tripwire

Top Five Tips for Communicating Information Security to the Board

Introduction

Given the high level of recent highly-visible security incidents, convincing a board of directors that information security matters should be an easy task—in theory, at least. In reality, it's much easier said than done.

From a lack of technical expertise on the board to the challenge of framing security metrics in a business context, security professionals—and CISOs especially—have their work cut out for them convincing the board to act wisely. So how does the CISO gain the attention of the board, and how do they justify future investments?

Raising Real Awareness

In August 2018, Tripwire conducted a cyber hygiene survey of 306 IT security professionals, all of whom are responsible for IT security at companies with more than 100 employees. The survey was conducted in order to assess how closely their organizations follow basic security controls.

Basic security controls are defined here by the CIS Controls, a prioritized set of steps maintained by the Center for Internet Security. There are 20 Controls, but implementing just the basic first six establishes what CIS calls "cyber hygiene."

The first control, for example, is hardware inventory and control. The study found that few organizations can say they have an inventory of the devices on their network: Only 29 percent track more than 90 percent of devices, and a third track less than 70 percent. More organizations say they're detecting new devices on their network within minutes (43 percent) than participants in a survey three years earlier (32 percent). That still leaves a majority (57 percent) who take hours, weeks, months—or even longer.

Organizations have an even harder time tracking software than the hardware on their network. Only 21 percent track more than 90 percent of their software, while 56 percent track less than 70 percent.

What about organizations' ability to enforce effective vulnerability management? The survey found that almost all participants are running vulnerability scans. However, only 50 percent are running authenticated scans, which are the most comprehensive. Forty-one percent of participants are running scans monthly, quarterly or less frequently—when weekly or more is recommended.

Most (56 percent) are able to deploy a patch within a week, but about a quarter are still taking about a month or longer. Among organizations that have implemented DevOps, 46 percent aren't scanning for vulnerabilities throughout the continuous integration and deployment (CI/CD) pipeline.

Drawing on the insights from this report, Tripwire has developed the following five tips to help CISOs communicate security at the board level.

> "Connecting what security teams are doing to recent high profile cybersecurity events is a great way to connect with boards and executives … If you can tie it back to that breach they already know about, give them a little bit of the inside scoop, and say, 'Yes, we know how that happened, and that incident points out just how important this one security control is,' then you have a jumping off point to educate them about a particular area of security…"
>
> — **Dave Meltzer**
> Chief Technology Officer, Tripwire

Tip 1 — Align cybersecurity to your organization's priorities

The first role of the CISO is to get to know the rest of the business, to understand the commercial agenda of the organization, and to have a clear picture of its priorities. This involves close communication and involvement with all departments, from HR to Marketing.

The benefit of this extensive and regular groundwork is that the CISO gets a reputation for helping to make things happen, and for helping department heads to avoid serious mistakes. By becoming an ally of each line of business, the CISO can then approach the board with much more confidence, and with support from fellow senior leaders.

Breaking down communication barriers is therefore essential, and it requires the CISO to take the initiative. The worst thing that any head of security can do is to get a reputation as the person who says no to everything. It is something of a cliché, but unless the security department can become an enabler for the rest of the business, it will get sidelined and bypassed in the decision-making process.

For example, if employees are being encouraged—or are insisting—to use their own mobile devices, then security needs to provide guidelines and help to make it happen in a secure fashion rather than attempting to ban it.

"While the technologies we use in business may change, the threat actors and the threat landscape will in many ways remain constant... The big change will be the technical savvy user who will look to use various devices, apps, and services... As such, CSOs will need to better communicate and engage with users to make them aware of the risks and provide secure alternatives."

— **Brian Honan**
Founder and Director of IRISS (Irish Reporting and Information Security Service, Ireland's first CERT)

Tip 2 — Understand that cybersecurity risk reduction requires the entire organization's support

With greater regulation and legislation in many industries, directors—even non-executive directors—may carry personal liability for any serious security breaches that the organization experiences. That personal responsibility can do wonders to focus the mind on security matters. The CISO in these circumstances becomes an important sounding board for their concerns.

Directors now realize they are more accountable and so when they read about breaches or see them on TV, they will want to know if their organization could be affected and how the CISO has prepared to meet the challenge.

