Communicate cybersecurity issues to corporate leadership

John Iliadis
Μέλος ΑΛΛΗΛΟΝ
President of the Board of Directors of ISC2 Hellenic Chapter
John Iliadis | LinkedIn

Περίληψη

In today's digital age, effective communication of cybersecurity's importance to corporate leadership is essential but often mishandled. Avoid presenting cybersecurity as a transient trend or relying on fear-based tactics, as these approaches can undermine trust and engagement. Instead, frame cybersecurity as a strategic investment and business enabler. Use clear, jargon-free language, data-driven insights, and align cybersecurity efforts with organizational goals. Demonstrate its role in fostering trust, enabling innovation, and gaining competitive advantage. By positioning cybersecurity as a growth enabler, security leaders can secure executive buy-in and resources while fostering a collaborative approach to navigating digital risks and opportunities.

In today's digital-first world, cybersecurity is critical to the long-term success and resilience of any organization. However, convincing executive leadership of its importance can be an uphill battle. Cybersecurity often struggles for attention against pressing concerns such as revenue growth, market expansion, and competitive advantage.

The reason for the aforementioned disconnect is that sometimes we tend to communicate cybersecurity issues to the corporate leadership, the wrong way. Let's review three often-encountered ways to present cybersecurity issues to the leadership and discuss their effect on the relationship between cybersecurity professionals and corporate leaders.

Cybersecurity as a fad: a no-no

One of the most common pitfalls in discussing cybersecurity with non-technical leadership is the overuse of jargon and buzzwords. Terms like "zero trust" and "endpoint protection" may be familiar to IT and security professionals, but they can be meaningless to business executives.

When security leaders rely on frequently-changing buzzwords to communicate their message, they risk losing their audience's attention. These phrases often obscure the true value of security initiatives, making them seem like fleeting trends rather than essential components of business operations. When cybersecurity is seen as a fad, it's easier for leadership to downplay its importance and delay critical investments. After all, why invest heavily in something that might be outdated tomorrow?

Cybersecurity using FUD: a no-no

Another common approach that cybersecurity professionals sometimes fall back on is the use of Fear, Uncertainty, and Doubt (FUD) to drive home the importance of security initiatives. In this approach, security leaders highlight the catastrophic consequences of potential cybersecurity incidents. They paint vivid pictures of data breaches, regulatory fines, and media scandals, aiming to instill fear and urgency in their audience.

While FUD can be an effective short-term motivator, it often backfires in the long run. Leading with fear can create a culture of anxiety and defensiveness, where risk owners feel perpetually uncertain about their ability to protect the organization. This can stifle innovation and collaboration, as teams become more focused on avoiding failure than pursuing success.

Moreover, executives are often wary of scare tactics. They may recognize the importance of cybersecurity but resist being driven by fear. Over time, FUD-based messaging can lead to skepticism and desensitization—exactly the opposite of what security leaders are trying to achieve. In the end, the perception of security is degraded to that of a burdensome cost center.

Cybersecurity as an Investment Center: *yes, please*!

We should strive to frame cybersecurity as an enabler of innovation and growth, showing how robust cybersecurity can open new markets, build customer trust and enable the adoption of emerging technologies. By shifting the narrative from fear to opportunity, we can foster a more proactive and engaged relationship with the executive team, aligning our efforts with the organization's goals.

Additionally, positioning security as a growth enabler can help shift the conversation from compliance and risk reduction to competitive advantage. In industries where trust and data security are critical, organizations that prioritize cybersecurity can differentiate themselves from competitors. This can be a powerful message for leadership, who are always looking for ways to gain an edge in the marketplace.

This perspective encourages stakeholders to view security as a critical component of their strategic decision-making. Highlighting the positive impact of security measures on the bottom line can transform conversations, making it easier to secure buy-in and resources from leadership. The most successful approach to communicating cybersecurity to leadership is to position it as a strategic investment that drives business growth; it does not happen by magic, neither by accident. There's a 3-part recipe one should follow.

Investment Center Recipe Part 1: Use ingredients (message) that are simple and digestible

To ensure your message is heard and understood, distill complex topics into clear, concise, and relatable language. For instance, instead of discussing "SQL injection vulnerabilities," explain how cybercriminals might exploit system weaknesses to access sensitive customer data.

Effective communication is a critical component; the need arises often to use behavioral economics principles that can enhance the way we convey information. Let's talk about framing as an example. Framing refers to the way information is presented and how this influences perception and decision-making. For instance, instead of saying that the annual cost of a cybersecurity service will increase from €15.000 to €30.000 (tens of thousands of euros), presenting the information as a daily cost increase from €41 to €82 might make the price change seem more manageable and easier to digest.

Investment Center Recipe Part2: Use data-driven insights

Boards rely on data to evaluate risks and make decisions. By presenting metrics and evidence-based insights, you can give board members the tools they need to understand the organization's cybersecurity posture.

Share key indicators such as incident response times, breach costs, or phishing success rates. These figures help quantify risks and demonstrate progress. Presenting data on the cost savings from proactive measures versus the potential losses from breaches can make a compelling case for funding.

Investment Center Recipe Part 3: Align cybersecurity with business goals

Boards are primarily concerned with achieving organizational objectives. Positioning cybersecurity as a strategic enabler of business goals rather than a technical hurdle can drive more engagement and support.

Highlight the role of cybersecurity in fostering trust. Strong cybersecurity practices reassure customers, partners, and stakeholders, building confidence in the organization. Demonstrate how a secure foundation enables the adoption of new technologies and business initiatives without undue risk.

Summing it up

Ultimately, effective communication between cybersecurity leaders and executive teams is about building strong, collaborative relationships. Cybersecurity professionals need to position themselves as trusted advisors who understand the business and can help leadership navigate the complex landscape of digital risks and opportunities.

To do this, security leaders need to focus on three key principles:

1. Speak the business lingo: avoid technical jargon and buzzwords. Frame cybersecurity in terms of business outcomes, such as revenue protection, customer trust, and regulatory compliance.
2. Be a partner, not a gatekeeper: avoid fear-based messaging that creates a culture of anxiety and focus on the positive outcomes of strong cybersecurity as a business enabler.
3. Position cybersecurity as an investment center, rather than a cost center, by using enhanced methods of communication, data-driven insights and by aligning cybersecurity with business goals.

Communicating cybersecurity effectively to leadership is both an art and a science. It requires a deep understanding of the business, a clear vision for the future, and the ability to tell a compelling story that resonates with executives. By moving beyond buzzwords and fear tactics and positioning security as a strategic investment, cybersecurity leaders can help their organizations navigate the challenges and opportunities of the digital age.

JOHN ILIADIS, Ph.D., CISSP, CRISC, C|CISO, is the IT Infrastructure Manager at Bank Information Systems S.A., Greece and also serves as President of the Board of Directors of ISC2 Hellenic Chapter. Opinions expressed herein are solely those of the author and do not necessarily express the views or opinions of any third party or employer.