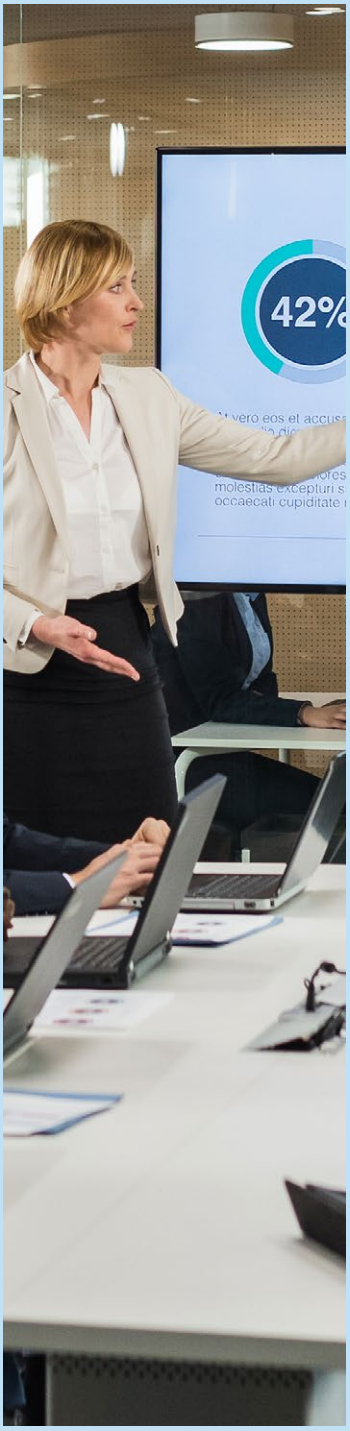
VIEW POINT



CYBERSECURITY IS NOW A BOARDROOM PRIORITY: WHAT CISOs NEED TO KNOW

Abstract

Chief information security officers or CISOs are in the business of selling confidence to the Board. The most effective way to do this is by producing tangible results such as no breaches, low vulnerability scores, and minimal attacks. However, it can be difficult for Board members to fully understand how these metrics translate to business benefits. Communication is often laden with technical jargon, leading to poor alignment between CISOs and overall enterprise strategy.

This paper examines some of the best practices and solutions gleaned from industry leaders on addressing problems within the cybersecurity space. It focuses on the rising importance of CISOs and provides guidelines for them to align their communication with Boardroom members.

Infosys®
Navigate your next

Introduction

Cybersecurity has evolved immensely over the years. In the beginning, cybersecurity was mostly about policy making for IT organizations, particularly for programmers, networking teams, and telecom providers. Dialogue often revolved around regulations, privacy, and compliance.

Today, cybersecurity has risen to become a Boardroom priority, particularly amid rising incidents of cyber-attacks on corporate as well as government organizations.

While cybersecurity is something that Board members want to be apprised of, it is important for chief information security officers (CISOs) to exercise caution while communicating that the digital environment is secure and free from risk.

The Role of CISOs

Simulations are the best way to depict the impact of security attacks. Hence, from ensuring there were no open modems in the network, today's CISO is tasked with simulating and addressing security events, particularly low-probability high-impact events. A typical day could involve running a 24-hour executive simulation program of different cyber events with top-level executives such as CFOs and CIOs. In today's enterprise IT environment, there are only two scenarios. Either the company is compromised and the CISO is aware of it or the company is compromised and no one is aware. The consequences of the second scenario are far more dangerous, emphasizing the need for real-time intelligence and up-to-date strategies.

Here are three key principles that CISOs should follow:

Know what you have. This refers to existing assets and assets to be protected. Some factors to consider are the layout of the enterprise network, whether data is classified, where sensitive data is located, etc.

Know and prioritize threats. CISOs must be aware of the relevant threat actors and their signatures, and what technologies help to safeguard against these attacks. A useful rule is to match the highest threat vulnerabilities to the greatest technology protection mechanisms.

Be prepared to recover from any incident. Security incidents are inevitable, no matter how much effort is spent on protecting the enterprise. Thus, apart from focusing on prevention, CISOs should also be prepared to respond and recover.

Digitalization technologies and IT are proving to be a great boon to industries today; but these quickly turn into a bane in the presence of inadequate security measures and controls. Hence, the role of CISOs today is becoming more critical to ensure that the organization continues to operate safely in order to reach its business goals.

What Boards Want to Know

On their part, the primary responsibility of Boards is to protect the assets of the company and the stockholder interests in those assets. The Board typically spends considerable time in understanding various risks; and cyber risk is one among them.

