Principles for Board Governance of Cyber Risk
Case Study: Arvest Bank/ VisibleRisk

MARCH 2021

WORLD ECONOMIC FORUM

This case study offers one example of how boards can understand the economic drivers and impact of cyber risk as recommended in the 2021 report Principles for Board Governance of Cyber Risk

Cybersecurity is recognized as a critical risk factor enterprises wrestle with in the digital economy. In confronting cyber risk, controls-based risk assessments have to this point enabled companies to identify critical programme and technology deficiencies and plan improvements. Where these assessments come up short is in their ability to be widely understood by non-technical stakeholders, such as C-suite executives and boards of directors, which naturally inhibit cyber decision-making processes. More importantly, the output of these assessments fails to align to the assessed company's specific business objectives and corporate strategy.

An evolved cyber risk assessment enables organizations to align its cyber strategy to its business objectives. This alignment requires business leaders to understand the financial impact cyber risk poses to their operations. These assessments must consider costs associated with the disruption of business activities, the costs of recovery for data and/or IP theft, and the legal fees and/or regulatory fines associated with a cyber event. Organizations can then take all of these factors into consideration to establish a risk appetite for losses resulting from cyber events. In turn, organizations can prioritize controls and investments that are inherently designed to reduce the frequency and overall economic impact of cyber risk.

This process, known as cyber risk quantification (CRQ), enables improved decision-making by informing executives whether their businesses should accept risk, implement defenses, or leverage insurance. Companies are further empowered to focus on mitigating cyber risks with the greatest potential for economic impact while utilizing a common, non-technical, financial language for discussing enterprise risk. This process fosters far superior communication by and among security leadership, executive leadership and the company's board of directors.

Shifting to cyber risk quantification

VisibleRisk worked with Arvest Bank, a US regional bank, to support its shift to CRQ. Arvest was proactively managing cyber risk using cyber control frameworks and multiple security assessment products to keep the bank – and its customers – safe. However, Arvest's board of directors and senior management wanted to implement a more risk-based approach to cybersecurity. By focusing on risks that posed the greatest financial threat to the organization, Arvest executives could manage cyber risk within their enterprise risk appetite. Furthermore, Arvest executives wished to better understand which controls and technologies were most effective against their most financially impactful risk scenarios; management sought greater insight into the effectiveness of their cyber risk mitigation, acceptance and transfer strategies. This required cyber risk reports that were standardized, easy to understand and actionable.

Although Arvest leadership had considerable technical information, they wanted to translate this into a financial context, so they could better align their cyber risk strategy with the bank's overall business goals. Arvest's technology team also recognized that translating cyber risk into financial language would help build better business cases for programme improvements while enabling non-technical executives and board directors to better understand the risk exposure.

To address these challenges, Arvest implemented a risk-based methodology. This approach uncovered the economic impact of cyber risk by assigning financial exposure figures to identified risk scenarios. The financial data then enabled the board and senior management to think more strategically about the bank's cyber initiatives.

Utilizing CRQ, Arvest worked with VisibleRisk to measure the frequency and impact of cyber events in the context of its governance, defensive capabilities and threat intelligence. Arvest then began the process to catalog, prioritize and implement the most effective controls for reducing the economic impact of specific risk scenarios. Arvest was also able to communicate about cyber risk clearly in a way that was aligned to business goals and risk appetite. These changes enable the board to be confident in Arvest's ability to keep cyber losses within the risk appetite.

Making better cyber decisions

Arvest Bank's forward-looking investment in cyber risk quantification directly aligns to the World Economic Forum's Principles for Board Governance of Cyber Risk, specifically principle 2 – understanding the economic drivers and impact of cyber risk. Arvest's innovative, risk-based approach to cyber risk management enabled the bank to manage material cyber losses to an appropriate level relative to their enterprise risk appetite. The bank's ability to communicate the economic impact of their cyber risk strategy in clear financial terms to key executives and their board of directors has improved enterprise-wide cybersecurity decision-making processes. In turn, Arvest has elevated cybersecurity as a core business issue and empowered its key executives, from the security team to the board room, to make better cyber decisions.

About VisibleRisk

VisibleRisk's cyber risk rating evaluates the economic impact of cyber risk by examining an organization's security programme, governance and risk management practices. The rating provides a series of reports and metrics that benchmarks a company against relevant peers, based on industry, size, geography and other business factors. The technology-driven platform utilizes proprietary and confidential data collection tools, methodologies and algorithms developed by VisibleRisk to holistically assess an organization. VisibleRisk is backed by two global leaders in related fields: Moody's Corporation, a leading provider of credit ratings, research and risk analysis, and Team8, a prominent cybersecurity-focused company creation platform.