

# The Time is Now: Making Information Security Strategic to Business Innovation: 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](http://www.rsa.com/securityforinnovation).*

## State of Affairs

Enterprises worldwide are implementing new technologies and global business models in order to reduce costs, increase efficiencies and generate revenue. However, in many organizations today, security is not considered strategic to business innovation initiatives. While some of the responsibility rests with the business, security professionals themselves are also to blame. The reasons vary widely across organizations; it can depend on their size, vertical industry, compliance obligations, presence of intellectual property, and level of connectivity with third-parties. Company culture may have created an attitude of complacency. Perhaps the security team is still relatively new and inexperienced. Many security programs were conceived in the heyday of compliance, so audits may still be dictating security priorities rather than business strategies.

## The Impact on Business

The consequences of not adequately evaluating and mitigating the risks of business innovation can be devastating. Serious security breaches could not only cost the enterprise enormous amounts of money in settlements and fines, but also damage their brand and reputation. On the other hand, if security practitioners focus too much on risks, their companies could miss out on the benefits of innovation such as new technologies or sourcing models. So risks have to be carefully weighed, but so do opportunities. The timing of the risk/reward evaluation is crucial and in order for it to be effective, it must be done in the project develop- 1  
ment phase rather than attempted afterwards.

## 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.

## Recommendations

The Council members have put forward seven key recommendations for making security strategic to the business innovation process. Following these recommendations can help build an innovation-enabling security program.

**Have the right mind set.** As a security practitioner, your mission is not to say “no,” but rather “how.” If the business wants to take a new direction, don’t try to prevent this from happening because of the risks; instead help the business understand the risks and build a strategy to manage those risks. Keep in mind that security is not compliance. If you’ve fallen into the compliance trap, try to get out of only responding to audits and instead, switch the focus to supporting business initiatives. Take a look at the big critical initiatives for your firm. Think about how you will support them. Can you help make them happen securely, but also, faster, better and cheaper? See the bigger picture: the risk and the reward.

**Know the business and speak business.** Understand your organization’s business, vertical industry, competitive environment, and strategic goals inside and out. Hone your consultative skills and be an expert at communicating and working with people across the organization. Transform your technical security vocabulary to a business language that stakeholders and partners will understand. Learn the business point of view and frame security in that context. Be equipped to convey your message in a concise “elevator pitch” so that people can understand it in ten minutes or less. Convey the benefits of an expertly managed security program in business terms; such as decreased time-to-market, more options for off-shoring, and reduction in external asset costs.

**Recognize and seize opportunities to add value.** Today’s business innovation projects have an inherent need for advanced information security. These projects include technology-driven innovation such as mobility, virtualization and cloud computing; as well as sourcing and globalization initiatives as organizations increasingly need to maximize the value of third-party relationships in order to be truly competitive. Security teams can enable these innovations and add value with strategies such as quickly and accurately managing identities and access, which delivers efficient integration with partners and accelerated on-boarding and off-boarding.

**Build relationships and win influence.** Converting your innovation-enabling security plans into action requires building relations and having organizational influence. Win over allies within the executive ranks in order to earn yourself a seat at the innovation table. Also, develop allegiance at all levels of the organization to gain enterprise-wide access and support for the security mandate. Track support for security within the organization, identifying key influencers and where relationships need to be built. An excellent approach is creating a matrix for your team that maps out all of the people, positions, and lines of power/influence throughout the organization and how to win their support for security. Have face-to-face interaction with stakeholders and meet in person with them as much as possible.

**Become a risk-versus-reward expert.** To help the business get where it wants to go without jeopardizing the organization, you need to be very good at weighing the risks versus the rewards and achieving the optimal balance between them. This will not be an easy task as methods for actually calculating and quantifying the risk/reward equation are not mature. Standards can help, but ultimately you have to be very good at making judgement calls. Get as much quantitative data as you can in order to make qualitative decisions. Understand that you can’t mitigate all risk. Ensure

that you have a strong understanding of the organization's risk tolerance and use this to help guide your risk decision making.

**Build repeatable processes.** Get security built into existing corporate systems for proposing, reviewing and approving business initiatives. Create fast and flexible processes that help to accelerate initiatives and make sure that these are consistent across projects. Once sufficient awareness and credibility for your security processes is created, the business will begin to think about information risk from the start of each project. The right point of engagement for security may vary from project to project depending on its nature, but ultimately the objective is to get security "built in" to initiatives rather than "bolted on." Create a "playbook" that can be used as a standardized template for new projects. This could be a playbook for doing new acquisitions, which would provide a standard set of security criteria for reviews. Another example is a security template for off-shore locations that would apply a standard set of security requirements.

Make time to be strategic. Make your traditional security operations as efficient as possible in order to make time for high-level planning and thinking. This will allow you to focus more on big-picture issues and free up budget so that you can invest more in forward-looking pursuits.

*"Typically, in most global organizations, security is viewed at best, as a necessary evil and more commonly as a necessary friction. This derives from security's primary 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."*

Bill Boni  
Former Corporate Vice President  
Information Security and Protection  
Motorola

### **Recommendations for Making Security More Strategic to Business Innovation**

1. Have the right mind set
2. Know the business and speak business
3. Recognize and seize opportunities to add value
4. Build relationships and win influence
5. Become a risk-versus-reward expert
6. Build repeatable processes
7. Make time for strategic thinking

### **Evolution of the Role of the Security Executive**

With significant change on the horizon for information security, the role of the security executive is likely to evolve substantially over the next several years. Many of the Council members feel that the concept of traditional information security will disappear and morph into the concept of information risk management. Enterprises are going to strive towards a much more consolidated view of risk and a more holistic approach to enterprise risk management, with the likely convergence of physical and logical risk management. It is certain that security executives will need to have a more international outlook and be able to think globally. Furthermore, they will also need to manage a more formalized and cooperative liaison with law enforcement in order to fight cyber crime. Additional responsibilities will likely include third-party management; having an influential role in how partners are selected and managed.



## What Vendors Can Do

The Council also commented on what vendors can do to help security become more strategic to the business innovation process. Vendors need to invest more time developing knowledge of their customers' specific businesses and industries and should be able to relate the value of their security solutions directly to their customers' business goals. Developing a partnered relationship with customers is key to making this happen. In today's globalized business world, vendors must put more emphasis on how their technology can be used to enable secure business-to-business integration. They should consider adopting a service-delivery model that transforms the traditional seller/buyer relationship into a collaborative partnership and be willing to make technology deployments a co-development, co-creation exercise. Through this type of collaboration, vendors will have a vested interest in driving security's ability to innovate within the business.

*"If you are doing your job, you shouldn't even sound like a security person. The business doesn't care how many viruses you stopped. They don't care how many cases you wrote. 'How are you helping me meet my business objectives?'"*

David Kent  
Vice President  
Global Risk and Business Resources  
Genzyme

## 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](http://www.rsa.com/securityforinnovation).



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