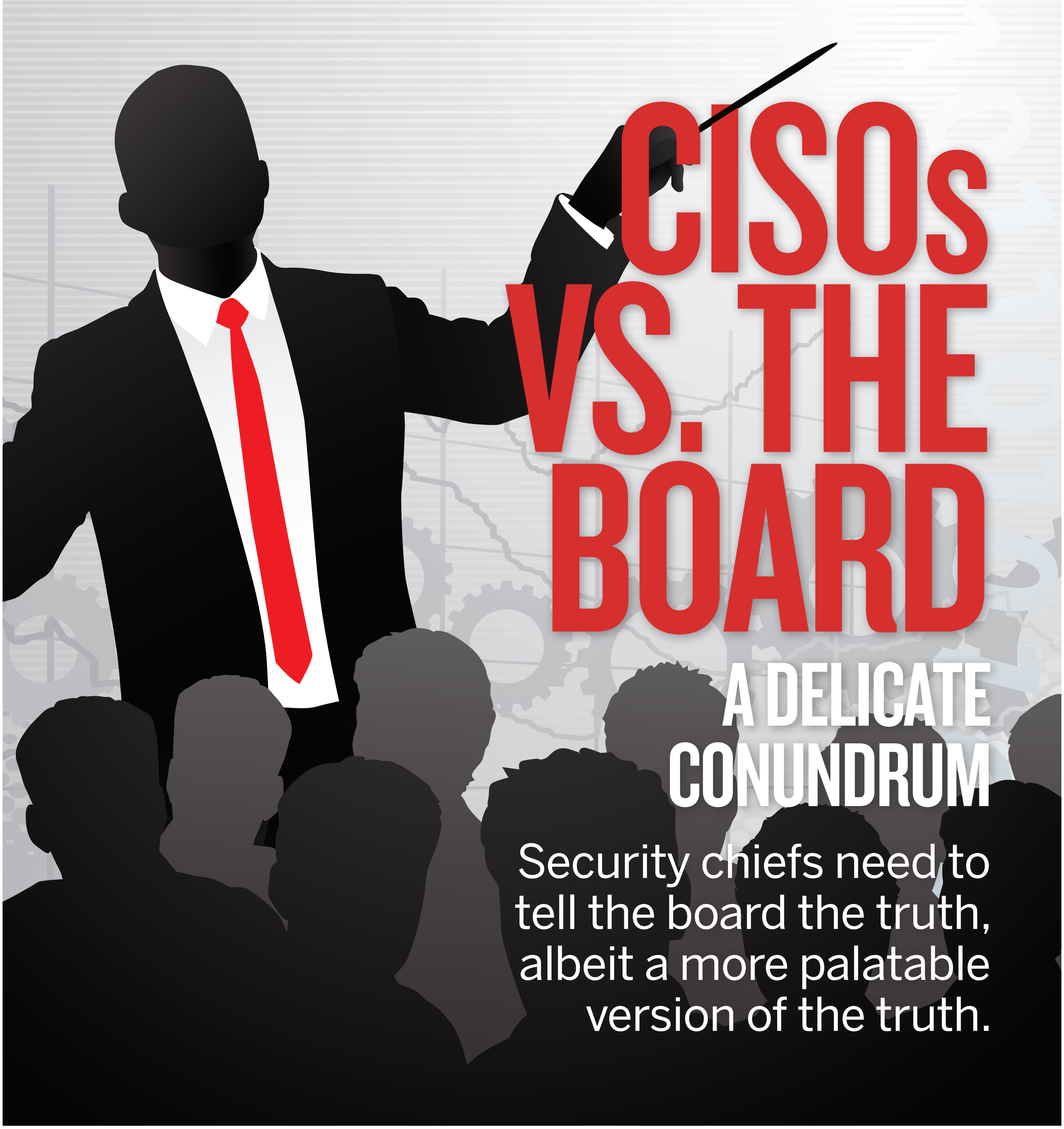

CISOs VS. THE BOARD

A DELICATE CONUNDRUM

Security chiefs need to tell the board the truth, albeit a more palatable version of the truth.

ebook
An SC Media publication

Talking to the board of directors: Shun brute honesty and techno jargon

CISOs need to learn to speak the language of the board if they expect to impact security decisions or find a sympathetic ear. Evan Schuman explains how the dance works.

For Fortune 1000 CISOs and CSOs, reporting to their boards of directors is, at best, a complicated and disquieting situation. CISOs must be specific and technical, but not *too* specific nor technical. They must be honest and comprehensive, but they also need to know which truths are best left unsaid.

CISOs facing a corporate board briefing might well be asked questions that forces them into the sensitive area of corporate politics. Questions such as: "Did you fight for this perimeter defense that we don't have?" must be answered truthfully, but the truth, unlike data, is not a binary "yes" or "no."

