Cybersecurity Needs to Be Led From The Top

Benjamin Donnachie, Senior Vice President in the Digital Practice at AlixPartners LLP, explains why the cybersecurity agenda needs to be led from the boardroom.

In our experience executive teams often perceive cybersecurity as a singularly technical rather than broadly commercial matter and therefore leave it to their IT teams to manage. What then follows is a classic bottom-up approach with an emphasis on compliance and 'box-ticking' in which the technology function is left to assess performance against their own strategy, effectively marking their own homework.

While many cyberattacks may subsequently be prevented, and their impacts significantly reduced, organisations all too often have scarce resources that need to be selectively, and strategically, allocated. Quantifying and ranking cyber-risk in terms of the potential financial, reputational, and compliance-related impacts in case of a data confidentiality, availability, or integrity issue empowers a business's leadership to understand the problem and address it like any other business risk. In short, it must be incorporated into the organisation's existing enterprise-wide risk management framework.

It is also essential to carefully map business processes, business assets, and technical assets, making sure to classify them by potential risk level and determining their level of criticality. This is the key connection between cybersecurity and business continuity and allows any investment in cybersecurity to be linked directly to the business's value and the importance of its information.

As senior management's appreciation of the cyber agenda develops, they will need to examine the company's wider risk appetite and identify any trade-offs. Any business processes or assets that demonstrate risk levels above the organisation's thresholds require defined mitigation activities involving an appropriate mix of people, processes, and technology.

Ultimately, it is up to the CEO and the board to define the strategic allocation of 'capital at risk' to mitigate cyber risks. The company can then design a detailed plan and investment - including capital expenditure and operating expenses - in which each cybersecurity investment is prioritised and, crucially, justified by the reduction in business risk thus defining cybersecurity return on investment.

Rather than keeping cybersecurity at arm's length, the c-suite needs to recognise it as a top-down issue that must be managed by a team of key people:

- CEO Clearly outline the policies, processes, and the roles and responsibilities of key stakeholders.
- CRO Provide the risk management perspective as well as appropriate metrics and risk analysis.
- CFO Assist with regulatory requirements and analysis of the economic capital implications and allocations.
- COO Embed the approach into IT operations and HR culture of the company.

Along with Benjamin, we recommend that chief executives establish a quarterly security advisory board that enables executives, risk and IT managers to discuss fundamental security issues, challenge existing protocols, and, crucially, include their business judgements. The agenda should focus on risk, continuous improvement, and the enterprise's overall operating model.

Framing the discussion in terms of commercial and operational risk reduction makes cybersecurity significantly more accessible and understandable to a business's leadership team. It allows investments to be focussed on areas of high risk and the return on those investments to be more easily understood, avoiding the perception that cybersecurity is a burdensome additional cost to the business.

In summary, to build the most effective cybersecurity programme possible, it needs to be grounded in the human component of the business and that begins with the boardroom.

We are grateful to the BCS for the original content in this document, some of which may have been modified to reflect changing news or events.