

Mastering the Risk/Reward Equation: Optimizing Information Risks to Maximize Business Innovation Rewards: Synopsis

Recommendations from Global 1000 Executives

Report based on discussions with the "Security for Business Innovation Council"

- **Anish Bhimani**
Chief Information Risk Officer,
JPMorgan Chase
- **Bill Boni**
Former Corporate Vice President,
Information Security and Protection, Motorola
- **Roland Cloutier**
Vice President, Chief Security Officer,
EMC Corporation
- **Dave Cullinane**
Vice President and Chief Information Security
Officer, eBay Marketplaces
- **Professor Paul Dorey**
Founder and Director, CSO Confidential; and
Former Chief Information Security Officer, BP
- **Renee Guttman**
Vice President, Information Security and
Privacy Officer, Time Warner
- **David Kent**
Vice President, Global Risk and Business
Resources, Genzyme
- **Dr. Claudia Natanson**
Chief Information Security Officer, Diageo
- **Craig Shumard**
Chief Information Security Officer,
Cigna Corporation
- **Andreas Wuchner**
Director IT Security & Risk, Deutsche Bank

This synopsis is a small teaser of the wealth of information provided by the Council. For a deeper dive, please view the full report at www.rsa.com/securityforinnovation.

Optimizing Risk

As enterprises implement new technologies and global business models to create value, the right frame of mind when it comes to enabling these business innovation initiatives is to optimize rather than mitigate risks. If you take away all risk, you take away all reward. Optimizing risk is about using risk-taking to its best advantage to help drive the business forward with new and innovative ventures. The enterprise must determine the magnitude of risk that it is willing to take and establish its risk appetite. It is not only the informational risks that need to be considered; organizations worldwide are currently striving for a more consolidated view of all of the risks they face. As enterprises begin to look at risk management more holistically, the processes for assessing information risks must be integrated into the overall risk assessment efforts.

What is the Risk/Reward Equation?

The risk/reward equation factors in many different variables to arrive at a solution. It considers factors such as the type and sensitivity of information; how it is being stored, processed or transmitted; the threats and vulnerabilities it faces; and the necessary protection requirements to keep it secure. The focus of the equation is to determine the appropriate level of controls to put in place given a pre-determined acceptable level of risk. Ideally, the calculation should be based on hard numbers.

Business Innovation Defined:

Enterprise strategies to enter new markets, launch new products or services, create new business models, establish new channels or partnerships, or achieve operational transformation.

As an illustration, in a perfect world an information security professional might be able to say something like, "This new business initiative is worth \$100 million to the business (in savings or revenue, etc.) and there is a 10% chance that this particular detrimental event will happen; if it does, it will cost the business \$250 million (in fines, direct incident costs, lost customers, etc.). The recommended security controls would cost \$500,000, which would reduce the chance of that event occurring to 5% and the impact to \$30 million, which is in line with the acceptable level of risk for this project.

However, with a lack of "actuarial" data, it may not be possible to always have those hard numbers to work with. Instead, security teams may use "high/medium/low" risk definitions or numerical scales that assign risk scores to qualitative measures in order to describe probabilities and impact. Whatever method is used, the key is that security and business executives all understand what the scores mean.

Moving from "Information Security" to "Information Risk Management"

A key component of building a security program that enables innovation is moving from the concept of "information security" to "information risk management" (IRM). This is because the goal ultimately is to match risk exposure to risk appetite, not to wipe out all risk. A risk-based approach shifts the perspective of security from an IT specialty to a business advisory and consulting function that is meaningful and enabling to the business.

Creating a Step-By-Step Process For Making a Risk/Reward Calculation:

Among many organizations there seems to be a common, emerging step-by-step process for making a risk/reward calculation for new business initiatives. Most companies do not yet have this entire process in place, but many are well on their way to formalizing a similar approach. While not all of the prescribed steps in this process are suitable for every company, they serve as a useful resource to consider:

1. New initiative proposed
2. Reward calculation
 - 3a. Risk calculation Part 1: "first pass" is done by business in a "self service" model
 - 3b. Risk calculation Part 2: if risk is relatively high, the security team does further analysis
4. Security controls determined and implemented: either standard or custom solution
5. Escalation and dispute resolution

For a detailed explanation of this step-by-step process please see the full report at www.rsa.com/securityforinnovation.

"Risk/reward decisions are business decisions. Not security decisions. So the business has to be involved and there have to be baseline policies in place that follow a standardized way to make the determination."

Roland Cloutier
Vice President, Chief Security Officer
EMC Corporation

Determining Risk Appetite

Since the goal of information risk management is to manage risks to an acceptable level, you have to be able to figure out what acceptable looks like. Risk appetite is very organization-specific and is driven by a myriad of different factors such as vertical industry, size, culture and regulatory regime. Furthermore, an enterprise's risk appetite will likely change over time and may even vary between business units. Although some organizations allow their business units to have some latitude in determining their risk appetite, the ultimate objective is to have a consistent decision-making process and interpretation of risks across the enterprise. The enterprise's risk appetite is rarely clearly spelled out for you and so you will have to go to several different sources to determine it. These sources can include statements by the board of directors (BOD) or leadership; conversations with the BOD, leadership, business unit leaders and other business executives; input from the Executive Risk Council (if it exists); as well as "situational analysis."

