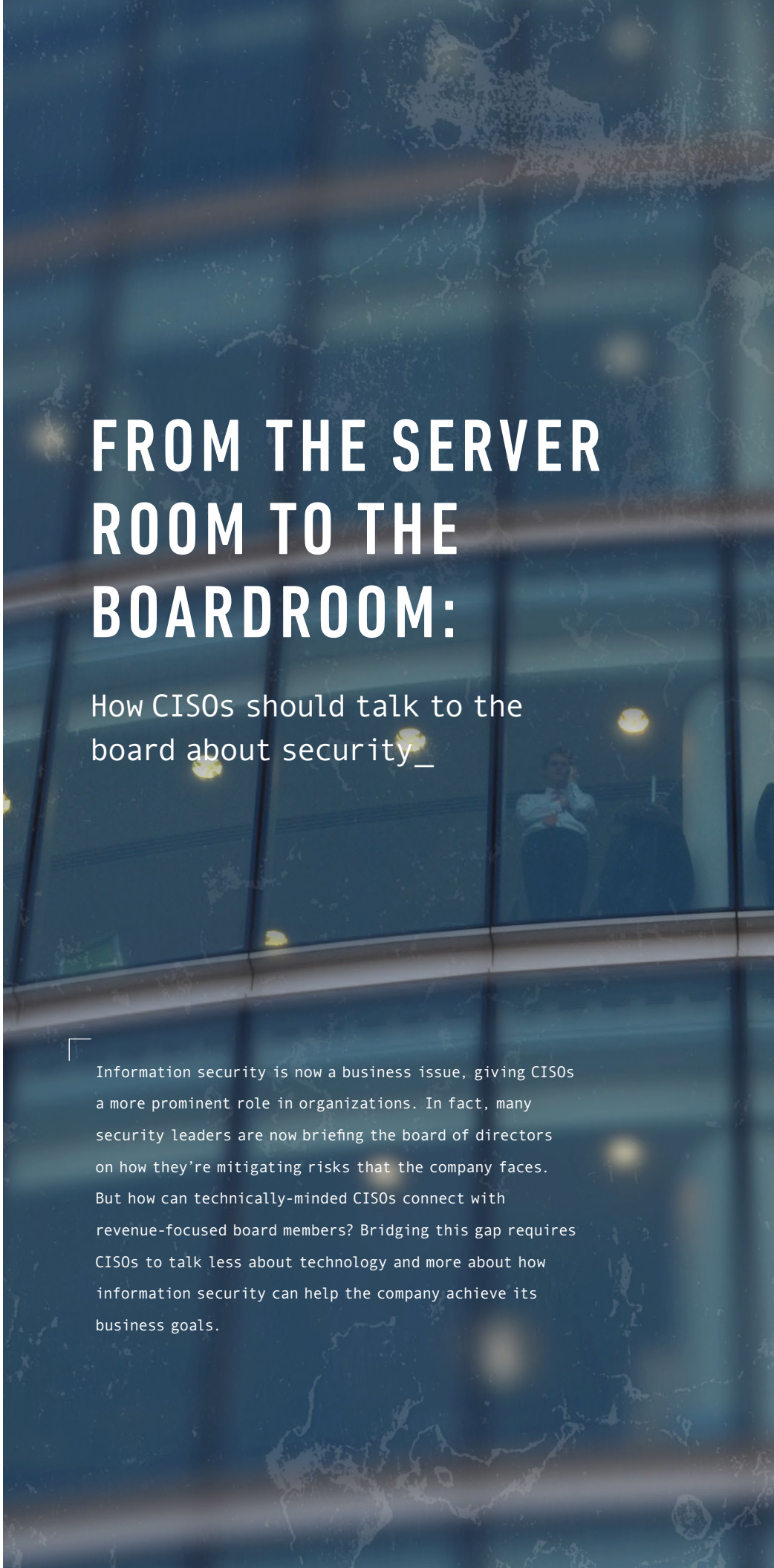
cybereason



FROM THE SERVER ROOM TO THE BOARDROOM:

How CISOs should talk to the board about security_

Information security is now a business issue, giving CISOs a more prominent role in organizations. In fact, many security leaders are now briefing the board of directors on how they're mitigating risks that the company faces. But how can technically-minded CISOs connect with revenue-focused board members? Bridging this gap requires CISOs to talk less about technology and more about how information security can help the company achieve its business goals.

