

# Bridging the CISO-CEO Divide

Recommendations from Global 1000 Executives

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

- **Anish Bhimani**  
Chief Information Risk Officer,  
JPMorgan Chase
- **Roland Cloutier**  
Vice President and  
Chief Information Security Officer,  
Automated Data Processing (ADP), Inc.
- **Professor Paul Dorey**  
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
- **Vishal Salvi**  
Chief Information Security Officer,  
HDFC Bank Limited
- **Craig Shumard**  
Chief Information Security Officer,  
Cigna Corporation
- **Denise Wood**  
Chief Information Security Officer, FedEx

And special guest contributor

- **Michael Capellas**  
Chief Executive Officer,  
First Data Corporation

*This synopsis is a small teaser of the wealth of information provided by the Security for Business Innovation Council. For a deeper dive, please view the full report at [www.rsa.com/securityforinnovation](http://www.rsa.com/securityforinnovation).*

## Information Security Comes of Age?

There are signs that information security, previously viewed as a necessary evil or inconvenient afterthought of corporate strategy, is becoming core to organizational success. This recognition is shared within the ranks of information security and also by senior executives across global organizations. In the study, "Global State of Information Security 2010," 52 percent of C-levels reported that the increased risk environment created by the economic downturn has elevated the role and importance of the security function.<sup>1</sup>

Many of the measures organizations are taking to survive in this economy – such as using new technologies and global business models to drive efficiencies – are both innovative and risky. Never before have information security officers been in such a strong position to help their companies take the right risks in the right ways. But first they must gain the confidence and support of their CEOs. And CEOs must recognize that their companies' success in recovering from the economic downturn and thriving in the longer term is dependent on their companies' ability to expertly manage the risks they are taking.

A divide between an organization's CEO and its security officer can detrimentally impact its risk profile and ultimate business success. Gaining and maintaining the support of the CEO (and other C-suite executives and the Board) is paramount for a strategic information security effort.

## State of Affairs: How CEOs View Information Security

Convincing a CEO that information security should be strategic starts by knowing where he/she currently stands. The CEO's view will depend on the vertical industry, regulatory regime and intellectual property; as well as third-party relationships and global reach.

Most CEOs today recognize the importance of having an information security strategy. Research shows that although they see it as important, they don't necessarily have a realistic picture of information security. Of course CEOs cannot be expected to be information security experts; that's why they have security officers. But the CEO can and should be expected to provide authoritative support for information security. And there are encouraging signs of this: more and more companies are beginning to address information security governance by putting in place oversight committees and increasing the frequency of reporting to the CEO, other C-level executives and the Board.

As CEOs increase their awareness and support, it's up to information security officers to better educate CEOs about the real risk picture and build on the momentum to position information security as a strategic business endeavor.

## Call to action for CISOs and CEOs

### Making the Case to Your CEO

Convincing the CEO and other executive leaders that information security has an important role to play in the business strategy is a critical part of the CISO's job. Ten ways to help security professionals gain CEO support are contained in the full Security for Business Innovation Council report. These include:

- Establish security champions within the CEO's circle of trust: Win over those who influence or interact with the CEO on a regular basis (the Board and C-level direct reports).

- Set up a clear organizational structure: The security organization should have an absolutely crystal clear organizational structure. It must be clearly articulated, socialized and institutionalized across the whole enterprise so people "get" what security does just as they "get" what other more entrenched departments, such as accounting and finance, do.
- Make it real: To help the CEO understand the risk, make it real. As much as possible, CISOs should quantify the risks. Don't just give vague explanations; instead describe realistic scenarios with actual numbers for probabilities, impact and financial losses. Address these within the context of the organization's market position, vertical industry and regulatory regime.

## Alienating Your CEO

Along the way there may not be many opportunities to make a good impression on the CEO – so it's important to know what not to do. The report outlines 10 surefire ways to alienate a CEO, offering advice including:

- Don't waste money: If you can't show that every security investment ties back to business risk, you'll be seen as wasting money in the eyes of executive leadership. Other areas of waste might be running an inefficient operation or implementing excessive security procedures that slow everyone down, reducing productivity.

