ISTARI Perspectives

From Guard to Leader: The Changing Role of the CISO

David Fairman

10 • 2021

Big changes in context propel big shifts in key corporate functions. Consider the chief financial officer. Long ago, when finance was less central to securing and maintaining competitive advantage, the CFO's job was closer to accounting.

It was more technical and operational, with little of the strategic and leadership dimensions that began to define it in the 1980s and have since become a core expectation.

A similar shift is underway in the role of the chief information security officer (CISO).

Digital transformation has gone from buzzword to imperative. Employees, customers and suppliers are rapidly moving to interact online. And while operational streamlining and cost reduction are significant benefits to organisations, the most important driver of transformation is value creation. Once the information generated by a business is digitised, companies can reap enormous rewards from data. Organisations can use data to gain greater customer insights, make better business decisions and gain competitive advantages.

The challenging role of the CISO

In a world where data is a major value-creation asset of organisations, protecting that data from cyberattack — a long-time priority of CISOs — is critical. Cyber risk has become a key agenda item for the executive leadership team and at board meetings. At the same time, however, most business leaders do not perceive the CISO as being part of the C-suite[1]. Instead, many see the role as a technology function that is not core to the business strategy.

Another complication for CISOs arises from related but separate roles. Many companies have a chief digital officer responsible for leading the digital transformation, and a chief data officer, who uses the data generated by digitalisation to gain greater insights and deliver more value. These roles often intersect, causing complexity and friction but also dependencies on each other. As companies accelerate their transformations, they move all things 'digital' and 'data' from their usual home within IT into being recognised as the core value-creation asset of the organisation. Concurrently, these digital and data roles also shift to support the organisation in achieving its strategic business objectives. Amid such complexity, it can be all too easy for CISOs to default to their traditional role as corporate guardians of data.

Reframing the CISO role

In theory, the CISO is already well-positioned to unlock value in enterprises. Cybersecurity teams often have good insight into how organisations operate and where the critical asset of data flows. This can be a source of intelligence. It can support the organisation in confirming that business processes are operating as they believe them to be and identify weaknesses where this is not the case. Companies can use their cybersecurity team to improve operations, build sustainable processes and create a resilient business foundation. CISOs are then no longer acting as a guard: they are creating value.

In such a role, CISOs act less like security professionals and more like senior business executives who focus on security, risk and resilience. They contribute to organisational growth just like any other executive, such as the CFO. In fact, without broader awareness of business value, cybersecurity teams may stifle digital transformations, agility and innovation.

Part of the CISO's redefined role must be to help the cybersecurity and other security teams to reduce risk — but in a frictionless way. Balancing security with ease of doing business requires that information security risks be thoroughly discussed and agreed upon at the highest levels of decision-making. Only then can risk to the organisation be understood, managed within the overall risk appetite, and "owned" collectively by the leadership team. CISOs need to be at the centre of business discussions with the mindset of a business leader, not just as a guard. To achieve this transition, they should focus on building four key qualities.

Skills and qualities of successful CISOs

Collaboration and influence.

Because CISOs need a broad view across the organisation, they should strive to bridge different parts of the business, negotiating between them, finding areas of commonality, and bringing people together to create more value. This requires building trust and working through strategic influence instead of relying on a command-and-control structure.

Toughness.

Difficult conversations are inevitable because it is not always possible to enable everything securely. As a result, the CISO must be comfortable having tough dialogues, driving robust discussions and taking a stand when needed.

Broad, business-focused perspective.

Executing the role successfully requires CISOs to build capability within their own function, and to understand the organisation itself – how value is created and delivered to customers. With this understanding, they will be able to make more informed risk decisions and have more meaningful dialogue with peers and stakeholders. CISOs need to learn the business, not merely the business of security.

Risk-tolerance.

While security people (understandably) would love to remove every risk, there is no such thing as 100% risk elimination. Trade-offs abound, and organisations cope with a broad range of business risks every day. CISOs must be able to understand and articulate the specific risks the organisation may be taking in terms of technology, cyber risk and business value. But they also need to lead the conversation with respect to where that risk falls, what the trade-offs are, and just how much risk the organisation can tolerate.

The role of the CISO is still early in its journey. So it is worth remembering that the modern CFO role took years to evolve as well. As digitisation advances, so will the role of the CISO. Those who want to help their companies grow and become more resilient need to build new skills and capabilities, and shift their mindset: only by moving from guard to leader can CISOs truly deliver the kind of strategic capability that companies require.

About the Author

David Fairman is an experienced CSO/CISO, strategic advisory, investor and coach. He acts as an advisor to ISTARI. David has extensive experience in the global financial services sector.

He has previously held leading cybersecurity roles at National Australia Bank, Royal Bank of Canada, JP Morgan Chase and Royal Bank of Scotland. He is a Professor at Deakin University in Australia.

David was recently featured by The Top 100 Magazine as one of Australia's Top 50 Professionals.

[1] Gallacher, L. A. (2019). Evolving the CISO role to make cybersecurity a competitive advantage. Harvard Business Review Analytics Survey