INTRODUCTION_

Information security is no longer just about setting up a firewall or installing antivirus software. The prospect of a NotPetya-like attack crippling factories and hurting profits and Chinese hackers pilfering intellectual property (among many other security threats) has made keeping companies safe a critical business issue.

This development has elevated the CISO role. In fact, some security executives have escaped the server room and now meet with the board of directors to explain how they're mitigating information security risks.

But meeting with the board brings a new challenge: how can CISOs convey the importance of security to the board? They're trying to connect with results-driven executives who think about quarterly revenue and profit margins, not hot fixes and false positives. And the sight of the CISO in the boardroom can be off-putting, given that security leaders have a reputation for slowing or scuttling projects over security concerns.

> "CISOs need to do a much better job educating boards on risk. The challenge some CISOs face is not getting too much into the technical jargon and security jargon with the boards and talking more about why they should care."

RYAN GURNEY
CSO
LOOKER, A SOFTWARE-AS-A-SERVICE DATA ANALYTICS COMPANY.

To help CISOs better communicate security's importance to the board, Cybereason created this guide. We talked to CISOs and CSOs from a range of industries to get their insight on how security leaders can be seen by boards as business-savvy leaders instead of technology hobbyists.

BY READING THIS GUIDE YOU'LL LEARN:

- How to speak the language of business
- How to frame information security discussions around risk mitigation
- The importance of using the board to create a culture of security throughout the company
- Why boards should hear about information security failures

LEARN THE LANGUAGE OF BUSINESS_

CISO can earn the board's trust and respect by getting information security in tune with business operations. Accomplishing this task means security leaders need to learn the language of business and use it to frame conversations around information security. The concept is simple: relate every information security project to a business objective and avoid technical jargon.

> "The board is never going to learn technical language. It's better for us to speak business language. That's how you get your budget approved and support from the board."

ERIKA MATA SÁNCHEZ
DIRECTOR OF INFORMATION SECURITY AND CISO
GRUPO NACIONAL PROVINCIAL, OR GNP SEGUROS

CISOS CAN CONNECT WITH THE BOARD BY SPEAKING THE LANGUAGE OF BUSINESS, WHICH CENTERS AROUND SIX THEMES, SAID CYBEREASON CSO SAM CURRY:

- Risk
- Employee productivity
- Cost
- Revenue
- Strategic value
- Customer Satisfaction

"Don't talk about anything else except those six things. The biggest problem CISOs have right now is bridging the gap between security and business," Curry said.

RISK

Risk mitigation is the link between a company's information security department and business units. Board members want to reduce risk and the CISOs are the ones who can help accomplish this task.

When discussing risk with board members, CISOs should avoid spewing technical details on how they plan to mitigate a threat. The board doesn't need or want to know about server configurations or the nuances of the organization's patch management strategy. But they do need to know if the company can muster enough servers to prevent a DDoS attack and has patched the critical Windows vulnerability that lets attackers use the EternalBlue exploit.

> “It comes down to a matter of trust. If CISOs have built the trust with the board they don’t need to know the details. They just need to know what the risk is, the impact of the risk and trust the person to make the right recommendations.”

BOB BIGMAN
FORMER CISO
CIA

Security leaders need to frame any conversation about risk around how an incident would impact the business. Security leaders can use examples from the news to illustrate how a security issue can affect a company. That includes talking about lost revenue, legal ramifications or the cost of restoring the business.

“It’s really important to take advantage of the data that’s already out there. You’re working for a business. You have to present things from a financial point of view, from a legal point of view. That really helps people visualize things. That’s going to have a much bigger impact than just arguing for a certain technology or saying, ‘We should proceed this way because it’s best practices,’” said Luis Torres, director of information security at RhythmOne, a digital advertising technology company.

But that doesn’t mean CISOs should sell security by spreading fear, uncertainty or doubt. Don’t just point out the risks and explain how they could impact a company. CISOs also need to tell the board how they plan to mitigate those risks and come up with an action plan and timeline.

