



The Security Division of EMC

Solution Advisory

# Information Risk Management



# Information Risk Management: A Practical Approach for Enabling Business Innovation and Managing Information Risk

Across the information security industry, there has been extensive discussion about the potential of information risk management strategies to enable business innovation and address the failures of today's "silo" security solutions. While much of the talk has been theoretical, RSA, the Security Division of EMC, has been pushing forward to develop a pragmatic and actionable approach to information risk management – an approach that is based on leadership thinking and underpinned by proven technologies.

This Solution Advisory describes the landscape that CISOs face today and outlines some key steps they can take to start implementing a risk-oriented approach to security within their own organizations. The paper profiles how RSA is incorporating risk management into the security and compliance solutions it offers to customers. Lastly, a "mini-case" describes how EMC Corporation is implementing these very same strategies and technologies to enable business innovation while reducing the company's information risk worldwide.

---

## Contents

---

The vision: To make security a full partner in innovation	page 1
Turning a stereotype on its head	page 1
Adopting a new mindset	page 2
Speaking the language of business risk	page 2
Security should be built in, not bolted on	page 3
RSA's Strategy for Information Risk Management	page 3
Risk doesn't go away – it just moves elsewhere	page 3
A Case Study Close to Home	page 7
It starts with a commitment at the top	page 7
Acquisitions: Protecting intellectual property	page 7
Partnerships: Trust but verify	page 8
Looking ahead: A dashboard view of risk, security and compliance	page 8
About EMC and RSA	page 8

## Risk aversion

In an IDC survey, 80% of business, IT and security executives surveyed admitted that their organizations have shied away from business innovation opportunities because of information security concerns.

Business innovation is now a top-level concern at most enterprises, driven by a fiercely competitive global environment. Today's most innovative business models target global markets and tap global resources, driving increased demand for technology that enables the secure and seamless flow of information. Secure technology allows companies to reach out, beyond the traditional walls of the enterprise, to foster open collaboration, direct interaction with customers, tighter integration with partners, and access to external talent and resources.

Regrettably, most IT infrastructures and even some security technologies were not built to support such a high level of openness. Inherent security weaknesses in hardware, software and policies prevent IT from saying "yes" to business innovation because the risk is too high. As a result, information security is not seen as being integral to business innovation. When entering new markets, building new channels, creating new sourcing models or delivering new products, the security team is often brought in only at the end of the process to "bolt on" the controls. Too often, the result is the worst of two worlds: high costs for security, coupled with ineffective protection.

---

### The vision: To make security a full partner in innovation

---

Now there is a growing movement among IT security leaders to make security a full partner at the innovation table. Many security professionals already recognize the need to better align security with the business, but often they struggle to translate this understanding into concrete plans of action. RSA is helping to drive the conversation by creating the Security for Business Innovation Council (SBIC), which is comprised of 10 highly successful security executives at Global 1000 enterprises. These leaders have agreed to share their ideas about the future of information security with RSA and its customers over the coming months.

As discussed in the council's first report<sup>1</sup>, the security function has traditionally been viewed as a barrier to business innovation and growth. In an IDC survey conducted for RSA, 80% of business, IT and security executives surveyed admitted that their organizations have shied away from business innovation opportunities because of information security concerns.

Council member Bill Boni, who is Corporate Vice President, Information Security and Protection for Motorola, describes the status quo in this way: "In most global organizations security is viewed at best as a necessary friction. This derives from security's focus on attempting to constrain behavior to prevent negative events. Although well-intentioned, the inevitable result is that security practitioners are not viewed as enablers of innovation but people preventing the business from doing what it needs to do."

#### Turning a stereotype on its head

Fortunately, there is growing momentum to "turn this stereotype on its head," as RSA President Art Coviello put it in his keynote address at RSA Conference 2008. Stressing the need to transform information security from an inhibitor to an accelerator of innovation and growth, Coviello noted, "The idea that we need to implement security not reactively, but holistically, commensurate with risk, is gaining traction."

The concept of information risk management is central to this new vision for security. In the study Information Risk Management in Financial Services, Tower Group Senior Analyst Rodney Nelsestuen wrote, "Practicing a holistic approach to security and information risk assures that business information contributes to achieving marketplace and business goals.... Information security policy, practices, and technologies that provide a defense for information also can support the business's offensive strategy."

