieve a degree of security, and project management helps you implement,” he says, “but it really comes down to governance.”

To get to the root of security, he offers, smart CISOs should ask and answer several key questions: What are the organization’s crown jewels? How difficult are they to protect? Why do they need to be protected? What and who do we need to protect them against? What are the risks? What is really important? Answer those, Mellinger maintains, and you will attain critical visibility into cyber risk. You will also stay more focused on what you were hired to do in the first place. “To me,” he contends, “it’s all really just a multidimensional risk management problem.”

> “As a CISO, you are an executive. You're not a Big C, but you're a C. So be prepared.”

IN RELATIONSHIP BUILDING, LOOK TO THE LEFT AND RIGHT

DARRELL KEELING

CISO
Lands' End

With more than 20 years' security experience across a range of disciplines and verticals, Darrell Keeling is the CISO at Lands' End. He is responsible for creating security strategic vision. His mission is to be viewed as a business enabler through strategic, innovative technologies and processes that protect what matters while providing an uninterrupted secure and quality user experience to users and customers. He is a results-driven, recognized executive who brings a unique combination of business acumen and security expertise.

Website

Darrell Keeling, CISO for Lands' End, has been the first CISO for several companies that he's worked with in the past. In these roles, Keeling had to help the companies integrate the role and responsibilities of the CISO. "My initial advice is relationship building is a key element of being a successful CISO," says Keeling. "You have to recognize you're the expert and you will have to educate others, and be patient in your efforts to drive sustaining change across your organization."

In part, Keeling says that driving this sustaining change requires that CISOs understand that nearly all businesses become great by taking risks, and that includes some security risks. "This will better equip you to understand the reasons behind your organization's business strategy. Understand and learn the risk appetite of your organization and its leaders."

That understanding can help CISOs change the security culture, says Keeling. "It isn't all about frameworks and IT controls. Yes, that is important but it's just as much about changing the culture of the organization from the top down and bottom up," he explains.

KEY LESSONS

1 **As CISO, part of your responsibility will be to use education and relationship-building skills to drive change across your organization.**

2 **Remember that your peers will be the people who help you drive the necessary change, so it's important to build relationships with these people.**

> *"You have to recognize you're the expert and you will have to educate others, and be patient in your efforts to drive sustaining change across your organization."*

IN RELATIONSHIP BUILDING, LOOK TO THE LEFT AND RIGHT

One step that he recommends to facilitate that change is to recognize that you need to have a relationship not only with the people above and below you but also with your peers. “Where a lot of CISOs fail is they look at the upper-level relationships above them but they don’t look at the relationships to the left and right. Their peers,” he says. “In many cases, CISOs are directors, so if you look to the left and right you have application directors and infrastructure directors and so on and so forth. But CISOs are taking for granted that those relationships are built just because they both report to the same people.”

However, more work needs to go into it than that. “I think that’s a breakdown,” Keeling explains. “Those relationships have to be built as much as the ones that you’re trying to build upwards, with the people that are making the decisions. There’s a gap there.”

Use the same skills to build peer relationships, Keeling says. “My thing is to get outside of my comfort zone and set up meetings with these leaders and have conversations. Learn about them. Learn about not only what they’re doing, what their mission is, and what they’re driving, but also learn about them as a person. And then it just kind of falls into a better business working relationship when you have tough challenges you have to work together to overcome.

“These relationships don’t come easy,” says Keeling. “Sometimes you’ll start out and get denied meetings. You just have to gradually keep working until you build the trust through other leaders until there’s some common conversation that happens across the board and then it kind of starts opening doors for you. My best advice is keep your integrity, keep building off your small wins, and be patient for change.”

> “My best advice is keep your integrity, keep building off your small wins, and be patient for change.”

DUAINE STYLES

Fortune 1000 Information Security Leader/CISO
Financial Services/Insurance

Duaine Styles is a strategic risk management professional with over a decade of experience leading information security programs. He collaborates with business executives and management peers to protect a company's valuable information assets. He holds a master's degree in Information Systems from the University of Texas at Arlington, is a licensed CPA in the state of Texas and holds certifications that include CISSP, C|CISO, CRISC, and CISA. Duaine also helped found the Cowtown ISSA chapter.

KEY LESSONS

1 **It is important to understand that the CISO's job is not to eliminate risk.**

2 **The CISO is an advisor with a specialized skill set and should report to one of the key decision-makers in the C-Suite, or another C-level advisor.**

The first step for someone considering a CISO position is to evaluate whether you possess the right skills for the job. You can be a security leader who, because of your strengths, demonstrates great competence in a security service delivery or IT capacity. That doesn't mean you will be successful in other security leadership positions.

"The first rule of leadership is to know thyself and to do that you must know your strengths," says Duaine Styles, whose background in accounting systems, IT auditing, and security engineering/operations became his path to strategic security leadership.