“It’s important to let them know the risks that exist. But it’s also important to let them know something is being done about it. They should know there are measures in place to prevent some of that and that there are plans to further address potential problems,” Torres said.

REVENUE

While security is usually viewed as a cost center, CISOs have an opportunity to show that their department can help an organization make money. Aligning security with revenue goals is the CISO’s best chance at demonstrating how security is in sync with the business.

While this point seems obvious, information security departments are often perceived as the department of no around approving products and services that are going to market. Even worse, security personnel, and the CISO in particular, are viewed as the people responsible for stifling innovation. And innovation gives a company an edge over competitors -- hurt innovation and you could hurt revenue, a situation that all boards want to avoid. “You have to demonstrate to the board that the intent is to enable the organization to do the things it needs to do to make money in a secure manner,” said Guy Daubenspeck, CISO at financial services company Kasasa.

> “We’re not in business to be secure, but if we’re not secure, we’re not going to be in business tomorrow.”

GUY DAUBENSPECK
CISO
KASASA

To avoid being seen as the department of no, CISOs need to talk to their colleagues and find out what projects different departments are working on. The sooner CISOs learn about upcoming projects led by research and development and the product and IT teams, for example, the sooner they can suggest ways to incorporate security. The result? Security is built into products and processes from the start, not tacked on as an afterthought. This leads to a secure product going to market, avoiding a sales delay due to security concerns and the board seeing a CISO who knows how information security can be used to help the business make money.

EMPLOYEE PRODUCTIVITY

Security is often seen as impeding employee efficiency and effectiveness. Countless employees can share anecdotes on how information security concerns prohibited their department from using a technology that would have increased employee productivity. Also, IT professionals can list security procedures and tools that slow down or crash employee PCs or make IT processes more cumbersome. If these stories reach the board, the CISO could be seen as enacting policies that slow down workers. To avoid giving the board the impression that security is stifling company productivity, CISOs need to adopt a “yes, but…” approach.

“There needs to be an understanding that you can’t just say ‘no’ across the board. You’ve got to say, ‘If you want to do this, yes, we can do it; but we need to include these technology controls or these process controls or this compliance control. We need to have some security attribute in the system, and then we can use it,’” said David Bryant, CISO of PSCU, a credit union services organization.

STRATEGIC VALUE

Information security has to show the value that it brings to an organization. Security programs can’t be carried just for the sake of security. They have to be conducted in the context of the organization’s overall business objectives and help the company meet those goals. In fact, the more financial-oriented board members may try to quantify security from a return on investment perspective.

Securing an organization is a critical part of any business but it isn’t the company’s sole function, a fact well-known to any board. CISOs, though, may struggle with accepting that they’re one piece, albeit a very important one, in the overall organization, said Jason Callahan, CISO and senior director of IT operations at Illumina, which designs and manufactures machines used for genetic analysis.

“Cybersecurity is not the goal of the organization. The goal of the organization is to turn a profit by selling a product or providing a service. Protecting that product is an important part of it, but that’s just one piece,” he said. “Good CISOs tie their initiatives and projects to the company’s strategic values and goals and showcase how security drives the company’s goals.”

COST

When buying security tools, hiring for the security team or making any security-related expenditure, show that the spend is smaller than the financial risk the company is exposed to by not addressing the vulnerability. This is especially true when discussing budgets with board members who relate everything to finance, money and return on investment.

"There have been many security incidents in the news and plenty of financial information has been published. Real world examples of financial impact are something that everybody in security can use to support their initiatives," RhythmOne's Torres said.

For an even more detailed view on how a business works, security executives should befriend the CFO and ask to look at the profit and loss statement. When discussing any financial matters with the board, CISOs can use these figures to illustrate a security incident's real fiscal impact. And if a company has been breached, the organization undoubtedly has numbers that show the revenue impact. A CISO shouldn't shy away from using them when talking about costs with the board.

> "If you've already been breached, then you'll have data regarding financial impact."
>
> **LUIS TORRES**
> DIRECTOR OF INFORMATION SECURITY
> RHYTHMONE

CUSTOMER SATISFACTION

Customers are undoubtedly on the minds of any board. After all, they're the ones who buy and use a company's products and help the organization make money. CISOs looking to prove to the board that they understand the business' needs should think how security can help a company's customers.

