IBM Newsroom

IBM Brings Risk Analytics to Security Decision Making

New Service Translates Security Risk Exposure for Areas Like Cloud, M&A and Remote Work into Financial Terms

CAMBRIDGE, Mass., Sept. 22, 2020 /PRNewswire/ -- IBM (NYSE: IBM) Security today announced a new risk-based service designed to help organizations apply the same analytics used for traditional business decisions to cybersecurity spending priorities. IBM's new Risk Quantification Services creates risk assessments to help clients identify, prioritize and quantify security risk as they weigh decisions such as deploying new technologies, making investments in their business and changing processes.

Chief Information Security Officers (CISOs) are often not the ones ultimately responsible for their organization's cybersecurity spending and policy decisions[1], so it's important that they're equipped with quantitative data to translate cybersecurity challenges into business imperatives for CXOs. The new IBM service provides CISOs with financial data to help them communicate to the C-suite and Board the potential business impact of security vulnerabilities and liabilities on their business, in order to make more informed business decisions regarding cybersecurity.

Identify, Prioritize, Quantify Security Risks

IBM's Risk Quantification Services can quantify risk by calculating the probability of a security event occurring, and the probable loss projection based on expected data loss, operational disruptions and business context. Organizations can also benefit from IBM's risk mitigation recommendations that are based on an analysis of value and impact by comparing their costs and expected risk reduction.

According to a NACD survey, nearly 70% of corporate directors surveyed report that their boards need to strengthen their understanding of the risks and opportunities affecting company performance. IBM Security's Risk Quantification Services aligns security teams and business leaders with:

- **Executive Buy-In** – Using a common language to articulate security risks to CXOs, security executives can align business leaders, C-Suite and the Board on the actions necessary to help mitigate security threats to their organization.
- **Informed Decision-Making** – Security leaders are able to translate risk into dollar amounts to deliver a cost benefit analysis that provides non-security leadership with the possible cost impact of risk, while translating security investments or remediation strategies into a business case and ROI.
- **Strategic View of Risk Management** – By bringing quantified security analytics to the C-Suite, CXOs are able understand security risks in terms of the probability of a security incident occurring, potential reputational damage, regulatory liability and business disruption.

"Security leaders have often struggled to communicate the value of a security investment to business leaders," said Julian Meyrick, Vice President, IBM Security. "Our Risk Quantification Services not only enables security leaders to articulate risks and potential exposure in terms of financial loss, it empowers them to measure the actual efficacy of existing security protocols, based on our analysis of their business environment, assets,

security architecture and the potential threats to their organization."

IBM Security will be applying the FAIR methodology, an open international standard for cyber risk modeling, and is collaborating with RiskLens and its proven quantitative cyber risk management platform to assess in financial terms the potential impact of security risks. IBM Security is establishing the necessary business context for its risk calculation models using the breadth and depth of its security portfolio and consulting services, including its expertise and insights gleaned from responding to security incidents around the globe and unparalleled visibility from IBM X-Force Threat Intelligence as well as IBM's mature understanding of client landscapes.

Applying its deep awareness of client business processes, IBM is developing use cases into risk calculation models to define a business's assets, security threats and the potential effect of a subsequent security incident. Some of the use cases include:

- **Mapping a Secure Journey to Cloud –** Companies have gradually been moving to the cloud for years, with a recent report by Flexera revealing that 59% of businesses surveyed plan on increasing their spending on cloud services amid the pandemic. A risk quantification assessment could help organizations distinguish which workloads to move to the cloud and how, while also recommending proper security controls to put in place based on a cost-benefit impact analysis.

- **Calculating Exposure in Mergers & Acquisitions –** As global M&A volumes are projected to amount to $2.1 trillion in 2020, it's important that organizations venturing into M&A transactions incorporate cyber risk assessment into their due diligence process to verify the valuation of a deal. A recent IBM Institute for Business Value study found that of surveyed businesses that had recently executed a major M&A transaction, 57% performed a cybersecurity assessment only after due diligence was complete. In fact, one in three responding companies experienced a breach that can be directly attributed to M&A activity during integration. Quantifying this potential exposure not only helps organizations proactively mitigate security risks before they turn into active threats, it enables them to assess the issues that might impact the target company's value.

- **Enabling a Zero Trust Remote Work Model –** A recent study conducted by Morning Consult and sponsored by IBM found that 61% of surveyed employees new to working from home that are using their personal computers stated they haven't been provided with tools to properly secure the devices. Now protecting wider, more diverse environments, organizations should proactively operate under the assumption of potential compromise, taking a zero trust approach to security. By defining what poses risk to their business and quantifying the impact, from third-party tools or applications to access controls, organizations are able to understand which risks they need to prioritize mitigating. In other words, assessing security risks, contextualizing them and calculating their business impact can help enable organizations to enforce their zero trust model and strengthen their cybersecurity resiliency as work models adapt to an evolving business landscape.

IBM's Institute for Business Value (IBV) also released a report on Assessing Cyber Risk in M&A. To download the report, visit: http://ibm.co/cyber-risk-mergers-acquisitions

For more information about IBM Security's Risk Quantification Services, visit: https://www.ibm.com/security/services/security-governance/risk-management

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 70 billion security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Press Contact

IBM Security Media Relations
Georgia Prassinos
gprassinos@ibm.com

[1] According to the 2020 Cost of a Data Breach report, sponsored by IBM Security and conducted by the Ponemon Institute, only 27% of respondents stated that the CISO/ CSO was ultimately responsible for their organization's cybersecurity technology and policy decision-making.

SOURCE IBM

---

https://newsroom.ibm.com/2020-09-22-IBM-Brings-Risk-Analytics-to-Security-Decision-Making