As Tripwire's CTO David Meltzer puts it, "Connecting what security teams are doing to recent high-profile cybersecurity events is a great way to connect with boards and executives. The latest major breaches all make it to the front page of the news, so you can assume you don't need to convince these people that security is a real problem and they should worry about it. They know it is a problem, and they are worried. But they probably do not know what they can actually do about it."

"So if you can tie it back to that breach they already know about, give them a little bit of the inside scoop, and say, 'Yes, we know how that happened, and that incident points out just how important this one security control is,' then you have a jumping off point to educate them about a particular area of security, why it is important to them, and how the budget and priorities they are setting can keep them out of the news.'"

CISOs should also develop personal relationships with other department heads and meet on a regular basis to address concerns and to provide assistance.

For example, one successful CISO based in the U.K. has a daily meeting with her head of internal audit to exchange information. The reason cited is that any fraud investigation might involve information security, and any information security concerns might indicate fraud.

By conducting such regular meetings, CISOs not only establish their credibility, but can assess where the business is going, what its priorities are, and where the new areas of risk might be.

> "As an executive, you should know that managing cyber threats is no different from managing other business risks... while you can skip the technical details you absolutely can't skip understanding how different threats would affect your business."
>
> — **Tim Erlin**
> Vice President of Product Management and Strategy, Tripwire

Tip 3 — Communicate in a way board members will understand

The successful CISO is always prepared to answer the question "Am I at risk?" by showing what they're doing to keep risks under control. Therefore, when a big breach (such as WannaCry) hits the mainstream press, the CISO needs to be proactive in informing board members about the threat, whether they are at risk, and how the risk is being mitigated.

Andrew Rose, chief security officer at VocaLink, says, "Visibility and influence at the board level is something that CISOs have sought for many years, and now it's becoming a reality. Unfortunately, many CISOs are struggling to deliver. Put simply, board members have a single question, 'How secure are we?' CISOs know that this is an almost impossible question to answer; however, we have no choice."

"Acknowledging this, you must seek out peer comparison, maturity assessments, and real-world examples to answer this question in as pragmatic a manner as possible. You can also tie your answers to established business metrics and show how your function not only protects your company's investment but builds value, too."

One CISO recommends creating a standing agenda with the board outlining three main risks (such as loss of customer data or intellectual property) to help maintain a focus on key business assets while providing a continuous benchmark of success from one meeting to the next.

One other way of maintaining contact with the board is to explain the threats that have been repelled and also any "close calls" that have occurred. By doing this, the CISO builds up a reputation for delivering good news and reassurance, rather than only appearing whenever a breach has occurred.

It also means getting the language right. CISO and award-winning blogger Thom Langford suggests, "One approach is to try to convey cybersecurity risks to executives in terms that they readily understand, e.g. financial, personnel or legal."

For instance, one CISO working in the insurance industry has applied actuarial techniques to illustrate, via graphs, how certain risks might be reduced by certain levels of expenditure. With the choices presented in a familiar way, the board can decide what level of risk it is prepared to accept—or how much it is prepared to spend to reduce the risk.

> "...Board members have a single question, 'How secure are we?' CISOs know that this is an almost impossible question to answer; however, we have no choice. Acknowledging this, you must seek out peer comparison, maturity assessments and real world examples to answer this question in as pragmatic a manner as possible."
>
> — **Andrew Rose**
> Chief Security Officer, VocaLink

Tip 4 — Find mentors in your organization to consult with on board presentations

In order to build up credibility and some level of personal rapport, the security chief should also miss no opportunity to meet board members outside the context of the formal board meeting. In addition to board members themselves, teaming up with a trusted partner in the marketing department can help you position and contextualize your board presentations for optimal response.

As Sarah Clarke, founder of Infospectives puts it, getting the perspective of your audience is vital. Asking for their input serves three key purposes:

1. Confirming the problem you want to solve is one they are aware of and consider a priority
2. Finding out about competing priorities your audience has that you could use the presentation to address
3. Making sure the audience immediately understands your pitch in terms of both language and supporting info

If you don't get in their heads, you will be the equivalent of a coffee break—time in the meeting to switch off and think about something else. For example, one successful CISO said that when board members assembled at a hotel the night before a board meeting, he would join them in a social setting and use the chance to chat to them on a personal level.

