Cybersecurity at MIT Sloan
A New Model of Cybersecurity Risk

Cybersecurity at MIT Sloan brings together thought leaders from industry, academia, and government with MIT faculty, researchers, and students to address strategy, management, governance, and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

> ***"Our goal is to use a language that executives and boards understand and can relate to other areas of risk in an organization."***

A New Model of Cybersecurity Risk

CAMS researchers developed a cyber risk cube, designed as a guide for organizations to highlight the six major domains of cyber risk management. The six domains are:

Internal

- All aspects of risk that can be controlled by the organization
- Controlling internal and external-facing cyber risk and security maturity level of the organization

External

- Assessment by external parties of the organization's risk level
- Assessment by the organization of external party risk

Qualitative

- Using ordinal rating scales to plot various risks
- Measure of security maturity level (e.g., FFIEC CAT)

Quantitative

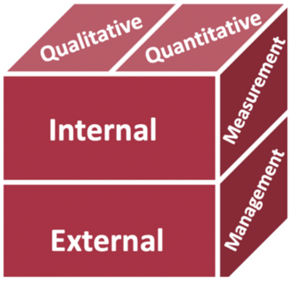
- Measurements using dollars and cents or scalar values (e.g., VAR), rather than an ordinal measures
- Address the prioritization suitable for active management
- Can be real-time

Measurement

- Measured and lightly managed
- Security metrics to measure cyber risk in the organization periodically
- Static management based on measurement

Management

- Managed and measured
- Dynamic management of cyber risk controls. Continuous development of mitigation plans designed to manage, eliminate, or reduce risk to an acceptable level



Right now, the cube is a starting point for conversations about managing cyber risk. The risk cube can help managers begin to answer the questions: Are we prepared for cyber risk? What controls are our peers taking? Where should we start? And What are the key factors for cyber risk management? It can guide organizations to develop a common understanding of cyber risk management, and lends insight into what competitors might be doing, and overall it provides a point of reference for how to tackle the various domains of cyber risk.

How to use the Factors:

Each face of the cube has two domains. On each face of the cube, the organization selects at least one domain from each of the sides. There are eight possible combinations. The cube helps to choose the combination by making recommendations specific to the organization's size, selected industry, rationale for risk management, budget, and other factors. After determining the recommendations, managers have a roadmap for articulating risk management. For example, for a large company depending on yearly audits, the tool factored in their size and suggested using a score card to determine their risk level internally. For companies that don't know where to start, this will provide an idea of the appropriate tools for their organization.

IMPACT: For internal communications, the risk cube is designed to work as a guide for cyber teams to use to formulate or describe their risk management approach and compare that approach with others.

About Cybersecurity at MIT Sloan

Cybersecurity at MIT Sloan brings together thought leaders from industry, academia, and government with MIT faculty, researchers and students to address strategy, management, governance and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

For more information, visit https://cams.mit.edu