



Bridging Transformation Enterprise - Wide

CITIE
Cambridge Technology Enterprises

An Approach to Understanding IT's Business Risk

There are many providers of security products, assessment services, and training that follow standard security best practices. These types of activities are necessary to reduce the risks related to information technologies. However, improving the quality of risk management requires improvement the quality of the decisions that can be made surrounding the trade-offs between technologies and operations. Risk management is performed to enable business; to be effective any solution that is developed will need to focus on supporting the business needs and goals of the organization. Ultimately, the best solution for the management of IT security and operational risks will include the integration of best of breed elements of technology and processes from several vendors along with the culture and goals of a client. We recommend starting with a common vision for IT risk management. With this vision, a roadmap can be created to pull together best of breed technical solutions and security expertise for the iterative creation of a system that provides effective and actionable risk management information for the firm.

Ari J Salonen, PhD

Chief Strategy Officer and Sr. Vice President, Partnerships

IT Risk Management

In order to make relevant decisions, business managers need to be provided with information that is relevant to their operations, not to their IT departments' operations. Managers need answers to questions such as "what losses am I risking?" not "what is the uptime of my servers?" Existing security dashboards and metrics do not do a good job of transforming technical data into information upon which one can make business decisions. For instance if a vulnerability is discovered or suspected in a web application, consider how to answer the following questions:

- ➔ Under what conditions should risk be borne in order to sustain operations?
- ➔ What would the cost be to the organization if the vulnerability was exploited?
- ➔ How much should a firm be willing to pay to insure against or avoid this risk?
- ➔ What is the optimal bundle of risks for the firm to take, given the impact of capabilities and constraints on business operations?

There are real challenges to managing IT security risks and providing answers to these questions. Attempts to manage such risks are hampered by the lack of statistically representative information and difficulty in determining the effectiveness of security that is in-place. Metrics involve costs that can be difficult to determine, such as the costs of private information becoming public, the loss of customer confidence in the privacy of their dealings with the firm, etc. The result is uncertainty both in the appropriate type and size of security investments as well as in the level of exposure of the firm.

The development of new types of metrics can provide this type of business decision support. The answers to all of these questions will result from considering a combination of technical data provided by IT, operational data provided by the line of business, and applying relevant risks models. The combination of security and operational risk data enable a holistic view of risk management across the firm. Finally, the key questions of how much money should be spent to mitigate risks, and where it should be applied can be determined by applying scenario analysis to such a dashboard system.

Risk Metrics

This uncertainty surrounding measuring IT security risks is beginning to be addressed. The economics of security is now a topic of research and conferences, and economic models are under development to understand the behaviors and returns involved. Security firms such as @stake Inc. have created proprietary databases on the types and frequencies with which security vulnerabilities exist within applications. In addition, they are creating metrics to describe the severity of vulnerabilities, such as Business-Adjusted Risk that incorporate the impact on operations and the risk of exploit. Activities such as this, along with collection efforts from the Computer Security Institute, CERT at Carnegie Mellon University, and others have now compiled sufficient data for useful analysis.

Like measures of financial risk, such as Value at Risk (VAR), these risk metrics will have components based on historical data and firm experience, public sources of information, as well as probabilistic estimates based on best available data. Only recently has enough data been accumulated that such metrics can begin to be developed, and the key to effectiveness depends on the details of the firm's infrastructure and operations. This is a trend that is going to have a real impact on the management of IT risks. The Basel II accords have already begun to consider the impact of operational risk on financial institutions. Firms that can demonstrate proper measurement of their operational risk may benefit from reduced reserve requirements, or gain other competitive benefits. As with financial risk measures, managing IT and security risks will have increasing importance from both a regulatory and profitability standpoint. A brief description of predictive metrics we developed for the utility JEA in order to identify power outages can be found in Appendix.

Getting Started: Setting a Common Direction

We always start from a common direction for risk management, based on the goals of the client. This vision must be based on consensus between business users and IT managers, and this approach must be tangible and communicable throughout the firm.