OUR EXPERTS:
Talking to the board

Mark Adams, practice director, Optiv Security
Marti Arvin, executive advisor, CynergisTek
Dan Burke, VP of cyber, Woodruff Sawyer
Kevin Carlson, partner, TechCXO
Rema Deo, managing director, 24By7Security Inc.
Jennifer DeTrani, general counsel and EVP, Nisos
Sean Goodwin, senior security consultant, Wolf & Company
Nick Merrill, founder, Broad Daylight
Dominic Wood, head of global security, BT Group

These encounters today come at a time when board members of publicly-held companies are being held to higher standards about security, when board members can be personally sued and even exposed to legal penalties.

Compliance issues, especially new rules specifying privacy requirements, can force board members to engage technical discussions where they might not be especially comfortable.

The question that perhaps best illustrates the conflict is "If we agree with your proposal and fund this effort, will it prevent any breaches? Will it make us safe?" The only completely honest answer is the one many CISOs fear giving, as it is absolutely not what board members want to hear: "Not necessarily."

Relative truth

"You're never going to get to a perfectly secure environment," says Sean Goodwin, a senior security consultant with Wolf & Company, a 107-year-old, Boston-based accounting firm.

When a board member asks the CISO, "How strong is our encryption?" the last thing that board member likely wants to know is the number of bits or other techno jargon. The board member wants to be told that the encryption will keep the company's data safe. How strong essentially is a board member's way of asking: Are we safe? Speak comfort to me.

Dan Burke, vice president of cyber for the San Francisco-based insurance broker Woodruff Sawyer, says that instead of answering the "will this block any attack?" question directly, the CISO should put the question and the answer into an appropriate context. "If they ask a question about encryption, they are not really wondering about encryption. They want to know: Are we doing everything we can to protect ourselves from an attack in an industry-acceptable manner?"

In short, tell the board that the investment

50%

Percentage of privileged accounts that never expire or get deprovisioned

– Thycotic

will make the company appropriately secure, given its position and the nature of the most likely attacks. Compare your company's defenses with other comparable businesses.

Jennifer DeTrani, general counsel and EVP, Nisos

Jennifer DeTrani, general counsel and EVP at Nisos, a cybersecurity consulting firm based in Old Town Alexandria, Va., says CISOs can face very troubling questions, perhaps even questions that have been posed before. "Remind the board member of what has been decided in the past. What has happened since the last board meeting may not be on the top of their mind," DeTrani says.

"Regulators have never been hungrier to make examples of companies. You are, in a sense, a [compliance] target," she warns.

One nightmare scenario when the CISO meets the board is if a board member asks about a project that would reveal too much insider discussions. Let's say the board member asks the CISO, "I was just reading in the business press about a security method that one of our competitors has deployed. Why aren't we doing that?"

> "Regulators have never been hungrier to make examples of companies. You are, in a sense, a [compliance] target."
>
> – Jennifer DeTrani, general counsel and EVP, Nisos

In this particular case, the CISO had been arguing for six months that the company should indeed deploy that approach, but the dollars were vetoed — repeatedly — by both the CFO and the CEO. Should CISOs give into temptation and throw their bosses under the bus in front of the board? Probably not, yet the CISO must also answer truthfully.

The best approach, DeTrani says, is to suck it up and give the corporate team answer, while also giving an honest opinion. Here is a typical example of such a response: "Thanks for asking. I happen to very familiar with that technology and I'm also a big fan. It can work extremely well and it's not especially disruptive to deploy. That said, it's not an inexpensive approach. We seriously considered it, but competing financial issues — such as the changes to our supply chain that we discussed and that acquisition in Italy — forced us to decide to not deploy at this time. We will absolutely reevaluate it next year and, depending on what the numbers look like, it's a possibility that we will then come to a different decision. In short, it's impressive technology but not one that we can cost-justify at this time."

If treading into this level of board-level politics doesn't keep the CISO up at night before a board meeting, it is difficult to imagine what might.

In the opinion of Rema Deo, managing director for 24By7Security Inc., a security and compliance consulting firm in Coral Springs, Fl, boards have little to no interest in being the best — and certainly not paying for the best — in security. They want good enough, given that company's security position.

Most corporate boards "don't want to be ahead. They don't want to spend too little or too much. A little ahead is fine," says Deo, who also holds a healthcare security certification. But the point CISOs must stress is that "no matter how much you spend, this is not completely foolproof. We can only work to reduce the risk."

But risk means something very different to the typical large-company CISO and the typical large-company board member. It is up

39%

Percentage of midmarket and enterprise companies taking a cloud-first approach to new application deployments

– Enterprise Strategy Group

to the CISO to describe all of the germane risks and to offer examples that will be meaningful for board members. That can be particularly difficult when board members come with a wide range of experience, expertise, technical acumen, and from different cultures.