---

<sup>1</sup> *The Time is Now: Making Information Security Strategic to Business Innovation*

## Risks worth taking

“There are some risks you want to take because the payoff is so great,” says Bob Blakely of Burton Group. “The challenge is to mitigate your risk to an acceptable level. A mature risk management program allows you to take risks that your competitors can’t.”

Bob Blakely of the Burton Group says there is a “process of enlightenment” that organizations need to go through to make the transition to a risk-based security model. “This process starts with understanding that risks have to be consciously managed and processes have to be put in place to assess an organization’s risk appetite, current risks, threats and vulnerabilities. You then need to design controls that mitigate risk within one’s appetite. And you have to assess the effectiveness of those controls to be sure you’re operating within your tolerance while also achieving regulatory compliance.”

Blakely adds, “Many people think risk management is just about risk mitigation, and it’s not. It’s about risk optimization. There are some risks you want to take because the payoff is so great; the challenge is to mitigate your risk to an acceptable level. A mature risk management program allows you to take risks that your competitors can’t.”

### Adopting a new mindset

CISOs who are serious about aligning security with the business may need to develop a different mindset – and learn to speak the language of business innovation and business risk – and they need to be strong advocates for making security an integral part of the business innovation model.

Motorola’s Bill Boni advises CISOs to “be focused on what’s important to the organization. What’s the lifeblood of the organization? Intellectual property? Cash flow? If it’s a governmental agency, it’s the public’s trust. Focus on what puts the important things at risk.” Dave Cullinane, Vice President and Chief Information Security Officer for eBay Marketplaces, and also a member of the SBIC concurs. “Be

active in the business discussions,” says Cullinane. “So when they’re opening a new business, doing an M&A, starting a new initiative, you can see the potential risk implications of that and what investments might be needed to protect your assets.”

### Speaking the language of business risk

It’s also important to understand how the company already defines and measures business risk, and use that accepted yardstick – rather than adopting security nomenclature – as you begin to quantify information risk. Gain a good understanding of the company’s overall appetite for risk and what kinds of risk different lines of business are willing to assume. For example, disruption in business continuity may pose a huge risk for manufacturing operations while data leakage is the top concern in finance or mergers and acquisitions. Within this larger context, create a risk assumption model for information risk management and get input and agreement from business and executive leadership. This will help guide decisions about risk-taking.

A risk assumption model should address the following elements:

- *Vulnerability*: Where are you exposed to information risk?
- *Threats*: What threats can exploit the vulnerabilities?
- *Probability*: How likely is it that a particular type of threat will occur, especially relative to other threats?
- *Countermeasures/Controls*: What controls are in place to protect against the threats and vulnerabilities? Do I need more controls?
- *Materiality*: What is the impact to my organization should we suffer and exposure?

### Security should be built in, not bolted on

So you don't need to reinvent the wheel for every initiative, it's important to get security built into existing corporate systems for proposing, reviewing and approving business initiatives. Start by insisting that your vendors embed security into their products and solutions, sparing you the time, cost, and complexity of bolting on niche products to compensate for inherent vulnerabilities. Internally, focus on creating fast, flexible yet consistent processes that help accelerate projects, not hold them up. As Cigna Corporation CISO Craig Shumard – also a council member – notes, “When you're not involved early on, it [security] is going to cost more money. It could potentially either delay a project or even stop a project...If you do things the right way and have security built into the process that really enables business to be innovative and move faster.”

---

### RSA's Strategy for Information Risk Management

---

RSA has argued strongly that, for security to truly drive innovation, a more holistic and risk-oriented approach to protecting the information infrastructure is required. Behind this belief is the realization that today's “silo” approaches to security are ineffective in the face of increasingly sophisticated threats. Enterprises face a crimeware ecosystem that perversely mirrors the business world in its inventiveness, adaptability and professionalization. Just like legitimate businesses, cyber criminals make risk-reward calculations and develop go-to-market strategies designed

to maximize their return on investment while minimizing their risk of being detected or apprehended. They're prolific too: according to an April 2008 threat report from Symantec, more malware is being developed today than legitimate software.

