

Charting the Path: Enabling the “Hyper-Extended” Enterprise in the Face of Unprecedented Risk: 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 Guttmann**
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.

The Dawn of the Hyper-Extended Enterprise

In the “new economy” the enterprise is becoming “hyper-extended,” exchanging information with more constituencies in more ways and more places than ever before. The tools of connectivity, collaboration and communication are enabling operating speeds never thought possible. Technologies such as cloud computing, virtualization, social networking, mobile devices, and VoIP services are being rapidly adopted because of the efficiencies and cost savings that they offer. Outsourcing is also being aggressively pursued. Over the past several years it has been validated as a business strategy as enterprises have built successful relationships with service providers globally and these providers have reached new levels of process specialization and sophistication. Enterprises are increasingly seeking new partners in new non-traditional locations.

The Unprecedented Risk Environment

At the same time that the enterprise is becoming hyper-extended, many factors are coalescing to create an environment in which it is becoming much more difficult to assess risk. Every day there are more threats coming faster than ever before, and they are changing and becoming more unpredictable all the time. Furthermore, the skill set of the bad guys is increasing tremendously. Today’s economic conditions are also increasing the threat because they are causing businesses to be more willing to assume high levels of risk tolerance. Companies are “leaping before they

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.

look” and diving into projects without considering security. Also, desperate economic times are causing a shifting moral compass among workers, damaging the employer/employee relationship and creating a greater danger of insider threat.

The Need for a New Information Security Paradigm

The current security model is ill-equipped for a hyper-extended enterprise operating in an unprecedented risk environment. If we don't figure out a better information security model and fast, there could be devastating consequences. The possible worst case scenarios are nothing new to security professionals. What is new is the likelihood of these kinds of incidents occurring and the magnitude of their potential impact. For example, on a national security scale – terrorists could take a hold of a country's electricity grid. Another potential scenario is a major attack for economic gain, such as extortionists threatening to take down a company's operations or reveal the personal data of customers. A major outsourcer or cloud vendor going down could result in large-scale disruptions to the business operations of huge numbers of companies. Indeed, some of these scenarios have already taken place. If competitive pressures force enterprises across the globe to take on higher levels of operational risk, the level of risk within the entire economy could reach unsustainable levels. A new security paradigm needs to be developed quickly.

Recommendations for Updating the Information Security Model

Rein in the protection environment. Curtail the use of security resources for protecting extraneous information assets. Take a complete inventory of applications and eliminate the ones that are rarely used. Look at data retention and dispose of the sensitive information that is being kept for unnecessary periods of time, creating needless risk. Also, reduce the number of different types of desktops, devices and servers that security supports down to a manageable number that meets business needs. By reducing your protection environment, you will reduce risk and free up resources that can be reallocated to high priority projects and/or strategic investments.

Get competitive. Move away from silos of security and create centralized shared services which are provided by the information security department to business customers across the enterprise. By delivering at least some components of information security as a set of centralized services, you can achieve not only increased efficiencies but also better risk management. The security department must also increase the focus on quality and efficiency of services as business units will be expecting the right product at the right price for all internal services, otherwise they will seek a better deal by doing it themselves or going to external providers. Inevitably, more external security service providers will be used and the core security team should be involved in

“The ability to define the perimeter of the enterprise has now firmly disappeared. That's both in a technical and business sense, with the level of third-party workers, outsourcing, supply chain, and "in the cloud" services. All of these are making it much harder to define where one enterprise ends and where another begins.”

Professor Paul Dorey
Founder and Director, CSO Confidential;
and Former Chief Information Security Officer, BP

“The biggest business driver for security is now innovation – enabling the business to be rapid, flexible and adaptive in this environment. It’s sort of the antithesis of what security traditionally has been, but building a new model of security means also being rapid, flexible and adaptive.”

Dave Cullinane
Vice President and Chief Information Officer
eBay Marketplaces

carefully managing this growth. To be competitive, information security must be able to articulate the value of the services it offers to its customers. Incentivize the business to use your services by offering quality services for a competitive price.

Positively embrace new technology on your terms. Information security departments must accept that it is not feasible to simply say “no” to new and emerging web and communications technologies; rather they have to figure out a way to enable their secure use. For example, get involved early and work with the business to create a transition plan for the secure use of cloud computing. Cherry pick what goes to the external cloud first and if your company uses the “public” cloud to manage sensitive data, de-identify the information first before it can be sent for processing. For large organizations, consider developing your own “private cloud,” which uses the same technology without sharing computing resources between multiple enterprises. Also, plan for the use of social networking within the enterprise because businesses are eager to leverage its potential for innovation and cost savings. Figure out how to allow for its use without putting the company at risk. Develop an Acceptable Use Policy and focus heavily on user education and training. Overall, be better versed in general technology issues in order to understand how developments in IT can deliver significant security benefits to the enterprise. One such area is virtualization, which is a growing trend in most enterprises today.

Shift from protecting the container to protecting the data. More and more, enterprise data is processed and stored in containers not controlled by the enterprise. For instance, the data may be processed by service provider facilities or held in a PDA used by an individual employee or in a laptop used by a contractor with multiple enterprise clients. Therefore, security needs to shift the focus from protecting the container to protecting the data.

Adopt advanced security monitoring techniques. Move away from concepts such as signature-based anti-virus and blacklisting and move towards more accurate techniques such as behavior-based monitoring and white-listing.

Collaborate to create industry standards. We have reached a critical point where the lack of uniform standards is not sustainable. Without standards, enterprises will not be able to truly evaluate security professionals, manage third-party risk or reap the full benefits of new technologies such as cloud computing. There are some

Recommendations for Updating the Information Security Model

1. Rein in the protection environment
2. Get competitive
3. Proactively embrace new technology on your terms
4. Shift from protecting the container to protecting the data
5. Adopt advanced security monitoring techniques
6. Collaborate to create industry standards
7. Share risk intelligence



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.

promising initiatives working towards the development of accreditation for security professionals, standards for assessing and certifying third-parties, as well as interoperability standards. Security practitioners need to actively engage in these efforts now before it is too late.

Share risk intelligence. Enterprises will not be able to defend against international attackers and the fraudster ecosystem without cooperating with other enterprises, law enforcement, and government. Working together is essential for developing enhanced intelligence capabilities so there is more information about who the fraudsters/attackers are and what they are planning. Various governments and industry associations have worked to create and sponsor information exchanges. Unfortunately, these current efforts at information sharing are still inhibited by liability issues, privacy concerns, and competitive fears.

Looking Forward

Creating a new information security paradigm will enable the hyper-extended enterprise to operate securely and successfully even in the face of unprecedented risk and a bad economy. A strategic approach to information security will help organizations deal with the constant evolution of technology and pace of change. In addition, increased collaboration between enterprises will help build a stronger global business community.



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.