Another recommended that an aspiring security chief would benefit by asking to be mentored by a board member. As information security speaker Jitender Arora says, "Board and C-execs are pressured to strengthen the balance sheet and improve the profitability of the business. They have a number of challenges on their mind and cybersecurity happens to be just one of many. Boards are not clueless about cybersecurity but badly informed because CISOs often fail to connect with the board. CISOs have yet to master the skill of perception management but they don't have to look far to learn from experts."

"CISOs should look for mentors within their organization who are experts in communicating effectively and perception management i.e. Internal Communications and Marketing departments. Every CISO must have a marketing champion in their organization with the sole purpose of building the positive image of the cybersecurity function and articulating value provided by the function to support the business. CISOs need to gain trust and build credibility with the board and C-execs. This cannot happen overnight, it's an organic process that requires persistent effort. Mentors can really help and act as a catalyst in achieving this outcome."

"CISOs should look for mentors within their organisation who are experts in communicating effectively and perception management... Mentors can really help and act as catalyst in achieving this outcome."

— **Jitender Arora**
Information Security Speaker

Tip 5 — Establish consistent communication beyond board meetings

The key is not to wait until the board meeting to communicate. Engage colleagues in other departments and establish your credibility. The security chief needs to establish a regular drumbeat of information about what is happening in information security, and especially about what is happening to other companies in the same industry. In that way, the CISO becomes a regular source of valuable information.

Jitender Arora says, "CISOs spend a lot of time communicating via scare. Trust and credibility need to be earned based on the consistent and persistent delivery supported by effective communication when talking about the success in delivering desired business outcomes. Board members are strategic with diverse experience and they focus on the big picture. CISOs need to position themselves as a strategic advisor by articulating strategic vision with a robust plan to win their trust and get their attention."

"Getting attention once is easy on the back of an incident or an external event. However, keeping that attention and staying at the top of the agenda is difficult—out of sight is out of mind. Relevant and meaningful metrics go a long way when dealing with the Board and C-execs because they get metrics. But before you introduce metrics and show reports at board level, it's important to test them with key influencers, internal mentors and trusted allies close to the board. By presenting relevant and meaningful metrics, the CISO can effectively articulate the return the business is getting from the money spent."

Successful CISOs do not just turn up for their allotted 15 minutes in front of the board, communicate their message, and expect to be listened to. All agree that the presentation itself needs to be the culmination of many smaller regular briefings and communications that will lay the ground for the presentation itself.

> "I believe a shake-up is overdue. Infosec professionals need to shrug off the trivial or "tick box" image of awareness. We should create a new role, a Security Communications Manager, who could be tasked with improving stakeholder interactions from shop floor to boardroom and using proven marketing and psychology tools to get it right. Effective communication isn't just a nice to have; it's the hub around which all security value cycles.
>
> — **Sarah Clarke**
> Founder of Infospectives

Conclusion

The key to success for any CISO is to communicate regularly with department heads and board members. Establish credibility by delivering valid and timely information that supports the business in its goals. And become known as an enabler.

To get started, download our workbook Communicating Cybersecurity to Boards and Executives

Request Your Demo Today

Let us take you through a demo of Tripwire® ExpertOps℠, our managed service solution that includes customized, board-ready metrics and reporting.

Learn how Tripwire's suite of security and vulnerability management products and services can be tailored to your specific IT security and compliance needs.

Visit tripwire.com/contact/request-demo

Learn More

1. Cyberliteracy for Boards and Executives resource page
2. UK Executive Cybersecurity Literacy Survey Highlights
3. Improving Cybersecurity Literacy in Boards and Executives article
4. The Voice of the CISO: Interview with Amar Singh
5. The Voice of the CISO: Interview with Thom Langford
6. Hem Pant, ING CISO, on Empowering Executives Through Cybersecurity Literacy article
7. Jitender's Perspective: Clueless Board... or Inarticulate CISO article

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at** tripwire.com

***The State of Security*: News, trends and insights at tripwire.com/blog Connect with us on LinkedIn, Twitter and Facebook**

BRCISTB2a 1905