"Ensure that your employees understand that you're a customer service organization. I worked at Zendesk where being customer service company was so critical. It bled through the whole company how important that is, and it's great to see that in our security team [at Looker]," Gurney said.

At Looker, this means considering the customer when incorporating security into Looker's product. Gurney, for example, didn't want to make risk decisions for customers when determining what types of security controls to include in Looker's analytics software. Instead, he worked with the product team to develop safe default product settings that customers can adjust depending on their needs.

And CISOs shouldn't forget that the information security department also has internal customers to serve.

"My internal Peraton customers are the sector presidents and the business managers who use and work with security procedures every day to make their missions successful and, in a way, support me if I support them," said Phil Mazzocco, CSO at Peraton, which provides services to the U.S. government.

"From increasing revenue to breaking into new markets, a CISO's internal customers are always looking for ways to increase business overall", said Sue Bergamo, CISO and CIO at digital commerce and content management company Episerver. CISOs need to be aware of what projects the business is working on and offer advice on how to incorporate security.

"In some cases, it may be a directive, but in my mind, it's more to offer guidance while they're out there trying to grow a business. The CISO needs to help protect what the business is trying to do," she said.

SECURITY TAKES A VILLAGE_

CISOs should explain to the board that information security is everyone's job and that anyone can bring potential security issues to the information security team. Protecting an organization includes the obvious initiatives (like keeping increasingly sophisticated adversaries at bay) as well as the less obvious ones (like getting product teams to consider the benefits of forcing users to change the default password on an Internet-connected device). This mindset shows that a CISO has a more expansive view of the risks facing an organization and is thinking holistically about risk.

> "They should know that security is not just people who interact with a certain system, but that it's more widespread across the company. Present security in a way that lets them know anybody can ring the alarm if they see anything out of the ordinary."
>
> **LUIS TORRES**
> DIRECTOR OF INFORMATION SECURITY
> RHYTHMONE

CISOs shouldn't be afraid to enlist the board's help in spreading a culture of security across an organization. Security programs only succeed with the support of an organization's board. After all, the board helps determine the priorities for a company and its executives. Getting buy-in from the board on security can strengthen an already robust program or start building the foundation for one.

"You need the support of the board of directors and other executives to have this culture across an enterprise When you do, it makes information security stronger," Mata Sánchez of GNP Seguros said.

DON'T SHY AWAY FROM DISCUSSING FAILURE WITH THE BOARD _

Talking about security failures with the board seems like a sure way for security executives to lose their jobs. But bringing up what went wrong is the only way for organizations to learn and improve their defenses. No one benefits when security mistakes aren't discussed.

"If I'm not comfortable going to the board and saying, 'We've had this happen because of a failure in our enterprise level of security,' then we're not going to learn the lesson so that we can prevent it from happening again. We learn our most important lessons the times we've failed," said Guy Daubenspeck, CISO at financial services company Kasasa.

A crisis is an opportunity, said the CIA's Bigman. To him, discussions on how to improve security are rarely held when a program is succeeding. In fact, just the opposite happens: budgets are usually cut. But when there's a problem, everyone (especially the board) is interested in figuring out what went wrong and how to prevent it from happening again.

> "If something went wrong, you almost always have improvements in your security as a result. When there was a crisis [at the CIA], that's when there was more interest in what we did and people were more receptive to hearing how to fix this. I was not crisis averse. I looked at a crisis as an opportunity."
>
> **BOB BIGMAN**
> FORMER CISO CIA

IT'S NOT ALL ABOUT INFORMATION SECURITY_

Sorry, CISOs, it's not all about you when talking to the board. Yes, the board wants to know about information security, but only in the context of how it helps the company mitigate risk, retain customers, grow revenue, increase employee efficiency, show strategic value and prove cost effective. In other words, use the language of business to show how information security can help the business achieve its goals. Remember, your job is to understand a business' needs and develop a security program that supports those initiatives.

"We really have to figure out what the business' real goal is and what the problem is. Then we have to allow them to work toward that goal, but we have to put safeguards around it that will allow them to do it in a manner where we're not exposing ourselves to risk," said PSCU's Bryant.