Kevin Carlson, partner, TechCXO

Thought experiment

"CISOs and other security managers need to steep themselves in the language of risk, downside, and liability familiar to executives and general counsels. 'Breach' is abstract. 'Legal liability' is specific," says Nick Merrill, founder of the Berkeley, Calif.-based cybersecurity consulting firm Broad Daylight.

"Here's a thought experiment I play with almost every non-security executive I talk to," Merrill continues. "If your customer database leaked, what would happen? Legally? In business metrics? What about your HR database? What would happen if your technical systems went down for an hour? A day? A week? The key is to get executives to quantify — however roughly — the monetary harms of likely cyberattacks. Once execs can price the attacks, they know how seriously to take them relative to the other five thousand things competing for their attention."

> "The key is to talk about how you're reducing risk and keeping the business running smoothly, not how you're running your own operations."
>
> – *Mark Adams, practice director, Optiv Security*

Still, such explanations do not always come easily to veteran CISOs. "Security specialists often miss that quantitative story of downside risk. Security folks like myself are trained in the technical and operational aspects of security," Merrill says. "The business and liability story often gets lost in translation."

Kevin Carlson, partner at Atlanta-based consulting firm TechCXO and a part-time CISO for hire, offers this insight: "This should include information on how it will affect compliance measures, the timeline and cost for mitigation efforts and the effect on staff and other company priorities."

Goodwin offers another example where the proper context can make a huge difference when presenting to the board: penetration testing. "A pen tester is always going to find something wrong. You really need to properly frame the results," he says.

That might mean pointing to the decrease in the number of issues discovered or, even better, a sharp reduction in how many of the issues are considered critical. That might mean stressing the stage of development, if it is relevant.

"Saying something like 'you have weak password requirements' is not as powerful as showing them how password spraying works and how anyone can guess easy passwords to log into their systems remotely," Goodwin says.

Goodwin also stresses that audit reports especially need extensive context.

"All too often I see audit reports calling out things like missing patches year after year. When looking at this from the perspective of a board member, it seems like management is simply not fixing issues after being repeatedly shown what to do. The consultant is not doing their job by just calling out a list of missing patches," Goodwin says.

2022

By 2022 cybersecurity ratings will become as important as credit ratings when assessing risk

– Gartner Innovation Insight for Security Rating Services, July 2018

"They need to be digging into the people, processes, and technologies in place to figure out why these patches are missing," he continues. "Perhaps there is a legitimate business need for excluding some of these, or perhaps resources are not allocated appropriately for identifying testing and deploying software patches."

Merrill says that he often hears of CISOs who present to boards, but do not effectively communicate because they leave too much to the imagination of board members, who might often not see the impact of security issues. "The CISO failed to connect the threat to the kind of harm [done] to shareholder value," Merrill says. "To the CISO, it was obvious."

Mark Adams, practice director, Optiv Security

Merrill argues that CISOs must make the human case to board members — and starting with a potential hit on stock price is a terrific way to grab the board's attention. "Talk about the human impact to board members. What is it going to mean for their portfolios?"

Dominic Wood is the head of global security for the BT Group, the $31 billion U.K. communications giant formerly known as British Telecom. He argues that differentiation is a key argument that CISOs use too rarely.

"One way to present security compliance issues to the board is to frame it as a key differentiator that will give them a competitive advantage in an increasingly digital world," Wood says. "Just as the use of interconnected technologies is unlikely to slow, so the importance of rigorous security protocols and systems will continue to grow, and consumers are growing increasingly aware of this."

Board members "have the right to know and understand the risk in detail," Wood says, but CISOs often "wrestle with the right level of details." Although he argues that "the level of technical understanding [for board members] is far better than it's ever been, having a purely technical conversation kind of misses the point."

Mark Adams, a practice director for risk transformation at Optiv Security, a security systems integrator based in Overland Park, Kan., agrees that CISOs need to learn the phrasing that works for well for the board.

"CISOs need to learn the language of enterprise risk. Business leaders don't care how many attacks you blocked today," Adams says. "They do care how much intellectual property you prevented from walking out the door with employees or how much revenue/minute you saved by stopping a DDOS attack on your e-commerce site. The key is to talk about how you're reducing risk and keeping the business running smoothly, not how you're running your own operations."

> "Not only do [board members] not know about security, they don't even know about what you think they know about."
>
> – *Nick Merrill, founder, Broad Daylight*

Adams points to the approach to security measurement as being a big part of the communication problem.

"At the board level, security leadership must take an inside-out approach to security measurement, where they demonstrate alignment between technology, operations and business objectives. Many security leaders take an outside-in approach, where they start with external threats and then highlight the tools they're buying to combat them," Adams says.