### Risk doesn't go away – it just moves elsewhere

When confronted with effective security measures, cyber-criminals often move on, probing for a more vulnerable point of entry to the same target. Their progress is abetted by point solutions that protect components of the infrastructure – laptops, mobile devices, file servers, storage devices, applications, and so forth – rather than directly protecting the data itself. This patchwork approach is expensive, hard to manage and still leaves countless vulnerabilities, which can be exploited by a determined attacker or lead to inadvertent security lapses by well-meaning employees. Additionally, strong security efforts in one silo can be quickly nullified by failures in another. When the end game is to protect the information, why make one silo impenetrable and leave another exposed? On the other hand, why use a sledgehammer when pushing in a tack? The goal should be to apply only the controls necessary to remediate the risk to acceptable levels.

In the face of these challenges, RSA is systematically incorporating a risk orientation into our own solution portfolio via a global risk framework that ties together people, processes and technology to help organizations assess and manage information risk. There are three pillars to the RSA strategy.

### A simple definition

The ISO/IEC 27005:2008 standard defines information security risk as the “potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization...It is measured in terms of a combination of the likelihood of an event and its consequence.”

## Risk management advice from top security executives

Based on in-depth interviews with senior security executives, the Security for Business Innovation Council report provides a conceptual framework, actionable recommendations, and a maturity model for developing an information risk management strategy and program.

### 1. Develop an information-centric view of critical information assets

An effective strategy starts with understanding the information itself and recognizing those points across the organization where it is most vulnerable. What types of information hold the most value to the business and therefore carry the most risk? Where does it reside within the infrastructure? What risks is it vulnerable to? Need further prioritization? Identify key business initiatives and the IT projects aligned with them. What high-risk information is central to those projects?

Aided by data discovery tools, like those incorporated in the RSA Tablus solution, you can now follow the information and see where it exists in production systems, is stored on disk, and backed up to disk and tape. Keep following it and see where privileged users connect to those systems remotely and make copies that are stored on laptops or e-mailed to colleagues and the user's own personal email addresses. Follow it still and see how it gets replicated for marketing analysis and application development and testing.

This process reveals the degree to which information sprawls across the enterprise and propagates into nooks and crannies you've never even considered. Following the information also provides you with a holistic view of information risk so you can determine which of the "6 bad things" and the "3 root causes" shown in Table 1 need to be addressed across the "4 IT domains". Furthermore, RSA has

found that data discovery is a powerful tool for persuading skeptical business management of just how exposed their critical data may be and how urgent is the need for them to take corrective action.

### 2. Prioritize investments based on risk

The second core concept behind RSA's strategy is the idea that security investments should be prioritized, based on an assessment of the amount of risk a given activity entails relative to the potential business reward. In today's resource-constrained environments, this makes perfect sense. Yet security investments are often reactive in nature and focused on solving isolated security issues. This results in over-scoping and misaligned investment in security. A phrase we use is that "many companies are putting locks on doors that almost no one is walking through," leaving less funding available for more urgent needs.

Even for organizations that embrace the value of a risk-based approach, measuring information risk is not yet a well-defined discipline, and many IT leaders wrestle with the challenge. RSA offers an excellent resource for learning how CISOs at some of the world's largest companies are approaching that challenge. The Security for Business Innovation Council's report, *The Risk/Reward Equation: Optimizing Information Risks While Maximizing Business Innovation Rewards* is available at [www.rsa.com/securityforinnovation](http://www.rsa.com/securityforinnovation).

Based on in-depth interviews with senior security executives, the report provides a conceptual framework, actionable recommendations, and a maturity model for developing an information risk management strategy and program. Areas of focus include:

- Engaging the support and involvement of executive leadership
- Building a risk assumption model to guide risk analysis and decision-making across the enterprise
- Creating formal and repeatable processes for making risk/reward calculations
- Developing a governance structure that integrates information risk management into overall enterprise risk management.

As one plain-speaking CISO put it, “I don’t think it’s appropriate for people who are not in senior positions to potentially make risk decisions that could sink the entire

ship. You’ve got to have some kind of process for identifying high, medium or low risks, determining what the impact would be...and then figuring out what the right level of acceptance is.”