The CISO needs different skills and strengths than an operational-level security manager. An IT security manager delivering security services in an enterprise has an operational focus. In this role, you have probably done well because you have strengths that lean toward the operational-to-tactical side of the strengths spectrum. A CISO needs to have strengths that lean more toward the strategic-to-tactical side of the spectrum. It is an entirely different mindset.

It is also important to understand that the CISO's job is not to eliminate risk. From a security operations perspective, the goal is to reduce risk as much as possible through excellence in operations. The CISO's job is to manage risk across the enterprise by seeking to align security risk levels to the risk appetite of the board and executive leadership. "The CISO needs to understand that risk is opportunity, and opportunity is profit, and there is no profit without risk," explains Styles. "So if you eliminate all risk, you eliminate possible profit."

> *"The first rule of leadership is to know thyself and to do that you must know your strengths."*

The CISO's organization is focused on identifying risks and what capabilities the company needs to mitigate those risks to leadership's risk appetite. Security risk is a business problem, but not all organizations see it this way. More mature businesses from a security perspective, such as financial institutions, look at security risk more on the front end of strategic discussion, along with other business risks. As you move down the maturity curve, the attitude tends to be that security is just an IT problem. "The most mature approach to information security is to view it as part of the overall enterprise risk management discussion," says Styles.

It is also important to understand where the CISO sits in relation to other members of the C-suite. Styles says, "At this point in time, the CISO does not carry the same weight as most of the players in the C-suite due to the immaturity of information security's risk management capability." However, you also need to understand that not everyone in the C-suite is created equal. In most companies, there are three to five people who make most of the decisions because they own organizational risk. The CISO is an advisor with a specialized skill set and should report to one of these key decision-makers or another C-level advisor with broader responsibilities.

In a mature organization, the CISO would be considered an enterprise-wide risk manager and would be administratively reporting to a COO, a general counsel, or a chief risk officer. The CISO in this environment would not be considered a resource devoted to IT service delivery. Regardless, the reporting structure should always ensure that security decisions can be made that reflect the board's and executive management's risk appetite and that decisions are not excessively influenced by either operational ease or budgetary constraints.

> "The CISO needs to understand that risk is opportunity, and opportunity is profit, and there is no profit without risk."

DON'T KNOW YOUR BUSINESS? HAVE A WALKABOUT

GARY HAYSLIP

Deputy Director/CISO
City of San Diego, California

As CISO for the City of San Diego, California, Gary Hayslip advises the city's executive leadership, departments, and agencies on protecting city information and network resources. Hayslip oversees citywide cybersecurity strategy, the enterprise cybersecurity program, and compliance and risk assessment services. His mission includes creating a risk-aware culture that places high value on securing city information resources and protecting personal information entrusted to the City of San Diego.

Twitter | Website

It was a zero-day at the U.S. Navy command where Gary Hayslip worked. He discovered a previously unknown information security vulnerability for which there was no patch. "Hackers love zero-days," Hayslip observes. "It allows them to do bad stuff as long as possible with no one knowing about it." Hayslip tried desperately to convince senior leaders of the gravity of the crisis and the urgent need to end it. But they rebuffed him: "They are all looking at me like I am stone crazy," he recalls.

Later that day, Hayslip went home, had a few drinks, and thought things over. "It just kind of clicked—my priority and theirs are not the same," Hayslip recalls. "Then it dawned on me: Whose priorities matter? *Their* priorities matter."

Hayslip, now CISO for the City of San Diego, had that epiphany a decade ago. A second quickly followed. Hayslip realized he did not understand his own business. He was laser-focused on cybersecurity, but his command repaired warships. It had various departments housing machine shops, engineers, welders, and architects. Hayslip knew next to nothing about them. "I was just in my silo," he says.

If you hope to transform yourself into an effective business leader as a CISO, Hayslip suggests doing what he did. Go on an extended walkabout of your business. His lasted six months. "Get out and meet people," Hayslip advises. "Understand what is important to them. What applications are critical for their department? Are they using sensitive data that has a compliance component to it?

KEY LESSONS

1 **Do a walkabout—get out and familiarize yourself with people in your business so that you can understand their needs, vulnerabilities, and pain points.**

2 **An MBA is strongly recommended to gain understanding into the needs and the risk tolerances of the business team.**

> *"It dawned on me: Whose priorities matter? Their priorities matter."*

You are going to need to know that. You need to find out their pain points."

While making his rounds, Hayslip learned that his zero-day event, although certainly a big deal, was not big enough to shut down the whole operation. Hackers were not yet exploiting the vulnerability, so a business decision was made to develop a patch as part of the regular schedule. That involved risk, he acknowledges. But in reality, it was minimal.