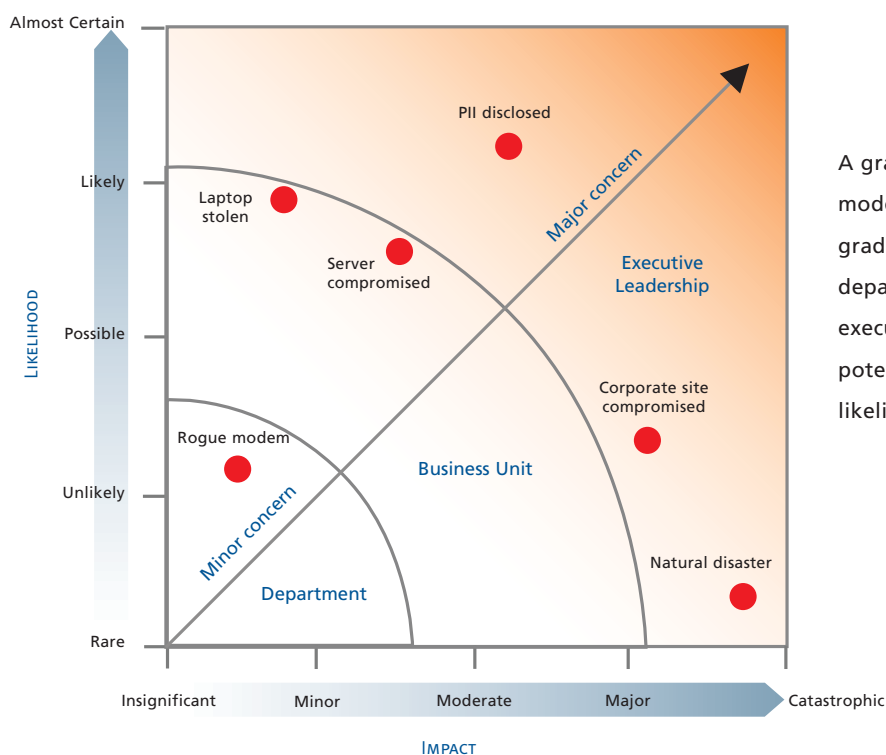
Information Risk Management is...

"Identifying and measuring the risks to information* and ensuring that the security controls implemented keep those risks at an acceptable level to protect and enable the business"

*Includes the systems, applications, networks and infrastructure that processes, stores and transmits that information

Building a Risk Assumption Model

Conversations about risk invariably come down to who has the authority to make what level of risk decision. Having a formalized risk assumption model helps to bring clarity and transparency to the process and delineates where and with whom risk-decision responsibilities lie. Understanding risk ownership is key because although risk is owned by the business, its leadership may not yet completely understand all of the risks or recognize that they own them. A formalized risk assumption model clarifies risk ownership by mapping the different magnitudes of risk to different authority levels within a company while delineating who can make each kind of risk decision. It also establishes the level of risk that each leader may assume.



A graphic representation of a risk assumption model might look something like this: various grades of risk decision authority – from department to business unit to enterprise executive leadership – are mapped to several potential security events, which have certain likelihood and impact.



Making it Sustainable: Governance

To effectively manage information risks on an ongoing basis, a governance structure must be in place. This will ensure that the effort is sustainable. Information risk management should be built into business strategy and processes, and risk decisions should be based on a well understood and defined methodology. The approach and level of formalization of the governance structure will depend on the maturity of information risk management (IRM) within the enterprise. The full report provides a "Maturity Framework" that synthesizes Council member experiences and presents a progression towards an IRM process for enabling business innovation.

An "Enterprise Risk Committee (ERC)" should govern the overall risk/reward calculation process. The name, structure and level of formality of this committee will vary between organizations, but generally it provides oversight to the management of risk within the enterprise and ensures that the risk/reward calculations happen consistently throughout the organization. It should be a cross-organizational and cross-functional team consisting of the most senior executives from various enterprise functions as well as business unit executives.

"Security is nothing special. It's not different than other business processes or risk management approaches. It integrates with and ties to and involves a lot of the same people that other types of risk management conversations involve."

Julia Allen
Senior Researcher, CERT, Software Engineering
Institute (SEI), Carnegie Mellon University

The Security for Business Innovation Initiative

Business innovation has reached the top of the agenda at most enterprises, as the C-suite strives to harness the power of globalization and technology to create new value and efficiencies. Yet, although business innovation is powered by information, protecting information is typically not considered strategic and information security is often an afterthought. Without the right security strategy, business innovation could easily be stifled or put the organization at great risk. At RSA, we believe that if security teams are true partners in the business innovation process, they can help their organizations achieve unprecedented results. This is why RSA is working with some of the top security leaders in the world to drive an industry conversation to identify a way forward. We have convened a group of highly successful security executives from Global 1000 enterprises in a variety of industries which we call the "Security for Business Innovation Council." We are publishing their ideas in a series of reports and sponsoring independent research that explores this topic. RSA invites you to be part of the conversation. To learn more about the initiative and the Council members, and to read the full reports, please visit www.rsa.com/securityforinnovation.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

RSA and RSA Security are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2008 RSA Security Inc. All rights reserved.

CISO2_SYN_0708