I Global Intelligence for the CIO

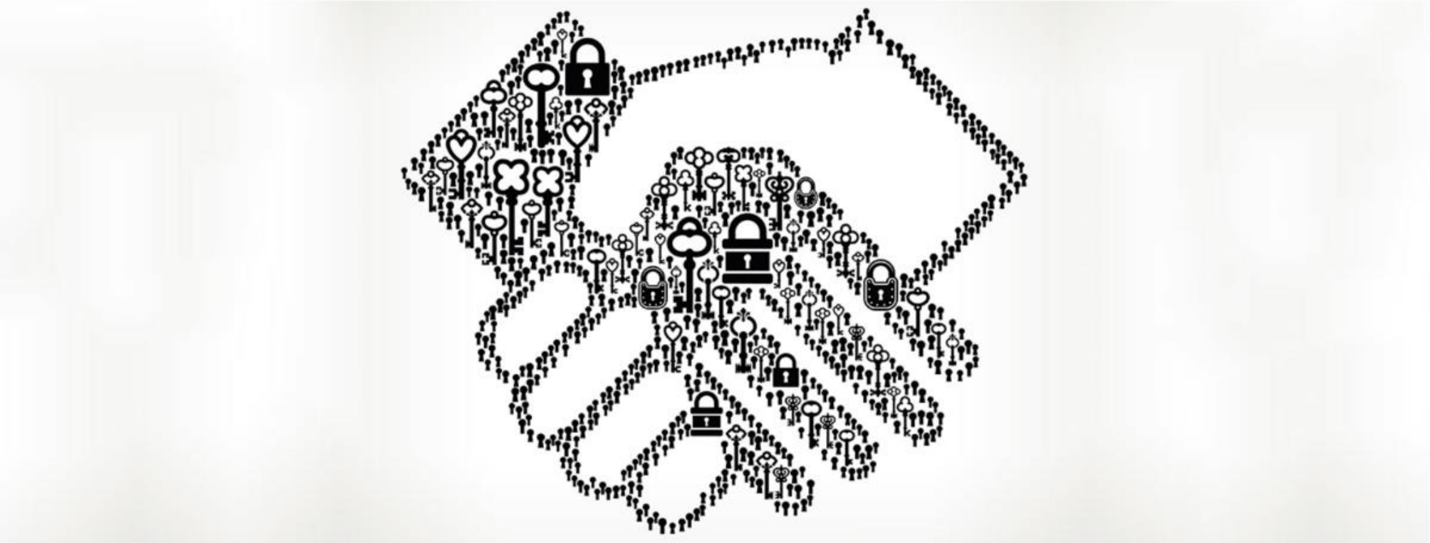

Image: Getty

Share

The changing relationship between the CIO and CISO

Maxine-Laurie Marshall – September 2017

The increased focus on cybersecurity has made CISOs more visible within most organizations. But how has this affected the pivotal relationship between the CIO and the security function?

There are some parts of IT that have always been seen as someone else's job. Communications — helping business colleagues understand what IT does and the value it delivers — is one, says Piergiorgio Grossi, CIO and digital transformation officer at Italian motorcycle-maker Ducati. Another, somewhat paradoxically, is information security.

Often viewed as a distinct discipline, IT security has long had its own communities, language, professional structures and reporting lines. But in recent years, as the scale, frequency and sophistication of security threats have escalated — from simply frustrating to business-threatening events — security has moved to the top of the CIO's agenda and become an IT-wide priority.

"Today, the only way to be sure your system is good enough from a security point of view is for the whole IT team to design everything with security in mind," says Grossi. "It's no longer okay to be only mobile first or cloud first; it's got to be security first."

That means the chief information security officer (CISO) now has a much wider and critical role: "To drive the whole IT team toward a security-by-design approach."

Security-savvy C-suite

This security-first way of thinking has come about because the threat landscape has changed dramatically in recent years. In the annual CIO survey by recruitment company Harvey Nash, a third of IT leaders reported their organization had been subject to a major cyber-attack in the past 24 months. Further to that, only a fifth of respondents feel their organization is currently well positioned to deal with such IT security issues. Such inadequate levels of defense can be costly. According to a report by Juniper Research, over the next five years data breaches alone will cost companies worldwide a cumulative total of $8 trillion in fines, lost business and remediation costs.

It's this evolving environment that is elevating the CISO's place within the C-suite. As Paul Watts, CISO at the UK's Network Rail, says: "Business is coming around to the reality that the impacts of cyber-attacks are no longer just isolated to the business' IT operation but absolutely have the capacity to critically disrupt and damage the very fabric of any data-driven, 21st-century organization — in some cases, permanently."

He continues: "As cybersecurity has become (sometimes grudgingly) acknowledged as a board-level, share-price sensitive, business-killing enterprise risk, it has attracted the interest of board-level executives, including CEOs and CFOs, and these executives are seeking to understand it better, influence it more directly and be seen to be advocates of it."