Another lesson learned was that Hayslip had much to learn. During executive meetings, for instance, he often felt overwhelmed by unfamiliar business jargon. So he enrolled in a master of business administration (MBA) program. "I really needed to add that to my skill set," Hayslip notes. "I honestly recommend it."

It might be tempting for a young corporate CISO to consider Hayslip's Naval experience irrelevant. That would be wrong, he cautions. Today, as San Diego's CISO, Hayslip implements information security strategies and enforces all cyber policies and controls. He reaches back to those old Navy lessons every day. "The approach to business and services, dealing with budgets, funding, projects—it's still the same," he notes. "What I learned in the Navy, I honestly think, I would have learned anywhere."

A core task for Hayslip today is to effectively communicate his security needs and vision to his bosses. He offers a simple framework for making presentations ring the way his do. Structure talks like this: First, identify the specific issues you face. Next, describe the overall current security state. Finally, offer leaders your envisioned future state.

That last point, Hayslip warns, will be met with predictable questions—how do we get there and what do you need from us? Do not be caught flat-footed. "You'd better be able to answer," Hayslip warns. "You'd better have your numbers and you'd better have a plan. This is where I think that MBA pays off for me in spades—because those questions are all about business."

> "This is where I think that MBA pays off for me in spades—because those questions are all about business."

BUILD STRONG RELATIONSHIPS WITH OTHER BUSINESS LEADERS

DANE SANDERSEN

Global Security Director
Trek Bicycle Corporation

Dane Sandersen is the Global Security Director (CSO) at Trek Bicycle Corporation, a billion-dollar, family-owned company. Sandersen is responsible for global information and physical security strategy, policy, and programs. He enjoys a collaborative approach, and works closely with senior leaders to balance security controls with costs and burdens to business units. Sandersen is also a Lieutenant Colonel in the Army Reserve and acts as G6 (CIO) of the Great Lakes Training Division.

Twitter I Website

The challenge for any new CISO coming from a technology background is focusing on what is best for the business as a whole and not just on the best technology solution. “New information security people often lean on that technology crutch, the hard controls of a security platform that perform some function,” says Dane Sandersen, whose security role is unusual in that he oversees both cybersecurity and physical security of corporate facilities. CISOs need to adopt a broader business focus and recognize they will have to compromise between optimum system security and what is acceptable to the business. Sandersen says, “As a security person, you can’t draw a hard line in the sand, because if you do, over the long run, you will lose your influence. Don’t say ‘no.’ Say, ‘here’s the risk.”

The long game for a CISO is to be part of the business discussion, to do the analysis, point out the risks, compromise when necessary, and to work as a business partner doing what’s best for the whole business. “You want them to come to you first,” says Sandersen. “It’s never a good idea for security to be an afterthought.” To accomplish that goal, the CISO needs to gain credibility among other business leaders in the organization.

KEY LESSONS

1 **By informing business leaders of risks, and making it their decision to accept or mitigate those risks, the CISO is also putting them on the hook for accepting the risks.**

2 **It is essential for the CISO to build strong relationships with business leaders in the organization because there will be times when their backing is needed to enforce a policy.**

> *“You want them to come to you first. It's never a good idea for security to be an afterthought.”*

BUILD STRONG RELATIONSHIPS WITH OTHER BUSINESS LEADERS

This gain often starts at the very beginning, by working to develop relationships with the business leaders. Sandersen says, "When I first started at Trek, I made appointments with all the senior leaders, the CEO, and all his direct reports, and mapped out the business processes that were essential to them." It helps to make an early connection with someone who really knows the organization, who knows who to talk to if you need to get things done, and can give you a head start in learning what the senior leaders of the business think is important.

In speaking to business leaders about security needs and requirements, Sandersen acknowledges that it's important to balance security controls against the cost and burdens to the business. This balance includes considering the impact a control or policy will have on people's jobs, whether it makes things more difficult or slows things down. These discussions need to happen in the context of the probability of those risks actually affecting the enterprise. As Sandersen explains, "By presenting the math behind the exposure and recommendations for addressing it, business leaders are less likely to wave away the issue." Engaging in this way has another advantage: By informing them of the risks and associated costs, and making it their decision to accept or mitigate those risks, the CISO is also putting those business leaders on the hook for accepting the risks.

Ultimately, it is essential for the CISO to build strong relationships with other business leaders in the organization because there will be times when the CISO needs their backing to enforce a new policy. Even when business managers and executives agree a new policy is the right thing to do, it may not happen, especially if it changes the way people work. Without those senior executives on the steering committee backing the CISO by saying this decision is the one we have made and this is what we are going to do, then it becomes much more difficult to make those kinds of changes and to enforce the policies that everyone agrees are necessary. "Sometimes it takes top-level executive buy-in and executive-level orders for people to actually comply. You really need to have those people on your side," says Sandersen.

> "By presenting the math behind the exposure and recommendations for addressing it, business leaders are less likely to wave away the issue."