Cybersecurity is a new but concerning field, and Board members often have numerous questions to assess whether they are above risk. It is up to the CISOs to periodically engage with the Board, gently sensitize them to cyber risk, and get involved with any strategy that has an IT component.

From a high-level view, Board members want to know whether CISOs have adequate budget and have instituted the most effective measures to mitigate the risk. This can include everything right from adopting best-fit technologies to educating employees about cyber hygiene. When choosing the right cybersecurity solution, enterprises also want to know whether aspects like ransomware, business loss, and legal liabilities are covered in the event of an attack.

Addressing these concerns effectively falls on to the CISO and how effectively they communicate the cybersecurity strategy. For example, regular third-party risk assessments allow enterprises to understand and benchmark themselves against their peers. Companies with access to law enforcement agencies should leverage that relationship and share any cyber intelligence on a quid pro quo basis to stay ahead of imminent threats. From an insider threat standpoint, understanding employee behaviors can help identify disgruntled as well as unsuspecting employees and the potential harm that might be caused by them.

Guidelines for CISOs

Even heavily-regulated industries like financial services and insurance are prone to security attacks. On their part, CISOs must be one step ahead to capture metrics, incident responses, and defense depth in the form of controls. This will instill confidence in the Board that even if an attack were to happen, the organization is equipped to defend and recover from it.

Nonetheless, engaging with the Board on the topic of cybersecurity is challenging. Here is what CISOs can focus on when sharing information with the Board:

- Highlight the current state of the organization, victories achieved, and the risks and threats that might exist
- Report on the work being done to remediate known risks, vulnerabilities, and attacks, improvements made from the last time, and the security roadmap
- Share the strategy to mitigate risk in the event of an attack in case remediation does not work
- Update on how risk is transferred to cyber insurance in case both remediation and mitigation do not work

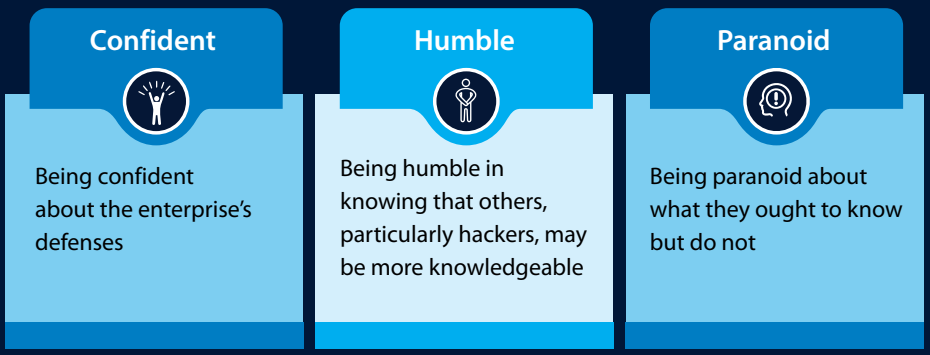
It is vital for CISOs to be well-prepared before conversing with the Board so that the interactions are meaningful, and solutions can be found to pressing concerns. This will instill confidence in both entities.

When conversing with the Board, some guidelines on preparation and communication are:

- Keeping it simple is very important. Refrain from using highly technical language. The use of analogies can help explain complex cybersecurity concepts and technologies in layman's terms for faster comprehension. Using real-life examples also helps ground the risk and impact.
- Leverage an approach of 'incremental messaging'. It ensures that the Board is not overwhelmed with excess information and also helps avoid the pitfall of having to repeat oneself.
- Use metrics, displayed through dashboards, to depict what is going well, what is not, and what needs immediate attention. Some of these KPIs include how the enterprise is blocking threats and how is the state of security improving.
- Board members often think in terms of business impact. Thus, translating how the probability of risk affects business operations is a good way to lead into requests for higher budgets, when necessary. CISOs should also be able to describe risk in probability terms.

Overall, CISOs should focus on establishing a functional relationship with the Board whereby members can communicate directly to the CISO for any concerns or clarifications.

Some key characteristics that will help are:



Conclusion

Building credibility and emphasizing the importance of cybersecurity is an important element of the CISO's role. As cybersecurity gains Boardroom interest, CISOs are tasked with safeguarding enterprise operations. This calls for significant spend and accountability. When communicating with Board members on cybersecurity initiatives, programs, and budgets, CISOs should focus on updating them on the current state of security, what risk looks like, and its business impact. Keeping conversations centered around dashboards that provide a single view into security KPIs, using analogies and real-life examples. Addressing top concerns of Board members in terms of risk coverage can ensure smooth alignment between the CISO and the secured sustained growth of the enterprise.

For more information, contact askus@infosys.com

Infosys®
Navigate your next