Addressing this same point, the report notes, “Conversations about risk invariably come to who has the authority to make what level of risk decision. Having a formalized risk assumption model for information risks brings clarity and transparency to the process.... Relatively mature programs will have established a framework that maps risk decision-making authority to levels of hierarchy or roles within the company...delineating who can make each kind of risk decision.”

### Qualitative Measures of Reputation Impact

Level	Example description
1	Local print media coverage only
2	Local print and televised media coverage
3	Regional print and televised media coverage
4	National print and televised media coverage; ‘front page’ national news
5	Global print and media coverage; ‘front page’ global news

To arrive at an estimate of the risk associated with a particular security event, an organization must take into account the likelihood of an event occurring, weighed against the severity of the various impacts that event would have on the business. (See the chart below.) Those impacts can be financial, operational or regulatory in nature, and each must be quantified. The table to the left provides a scale for measuring the impact of an event, such as a data breach, to an organization’s reputation.

### How Does an Organization Measure Risk?

Likelihood of occurrence	Impact Severity					
	Insignificant	Minor	Significant	Damaging	Serious	Critical
Negligible	Low	Low	Low	Low	Low	Low
Very low	Low	Low	Low	Low	Moderate	Moderate
Low	Low	Low	Moderate	Moderate	High	High
Medium	Low	Low	Moderate	High	High	High
High	Low	Moderate	High	High	High	High
Very High	Low	Moderate	High	High	High	High
Extreme	Low	Moderate	High	High	High	High

## Information Risk Management

Seeks to protect sensitive data from “6 bad things”...	...caused by 3 root failures...	...across 4 IT domains
Unavailability	Hardware failures	End points
Data corruption/alteration	Software failures	Networks
Loss	People failures*	Applications
Theft		Files/storage
Unintentional distribution		

Information risk management attempts to protect an organization from the wide range of adverse events that can be caused by various types of failures across key IT domains.

\* People failures may include honest mistakes by well-intentioned users, failure to follow policy due to a lack of policy knowledge or a desire to save time, as well as malicious efforts to steal or misuse business-sensitive information.

### Qualitative versus Quantitative Measurements of Risk

One significant challenge in managing information risk is developing a standardized, enterprise-wide approach to defining and measuring specific risks across widely varied business units and geographies. Risk measurements must take into account the probability of an event occurring and the likely consequences for the organization. Qualitative approaches typically measure risk on a scale of high, moderate or low. Quantitative methods assign numerical values to risk probabilities and consequences to arrive at a numerical risk score. In either case, it is essential to have a clear and consistent understanding among security and business executives and personnel of what is meant by these defined levels of risk.

### 3. Apply controls with an eye to repeatability and standardization

Once enterprise information has been located and a risk-reward assessment has been performed, it is essential to put appropriate controls in place to enforce information security policies. According to the *Verizon 2008 Data Breach Investigations Report*, 87% of breaches could have been

prevented if basic security controls had been in place at the time of the attack. For one category of breaches, 71% of the breaches were made via vulnerabilities for which a patch had been available for a year or more.

Controls can be manual – for example, shredding sensitive documents – or they can be technology-based, e.g., scanning file shares to be sure Track 2 credit card data, which includes a customer’s account number and expiration date, is never stored.

There is a growing array of technology-based controls available in the market, such as user authentication, access management, encryption and data loss prevention (DLP). However, RSA and EMC fundamentally believe that controls should be embedded in the IT infrastructure. That’s why EMC has integrated RSA’s authentication, authorization, encryption, and key management technology into its storage systems, content management systems, and the virtual desktop products offered by VMware, an EMC company.

Here, repeatability and standardization of controls is central to RSA’s information risk management strategy. Repeatability comes from using standards-based frameworks and best practices, such as ISO 27002 and CoBIT; these can promote a more comprehensive security posture and greatly reduce the cost and complexity of regulatory compliance by eliminating redundant controls. This view is reinforced by a Gartner Group study where some companies using a risk-oriented approach to compliance reported they had been able to eliminate 30% to 70% of their controls<sup>2</sup>.