*"You have to be able to understand risk analysis as the premise. That's where you start. This is about risk. The language of business is about risk. And if you sit in a CISO position and you can't meaningfully talk about measures of risk and layers of risk, you're probably not going to be successful."*

Michael D. Capellas  
Chairman & Chief Executive Officer, First Data

“CEOs don’t want to hear about projects. They want to hear about transformational programs – how are you going to get the organization to where it needs to be? And what are the metrics you’ll use so you know you’re making improvements? That’s what they care about.”

Denise Wood  
Chief Information Security Officer, FedEx

- Don’t expect special treatment: Some information security professionals believe if risks are increasing, so should their budget. But it’s not necessarily a direct line from more risk to more spending. Consider that when the business units face increasing competitive threats, their budgets do not automatically increase in order to fend off competitors.
- Don’t operate in a vacuum: Have security goals that are not aligned with the executive leadership’s goals and you’ll become irrelevant. For example, continuing to focus on fortifying the network perimeter protection while all the heads of the business units are busy trying to save costs by moving data processing to third-party service providers reflects a serious misalignment with the objectives of the business.

### How does the “new economy” change making the case?

Ultimately the approach to making the case for strategic information security doesn’t change in the current economic conditions. It is still risk-based and business-driven. What changes is the focus on costs. This means looking at what must be done rather than what should be done and prioritizing based on the risks that are most relevant to the organization’s strategic imperatives. The security officer needs to proactively determine what parts of the information security program could be deferred making it completely clear how deferrals change

the risk picture. As economic conditions change, the CEO and other leaders may change their appetite for risk. If they decide cost savings trump risk reduction, it’s the CISO’s job to make sure that they understand exactly what level of risk they will be accepting as a tradeoff, and get them to agree to accept that increase. Ultimately, security will always be adequately funded because “adequate” means it matches the level of risk that the business deems acceptable.

### How CEOs Can Put their Organizations at Risk

CEOs need to understand how significantly their actions and attitudes will impact the effort to protect information at their companies. The full Security for Business Innovation Council report covers a list of ten top ways that CEOs can unwittingly put the company at risk when it comes to information security including:

- Setting the wrong tone at the top: If organizational leaders create a culture of apathy towards protecting information, the organization will do the same. The CEO can set the right tone by actively communicating the strategic importance of this responsibility and establishing shared accountability for the protection of information throughout the organization.
- Thinking about information security as just a technology or a compliance problem: Information security needs to be viewed as a risk management problem. When the CEO doesn’t see the bigger-picture context surrounding security decisions, their company is inevitably exposed to all kinds of other risks.
- Failing to set up proper organizational responsibility: If information security ownership is not established at the appropriate level of seniority within a company, it will not be seen as serious. A role that directly impacts a company’s brand, reputation and information assets should have a security leader appointed to it such as a CISO or equivalent.



## Conclusion

In the past it may have seemed like an uphill climb just to get the executive leadership to recognize the importance of information security, but increasingly this is a given. Now the campaign must shift from creating awareness of the need to actually implementing a strategic approach to information security. The CEO is your most important ally in this endeavor. He/she needs to lay the foundation on which you will build across the entire organization. It is absolutely key that you earn the confidence of the CEO; he/she must trust that you know what you're doing and have the company's best interests in mind. The benefits are clear. As enterprises navigate through a long and spotty economic recovery, a strategic, risk-based approach to information security will optimize risk-taking and maximize the rewards of business innovation.



The Security Division of EMC

[www.rsa.com](http://www.rsa.com)

EMC, RSA and RSA Security are registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other products or services mentioned are trademarks of their respective owners.

©2009-2010 EMC Corporation. All rights reserved.

CISO4\_SYN\_0609

## 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 there is still a missing link. Though business innovation is powered by information; protecting information is typically not considered strategic; even as enterprises face mounting regulatory pressures and escalating threats. In fact, information security is often an afterthought, tacked on at the end of a project or - even worse - not addressed at all. But without the right security strategy, business innovation could easily be stifled or the organization could be put 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. The time is ripe for a new approach; security must graduate from a technical specialty to a business strategy. While most security teams have recognized the need to better align security with business, many still struggle to translate this understanding into concrete plans of action. They know where they need to go, but are unsure how to get there. 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.