Historically, however, it has been very difficult for organizations to have a common vision where strategy and technology initiatives complement each other. It is very typical for a large organization to have disparate groups and leaders in charge of their business and technology strategy. The end result is inefficient alignment of internal forces that in the long term inhibit the growth of any organization and the success of any given initiative. Business leaders end up wanting systems that IT departments are not able to deliver on time and budget, while IT departments spend precious time and resources on systems that are not accepted by business leaders.

To address the risk issue specifically, some companies have formed separate organizations for risk management, including IT risk management. Counterintuitively, this approach often results in further fragmentation and lack of ownership of IT risk issues.

To support such early development of shared tangible direction across organizational silos, Cambridge Technology Enterprises (CTE) typically uses various kinds of workshops. The objective of these workshops is to create a common vision for the goals of an IT risk management effort, identify key processes and systems, and develop a plan to achieve quick measurable results. The workshops also secure visibility to and buy-in from senior business leadership.

Typical End Product - Risk Management Dashboard

The information needs of the business are unlikely to be met with available off-the-shelf solutions, because the information and risk related decisions are all unique to the business lines. Therefore, the workshops have been designed to generate a shared understanding of a system to support the IT risk management goals. The key functionality of such a system includes collecting, consolidating, correlating, and providing information, predictive metrics, and key risk indicators to improve risk management decision making. To the end user, the system is accessible as a dashboard that is customized to his or her needs.

CTE has been successful at bringing together IT and business stakeholders to develop unique capabilities for the provisioning of real-time actionable information. Appendix shows an example of a dashboard designed for the USAF that provides actionable information on mission capabilities based on the uncertainty and risk of the underlying structure, including IT.

APPENDIX A - Predictive Indicators for the Jacksonville Electric Authority Jacksonville Electric Authority

JEA is an integrated supplier of Electricity, Gas, and Water services, and is the 4th largest municipal utility system in the United States. They manage a number of infrastructure projects, and spend over \$600 million annually on their portfolio of capital projects.

JEA needed a way to improve the quality of the delivery service by reducing the frequency and duration of power outages. CTE developed the Outage Trending Information System (OTIS) to provide these predictive indicators of outages, while simultaneously collecting and providing access to a variety of information on their distribution system.

JEA needed a way to reduce the frequency of power outages

- ➔ No easy way to see information on distribution equipment
- ➔ No single picture of complex system
- ➔ Difficult to identify failure points of system

An Approach to Understanding IT's Business Risk

Solution provided predictive indicators through outage trending dashboard

- ➔ Correlation of data from disparate sources
- ➔ Root cause identification
- ➔ Trending information

Results are reduced outages and improved service quality

- ➔ Reduction of outages through targeted maintenance at likely points of failure
- ➔ Increased visibility into the performance of system components, enabling improved purchasing and system development



Results provide a common view of capabilities

- ➔ Faster, better, and more accurate decision-making and tactical response
- ➔ Ability to link strategic decisions to trends based on real-time information, reducing the length of the strategic planning cycle



Transforming Data into Mission Capability for the United States Air Force

The United States Air Force Installation and Logistics Group (ILG) is the integrator of installations and logistics management in the Air Force. It supports 22 functional areas (e.g., securing fuels, vehicles and equipment to all of the air force bases. ILG is also responsible for the Combat Support Center (CSC), which reports on the status of forward operating locations, (i.e., any domain where Air Force personnel or equipment are deployed).

Combat Support Center has difficulty in reporting on capabilities

- ➔ Manual methods used in collection, compilation, and reporting of data
- ➔ Trends cannot be established at either a granular level or a rolled up view
- ➔ Clear accounting for resources but difficult to report mission capabilities

Expeditionary Support Solution enables understanding of capabilities

- ➔ Single source for consolidated logistics information
- ➔ Macroscopic and granular views into resource availability
- ➔ Correlating multiple data points to provide information on mission capabilities