<sup>2</sup>Gartner, *How to Implement a Risk-Oriented Approach to Compliance*, G00141561, August 2006.

While reducing cost and complexity, a risk-driven approach also results in better security because controls have been rationally applied – based on an assessment of vulnerability, probability and materiality – rather than in a reactive state, based on fear and guesswork.

#### **Audit your environment**

Audit and reporting capabilities are a critical element of information risk management. They support forensics investigations of security events, allow you to measure progress in reducing risk, and assist in documenting regulatory compliance. Used in conjunction with other tools, RSA's enVision platform for security information and event management (SIEM) supports these tasks by capturing log data on all security-related events and activities, such as user logins, data access activities, configuration changes, and copying, printing and emailing sensitive documents.

The methodology outlined above is more than just a conceptual framework: RSA has translated it into a portfolio of information risk management services that are delivered by its Professional Services group. (See "Bringing Together the Right Technology, Methodology and Expertise" on page 9.)

---

## **A Case Study Close to Home**

---

### **How EMC is Putting Information Risk Management into Practice**

For EMC, which is RSA's parent company, information risk management is not just a theory. It's a mindset, a discipline, and a set of practices that we are working to cultivate in every corner of the organization. We have already discussed how RSA solutions are increasingly organized around a risk management framework. EMC is also using the same solution approach and tools to manage our own information risk.

#### **It starts with a commitment at the top.**

Recognizing that a risk-oriented approach to security requires executive visibility and commitment, EMC in 2007 established the role of Chief Security Officer, now held by Roland Cloutier. In 2003 we also created an Executive Security Council, which consults on strategic decisions relating to information risk management. The Council includes senior representatives from our legal, human resources, and compliance teams.

To put muscle behind these organizational changes, EMC has invested significant resources to strengthen our Global Security organization, which has grown from a handful of people to more than 80 professionals worldwide. We have acquired several best-in-breed providers of security and compliance solutions to enhance our own product offerings – and have subsequently deployed those acquired technologies to protect our own infrastructure. And we have developed and continue to refine rigorous processes for assessing and managing information risk, focusing on those aspects of the business that are most critical to our success. Below, we'll examine initiatives in two of those areas: acquisitions and partnerships.

#### **Acquisitions: Protecting intellectual property**

Acquisitions are a core element of EMC's business strategy. Over the last five years, we have acquired 44 companies and incorporated their technology assets and expertise into EMC solutions. The intellectual property that we acquire, primarily software source code, is a key source of innovation and competitive advantage, but it is also a source of risk. Code is scattered across disparate IT infrastructures and under the control of different IT groups, making it difficult to protect. In addition, many of the acquired companies had another sensitive asset – customer credit card data, which is subject to Payment Card Industry (PCI) compliance requirements – stored on their systems, creating a second source of risk.

Until recently, we had little visibility into – and therefore almost no control over – where these assets reside, who was accessing them, or when attempts were being made to move sensitive information and files outside the network. That has changed dramatically as a result of our implementing a data loss prevention solution based on technology gained in our 2007 acquisition of Tablus.

## Technology puts teeth into policy enforcement

The solution provides a dramatic example of how technology has evolved sufficiently to “put teeth” into strategies for information risk management. For example, data discovery tools give us the means to search out and identify IP assets and PCI data occurring across our global infrastructure and endpoints. The system monitors data on the move and immediately recognizes when an attempt is being made to move protected information – such as credit card data or source code files – outside the network.

Tablus allows us to automate policy enforcement through the use of security controls such as Information Rights Management, S/MIME, and identity-based encryption. In many scenarios, the solution can advise employees when they are about to violate a policy – for example emailing sensitive information without encrypting it – and ask them if they want to continue. This educates well-meaning users about policy, so they’re less likely to make the same error again, and it deters wrong doers by letting them know their actions are being monitored. Depending on the likely severity of a data loss, the solution can modify or even block a prohibited action, for example quarantining suspect email for inspection by a security analyst.

In implementing DLP, one important organizational challenge we faced was persuading business units to expose their data to the DLP solution. EMC addressed this issue by incorporating data loss prevention into our Mergers & Acquisitions playbook. By “day 90” following an acquisition, it is standard practice for network traffic from an acquired company to be routed through a DLP server and scanned to detect potential data loss incidents.