4.6%

Percentage increase in software and IT services hiring in 2019 over 2018

– LinkedIn

"This approach makes it impossible to prove value. Buying a tool to stop a type of threat does not prove anything and it drives the bloated infrastructure and operational problems that are perpetuating the breach epidemic," he notes.

Marti Arvin, executive advisor, CynergisTek

Marti Arvin, an executive advisor at CynergisTek, a healthcare cybersecurity consulting firm, points to cybersecurity insurance as a good example of a rarely-referenced example of risk. Arvin says some board members think "We've got cybersecurity insurance, so we're OK, right?" The proper CISO reply, says Arvin: "'Are you sure that we're covered? Part of the coverage criteria may be something that we're not doing, such as a specific approach to patch management.' Put it in business terms."

Do you know the time? Yes.

One factor that can cause a collision course between the CISO and the board is psychological. Many board members are not comfortable with security technology. When people are uncomfortable, they tend to have a greater desire for absolutes. CISOs can often be a little nervous when presenting to the board of directors.

When highly-trained technologists get nervous, they tend to default to precision in their language, which can mean getting technical. This sets up a scenario where both participants want something the other is uncomfortable offering. In short, a highly likely communications collision.

This is an example where training plays a big role. Many senior executives — CISOs and CSOs among them — get trained by the legal department how to testify in court and how to give legal depositions. And those executives almost never get trained in speaking to the board.

The legal training stresses that they must be precise and, most critically, to answer the questions asked literally and without volunteering anything. The quintessential line that epitomizes this comes from an episode of the popular television drama *The West Wing* in which a lawyer asks, "Do you know what time it is?" The correct answer is not "It's 2:17 p.m.;" the correct answer is, "yes."

Those are fine skills for the courtroom, but it is the opposite of how CISOs need to communicate with their boards. It is not about answering precisely what is asked; it is about interpreting the question and the context and saying what the CISO thinks the board member really wants to know.

Know your audience

Who are these board members? Although it is widely known among CISOs that board members tend to not have technology backgrounds — and especially not in data and cybersecurity — a popular misperception is that the board of your company knows your company intimately. The internal board members (your CEO who might also serve as chairman of the board and perhaps your CFO or others senior executives) certainly know your company, but many of the external board members might not.

> "One way to present security compliance issues to the board is to frame it as a key differentiator that will give them a competitive advantage in an increasingly digital world."
>
> *– Dominic Wood, head of global security, BT Group*

First, the typical external board member

80%

Percentage of data breaches that involve privileged credentials

– Forrester

has a different primary focus, whether it is serving as an executive for a different large company or perhaps the board member is retired from such a position. It is not unusual for board members to serve on four or more different boards. And given that your board might only meet monthly or perhaps once every two months, it is not unheard that a board might not be aware of a key move that your company made in the past year, especially if the move did not require board approval.

That means that presentations must present any relevant background directly.

Nick Merrill, founder, Broad Daylight

"Not only do [board members] not know about security, they don't even know about what you think they know about," which is your company's key recent history, Merrill says.

The CISO is before the board primarily to do one thing: identify and mitigate risk in all of its many forms. Think of it as a verbal equivalent of those risk descriptions in the back of an initial public offering prospectus where the lawyers dream up anything and everything that could possibly go wrong. That is what many boards expect the CISO to do routinely when meeting with them.

CISOs can also take a lesson from lawyers who are used to arguing before the Supreme Court, whether at a top state court or the federal level. They study each justice's history of decisions and are prepared to answer each justice with references to their specific earlier decisions. In the board room, the extensive bios and histories of each board member is easily found.

The CISO can know which company they run, as well which other boards they have served on and when. This could allow for the CISO to cite extremely germane examples that would have meaning to that board member. "Last year, ma'am, when XYZ suffered a breach, your team there deployed an ABC strategy. What we're proposing is just about the same thing, except that we're proposing 123 instead of 567," Merrill says.

"These different board members — you can find their histories. Use that to your advantage," he adds.

Here is a common question that can get CISOs into trouble: When describing a bad security problem, they could be asked, "How likely is that to happen?"

Sometimes, Merrill says, "the CISO punts on the likelihood. 'We cannot establish the likelihood. It is fundamentally unknowable.' And sometimes, the CISO tries to quantity. CISOs don't really know."

But Merrill says not every question needs to be answered directly. "Board members are used to not knowing things. [It is an error] that CISOs think that they need to answer that question. Nine times out of ten, it's an error that they think they have to answer it and it's incorrect to answer it."

Yet again, it just requires context and explanation. A CISO can point to other companies that have been attacked in that way, but must stress that there is little solid data to predict definitively whether cyberthieves will choose to attack your company.

All a CISO can do is prepare operations in as secure a method as practical, given that no one has an infinite budget. ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

63%

Percentage of respondents who said their company cannot turn off privileged access for an employee within a day

– Centrify