The increased interest from the C-suite has also led to a change in perception of the CISO; no longer is the head of IT security seen as a blocker of new enterprise initiatives. Grossi says it's up to the CISO to help the IT team provide more robust products and services rather than simply saying 'no.'

And, noting the positive change, Thom Langford, CISO at French marketing communications group Publicis, says: "CISOs are finally doing a better job of articulating value to the business, and changing their modus operandi. No longer are they a blocker to the business or seen as a hurdle for the business to jump over in order to get things done."

Thom Langford, CISO of Publicis

CISO versus CIO

The threat landscape may have propelled the CISO into the limelight but the ultimate responsibility for IT rests with the CIO. Their different priorities — risk mitigation versus the delivery of business value from technology — creates a natural tension between the two roles.

Marc Lueck, chairman at Club CISO, a private members' forum for European information security leaders, alludes to this delicate balance: "In the past there was certainly an often-combative relationship between the CISO and the CIO." But he believes the requirement to work together is bringing the two roles together in a symbiotic way. "As information security has increased in importance, the roles of the CISO and CIO have certainly become more collaborative. Now, both execs tend to be pulling together towards the same goals of accessibility, security and organizational resilience."

They both have a shared responsibility to the business, and Lueck believes the way they convey important information to the organization is a critical part of the working relationship. "It is still usually the CIO's responsibility to advise the board about the state of cybersecurity risk. That translation of security information into board-level understanding is the CIO's most important responsibility for security, and gives the best chance of success. Alongside, the CISO needs to be able to provide information to the rest of the organization in a way that makes it relatable and ultimately actionable. Having a collaborative relationship between these two job functions ensures that there are no chasms in communication from the top to the bottom of the pile."

That importance for communicating information about security to senior management is echoed by Juha Eteläniemi, CIO at Finnish financial management services company OpusCapita. He argues that it is best to frame the conversation around a topic that is easily understood: "For the CISO, the business continuity agenda is often an excellent one to discuss with concerned top management. Business continuity is a lot easier to understand than crypto-technology attacks."

Alexander Bockelmann, CIDO of UNIQA

While adopting board-friendly communication is vital, another important facet is presenting a united front. Alexander Bockelmann, chief information and digital officer at Austrian insurance group UNIQA, says: “Teamwork is key for a successful security strategy. When the CIO and CISO join forces and align on a common agenda and priorities, they have a much stronger position in board discussions and will ultimately be more successful working together. As Network Rail’s Watts emphasizes: “Support each other publicly, argue privately.”

While the relationship between these two technology executives needs to be symbiotic, it is not without its challenges. Publicis’s Langford insists there must be clarity around the scope of responsibility of each role and, critically, accountability. “Accountability needs to be articulated and agreed upon at both an individual and business level. Issues arise when there isn’t that level of clarity,” he says.

But as IT security has become a critical business capability, the reporting line of many CISOs is still up for debate. In the early days of the role, the CISO “would be lucky to report to the CIO,” says Lueck. “More typically, they would be buried in some convoluted reporting structure.”

While Eteläniemi believes the CIO’s office is the most logical place for the CISO to report today some businesses note the importance of CISO impartiality and have removed any direct reporting line to the CIO. Watts explains the thinking: “It enables an ability to call out poor practices within the organization’s IT operations that could be amplifying risks unnecessarily.”

This debate suggests a new reporting structure might be on the horizon. “Security is becoming a strategic aspect of the enterprise, and in a digital world is only growing in importance,” argues UNIQA CIO Bockelmann. “So CISOs should report to the board level.” That is a trend being witnessed by Club CISO’s Lueck: “With the higher public profile of security breaches, and the general increase in threats, there are occasions where CISOs are reporting to the board above the CIO in order to provide their valuable insight in this area — especially during times of crisis.”Does that increased responsibility and visibility mean CISOs should be taking on a larger slice of the IT budget – or even a separate budget? Bockelmann believes the CISO can argue for funds separate to those managed by the CIOs based on compliance and regulatory needs. “The two budgets complement each other but prioritization needs to occur to channel the funds to the respective budgets.”

The hint of budget conflict is carried further by Lueck, who sees some CIOs actively protecting their budgets from CISOs. He explains: “Cybersecurity is generally a massive expense coming out of the CIO’s budget, with little or no obvious link to business goals. And security budgets tend to be very large — and increasing, as the complexity of the threat landscape is ever-expanding.”

However, given the potential impact on both the business — and IT management careers — there is a growing realization among CIOs that such outlay is very necessary, says Lueck. What it comes down to is maintaining a high level of trust between the CIO and CISO. As Watts says: “CIOs are now more interested in engaging with their CISOs as they feel more and more exposed at a board level. When answering such questions as, ‘Are we secure?’ they need the CISO’s support and expertise.”

First published September 2017

Share