### Partnerships: Trust but verify

For EMC, as for all large organizations, business innovation requires us to foster tighter integration with partners by giving external people access to our internal systems. Yet doing so carries risk: According to the Verizon report on data breaches, “business partners were behind well over a third of breaches, a number that rose five-fold over the time period of the study.”

With EMC having 3,200 partners to manage, providing user-appropriate access in a timely way while safeguarding business-sensitive information is a major task. In response, we developed a third-party access management system that

streamlines on-boarding processes down to three days. Varonis data governance technology has allowed us to automate and facilitate how data permissions are determined, based on business need. Principles such as least privileged access, segregation of duties, and time-limited access privileges that require periodic renewal provide multiple safeguards against abuse. Furthermore, we have the ability to determine who has access to folders containing sensitive data; this is fed into the SIEM system, where it is available to support analysis and investigations of known or suspected security incidents.

### Looking ahead: A dashboard view of risk, security and compliance

Building on these and other initiatives, EMC is planning to deploy an enterprise-wide solution for governance, risk and compliance (GRC). Bringing together inputs from many corporate systems and data sources the solution will provide our CSO, Executive Security Council, and senior security and compliance professionals with a real-time, dashboard view of EMC’s posture for all three aspects of GRC, enabling us to identify and mitigate immediate threats, prioritize vulnerabilities that require investment, and continually improve compliance.

EMC sees information risk management as an ongoing journey, not a final destination. We will continue to apply these strategies and tools to a wider and wider range of business functions and information assets while refining our processes and technology solutions to systematically identify, manage and reduce sources of risk.

### About EMC and RSA

EMC Corp. is a leading global provider of solutions for managing and protecting information infrastructure and information assets. RSA, the Security Division of EMC, is one of the world’s most widely respected security brands.

Through its Information Risk Management solutions, RSA brings together all the elements required for organizations to enable business innovation including risk assessment, information security policy development, and other consulting services; security technologies such as data loss prevention, authentication, and information rights management; and related partnerships, support and services.

### For more information

To learn more about RSA’s Information Risk Management solutions or to download the latest quarterly report from the Security for Business Innovation Council, visit [www.rsa.com/securityforinnovation](http://www.rsa.com/securityforinnovation).

### Bringing Together the Right Technology, Methodology and Expertise

Leveraging the expertise of its Professional Services organization, RSA brings together the technology, services and partnerships enterprise customers need to plan and implement an Information Risk Management Strategy. The key aspects to RSA's approach include:

*A Global Risk Framework:* Security is aligned with key business initiatives. For critical data, a risk assessment provides a holistic view of risk across lines of business and operations. Policy is developed based on best practices. Offerings include: Risk Assessment Services, Policy Review and Development, and Security Assessments.

*Information Classification and Discovery:* Information is classified so appropriate policies and protections can be systematically applied. Data and application discovery tools are used to locate all instances of sensitive information across the infrastructure. Offerings include: Information Classification, Information and Application Discovery.

*Controls on People:* Policy is automatically enforced by implementing controls such as authentication and access management, enabling users to securely access enterprise resources and perform transactions while maintaining a balance between risk, cost and convenience. Controls are based on standard frameworks such as ISO 27002 and PCI DSS, facilitating repeatability. Offerings include: Credentials Management and Credentials, Authentication, Access Management, and Integrated Intelligence (transactions monitoring and adaptive authentication).

*Controls on Data:* Automated controls are implemented to protect structured and unstructured data, whether it is in use, in motion on the network, or at rest on endpoints and servers. Offerings include: Data Loss Prevention, Encryption and Key Management, Information Rights Management.

*Reporting, Auditing and Compliance:* Compliance with security regulations and policies is validated by auditing your controls and documenting their effectiveness. Offerings include: Event Management, Compliance Reporting.

## Putting teeth into protection

EMC's implementation of DLP to protect intellectual property provides a dramatic example of how technology has evolved sufficiently to "put teeth" into strategies for information risk management.



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC

RSA, enVision, SecurID, the RSA logo 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.

IRMSA\_WP\_0908