CFOS: THE NEW GUARDIANS OF CYBER SECURITY

It is well-known that cyber security breaches can impact a corporation's employees, customers, processes, and technology, with IT and finance executives often working together to get systems back online after a cyber-attack. While many aspects of cyber security are rooted in technology, there is a growing need for finance professionals in organizations, especially in middle-market companies, to take ownership of their cyber security program.

Driving the deepening involvement of the finance function is an understanding that a business approach can positively impact cyber risk methodology. Finance executives can add value to an organization's cyber security strategy, focusing on critical areas including risk, compliance, reporting, valuation, business continuity, and ERP.

CONTACTS:

MIKKEL JON LARSEN
Partner, Risk Assurance
Denmark
+45 30 70 43 34
mla@bdo.dk

There are five central areas of the finance executive's engagement in cyber security:

Risk

Risk managers oversee the risk to the organization, its employees, clients, reputation, assets, and the interests of stakeholders. Converging with operational risk, cyber risk has made its way to the desk of the corporate treasurer. She or he becomes a key factor in an effective and holistic cyber risk defense program, evaluating cyber risk exposure and ensuring adequate cyber insurance coverage for non-remediated risks.

Compliance

Far-reaching compliance rules have emerged since the financial crisis, including mandatory breach reporting which is now in effect for both US and European organizations. cyber security compliance oversight naturally engages the Chief Compliance Officer, who is usually located in the finance department. In mid-market companies where roles may be combined, a finance manager could very well find cyber compliance within their purview.

Valuation

On top of the legal, insurance, and technology costs, cyber incidents can cause significant reputational damage. This affects valuation, jeopardizing a company's position in M&A negotiations. The finance manager engaged in deal making can leverage their cyber security knowledge to estimate the value of an organization's cyber defenses, as well as the impact of a breach on the overall company valuation.

Reporting

Audit committees typically interact with CFOs, controllers, and auditors in reviewing and dissecting cyber security reports. A complicating factor is that responsibility for protecting digital assets is distributed over various roles within an organization and even external service providers. In the absence of a dedicated CIO, audit committees benefit from contact with a business owner to assess cyber security. Finance executives are natural cyber owners as they are capable of addressing committees in the language they are most used to: financial terms.

Vendors

Cyber supply chain risks require a coordinated effort to address because they touch sourcing, vendor management, supply chain continuity and quality, transportation security, and many other functions – all of which intersect inside the finance department.

The finance executive in a middle-market company is a business partner who understands and integrates key drivers across business models, generating exponential value. They offer true cyber security defense and resilience by leveraging the legacy ties that the finance role has to risk, assets, sourcing, systems, and people.