Cyber Risk = Business Risk

The Need for Business-Driven Security

The Digital Revolution and the Emergence of New Risks

Business processes have digitalized at an accelerated pace over the past decade. While business executives leveraged this digitalization to enable phenomenal business efficiencies and growth, it also brought a new range of technology risks that need to be understood and managed.

- **The impact of cyber threats is no longer limited to IT**. The potential and the actual damages to the business have increased to the point where they are impacting the bottom line and have become a source of major concern for most business executives and corporate boards.

- **There has been little financial accountability for cybersecurity**. Most often, cybersecurity has been treated as a technical concern and simple business questions such as "Are we doing enough?" or "Are we spending too much or too little?" get unsatisfactory responses or none at all.

- **There is no such thing as perfect security**. It's all about balancing the digital opportunities with the associated risk and achieving a sustainable risk posture.

The Digital Revolution Has Changed How Risk and Security Deliver Value to the Business

The overall governance of cyber risk is undergoing a deep transformation. Board and executives can no longer delegate risk decisions to IT and must 'own' cyber risk. CIROs, CISOs and other risk and security professionals must use the power of cyber risk management to deliver value and influence business decision making

- **Cyber risk = business risk**: as part of their fiduciary responsibility towards shareholders and customers, boards and business executives are expected to incorporate the

organization and running the business

- **Talking the language of business**: risk and security professionals must learn about and communicate the impact that cyber risk has on business outcomes in a language that the business can understand, e.g. dollars and cents
- **The organizational impact**: interestingly, an increasing number of CIROs and CISOs no longer work in IT and are transitioning to the business risk side of the organization

Communicating the Impact Cyber Risk Has on Business Outcomes

Enable Financially Driven Business Decision Making

The effectiveness of CIROs, CISOs and other risk and security professionals as facilitators of business decision making depends on the implementation of a financially-driven, business-aligned approach to managing cyber risk.

- **Beyond FUD**: conducting board and management-level presentations about cyber risk at a technical or qualitative level, often based on FUD (Fear, Uncertainty and Doubt), doesn't allow for objective business analysis or effective decision-making and should become a thing of the past
- **A modern communication approach** will capture and translate the wealth of information that an organization is already collecting, conscious or not, in financial terms that the business can understand and use as a basis for effective decision making

Support Conscious and Explicit Choices About Managing Cyber Risk

Using financial data helps organizations to be proactive in deciding where they want to be on their risk and security investment continuum.

- **Risk posture is a choice**: whether implicit or explicit. Every choice made as part of a risk program or security influences where the organization ends up risk-wise
- **Trade-offs**: an organization can chose to either invest more resources and experience less risk, or to invest less and experience more risk
- **Compliance vs. risk**: most organizations treat this decision as a compliance check-box exercise with little regard to the real risks the organization faces
- **A financially-driven, risk based approach** helps executives understand the business impact of decisions and select the controls that actually help the organization succeed

- **Utilize a common language** that all stakeholders (board of directors, operations and IT) can understand: dollars and cents
- **Help them understand** the organization's exposure to cyber risk in financial terms
- **Provide a decision-making framework** for prioritizing risk mitigation, optimizing security investments and transfering risk

A Standard-Based Cyber Risk Quantification Solution

Go Beyond Qualitative, Compliance-based Approaches

Most organizations do not have common methods in place to quantify and manage cyber risk from the business perspective.

- **IT-centric perspective:** in these cases, boards and business executives rely heavily on IT security professionals to make decisions pertaining to cyber risk
- **Broken communication:** In absence of a common language, the discussions among all stakeholders end up being either overly technical or very generic
- **Qualitative assessments**: in both scenarios, it is difficult to assess the level of cyber risk exposure from the business perspective other than in broad qualitative strokes... or not at all

Some companies have their IT security professionals leverage GRC solutions with the goal of managing risk, but most of their functions are meant to help meet minimum regulatory compliance, not quantify the actual cyber risk associated with key assets and business processes.

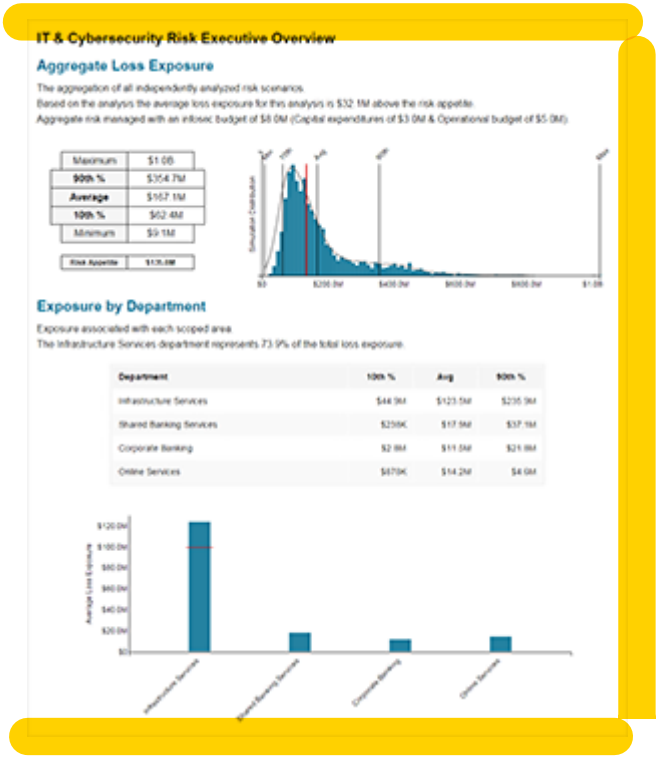
Adopt a Proven Cyber Risk Quantification Approach

Consider RiskLens to quantify the true measure of cyber risk, dramatically improve the communication and the decision-making among all stakeholders and optimize your security investments.

up on FAIR, the only international standard quantitative model for cybersecurity and operational risk

- **Our solutions are purpose-built** to solve the pervasive challenges that exist in merging financial, operational, and IT security data to deliver improved analytics, reduce cyber risk, and sustain business value

Next: Why Choose RiskLens?



RiskLens

+1 (866) 936-0191