Finance directors promoted to cybersecurity custodians

Although many aspects of cybersecurity are rooted in technology, a change in understanding is emerging that cyber risk's historically technological perspective benefits from the business approaches that are native to the finance department.

Finance Directors' specific experience adds great value to an organisation's cybersecurity strategy. They approach cybersecurity from a holistic business angle, integrating risk management, ERP, compliance, reporting, valuation and business continuity.

These are the 5 key levels of finance executives' strategic engagement with cybersecurity:

· Compliance – since the financial crisis, far-reaching compliance rules have emerged. Mandatory breach reporting followed, now affecting both US and European organisations. Cybersecurity compliance oversight naturally engages the chief compliance officer, who is usually located in the finance department. In mid-market companies where roles are combined, it may be the finance manager who finds cyber compliance within his or her remit

· Valuation – on top of legal, insurance and technology costs, cyber incidents cause reputation damage. This affects valuation, jeopardising a company's position in M&A negotiations. The finance manager engaged in deal making will leverage their cybersecurity knowledge to estimate the value of an organisation's cyber defences, as well as the impact of a breach on overall valuation

· Partners and 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

· Risk - risk managers manage the risk to the organisation, 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 defence programme, evaluating cyber risk exposure and ensuring adequate cyber insurance coverage for non-remediated risks

· Reporting - cybersecurity reports are typically jargon-filled reports. Next to this, audit committees typically interact with CFOs, controllers, accountants and auditors. A complicating factor is that responsibility for protecting digital assets is distributed over various roles within an organisation and even external service providers. In the absence of a dedicated CIO, audit committees benefit from contact with a business owner to assess cybersecurity. Finance executives make for natural cyber owners as they are capable of addressing committees in the language they are most used to: financial.

Gregory Garrett, Head of International Cybersecurity, adds: “We are witnessing a budding crisis in the implementation of cybersecurity information governance, risk management and compliance (iGRC) requirements and organisations are facing ever more stringent cybersecurity regulations: it is not surprising that many of them feel overwhelmed. The recruiting, staffing, training and retention of cybersecurity talent is a significant challenge for nearly all companies – and the global shortage of experienced cybersecurity professionals is expected to increase over the next three to five years. It is vital that finance, risk and compliance management professionals in public and private organisations - in particular SMEs - step up and take ownership of the growing financial responsibilities in cybersecurity”.

Cooperation is a cybersecurity cornerstone. Breaches impacting people, processes and technology, IT and finance executives have to work together getting systems back online, but also writing to regulators, investors, filing insurance claims and compensating losses.

The finance executive in today’s mid-market organisations is a business partner who understands and integrates key drivers across business models and client accounts, generating exponential value. This ‘exponential’ CFO provides true cyber defence and resilience by leveraging the legacy ties that his role has to sourcing, systems, people, premises, assets and risk.

BDO’s cybersecurity expertise can be invaluable to organisations in search of reassurance in cyber matters. As a network, the experts in our firms are known for listening carefully and delivering tailored solutions in the form of the right advisory services for any one company.

Note to editors

Service provision within the international BDO network of independent member firms ('the BDO network') is coordinated by Brussels Worldwide Services BVBA, a limited liability company incorporated in Belgium.

Each of BDO International Limited (the governing entity of the BDO network), Brussels Worldwide Services BVBA and the member firms is a separate legal entity and has no liability for another such entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BVBA and/or the member firms of the BDO network.

BDO is the brand name for the BDO network and for each of the BDO member firms.

The fee income of the member firms in the BDO network, including the members of their exclusive alliances, was US$ 7.6 billion in 2016. These public accounting, tax and advisory firms provide professional services in 158 countries, with 67,700 people working out of 1,400 (+1) offices worldwide.

Media contact
Jan Schiettecatte
PR and Communications Manager BDO Global Office

Tel +32 478 845130
Jan.schiettecatte@bdo.global

BDO Global Officenewsroom