

Synopsis of the Report  
based on discussions with the

VOLUME 3, fall 2010

# Security for Business Innovation Council

An industry  
initiative  
sponsored  
by RSA



The Security Division of EMC



**ABN-AMRO**

DR. MARTIJN DEKKER,  
Senior Vice President, Chief  
Information Security Officer

**ADP INC.**

ROLAND CLOUTIER, Vice  
President, Chief Security  
Officer

**BHARTI AIRTEL**

FELIX MOHAN, Senior Vice  
President, CISO & Chief  
Architect

**CSO CONFIDENTIAL**

PROFESSOR PAUL DOREY,  
Founder and Director and  
Former Chief Information  
Security Officer, BP

**CIGNA**

CRAIG SHUMARD, Chief  
Information Security Officer

**DIAGEO**

DR. CLAUDIA NATANSON,  
Chief Information Security  
Officer

**EBAY**

DAVE CULLINANE, Chief  
Information Security Officer  
and Vice President

**EMC**

DAVE MARTIN, Chief  
Security Officer

**FEDEX**

DENISE WOOD, Chief  
Information Security  
Officer and Corporate Vice  
President

**GENZYME**

DAVID KENT, Vice  
President, Global Risk and  
Business Resources

**JPMORGAN CHASE**

ANISH BHIMANI, Chief  
Information Risk Officer

**NOKIA**

PETRI KUIVALA, Chief  
Information Security Officer

**HDFC BANK**

VISHAL SALVI, Chief  
Information Security Officer  
and Senior Vice President

**T-MOBILE USA**

BILL BONI, Corporate  
Information Security  
Officer, VP Enterprise  
Information Security

**TIME WARNER**

RENEE GUTTMANN, Vice  
President, Information  
Security & Privacy Officer

**WITH GUEST CONTRIBUTOR:**

STEWART ROOM, Partner,  
Privacy and Information  
Law Group, Field Fisher  
Waterhouse LLP

## A New Era of COMPLIANCE

### Raising the Bar for Organizations Worldwide



RECOMMENDATIONS FROM GLOBAL 1000 EXECUTIVES



*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).*



# The End of Business as Usual

**"TEN YEARS** ago, security wasn't a common business practice. But compliance has made security a business imperative. Enterprises today are expected to have mature disciplines of privacy and risk in order to do business in an international environment."

ROLANDCLOUTIER, VICE President, Chief Security Officer, Automatic Data Processing, Inc.



With the dawn of the Internet age, huge volumes of business transactions and personal data moved online. About 10 years ago, government and industry realized that organizations should be held responsible for protecting this digital information and started mandating safeguards. Since then, there has been a constant flow of regulations and standards globally.

Now regulators around the world are upping the ante, prompted by massive data breaches over the last few years, which have dominated the headlines and caused public outcry. New breach notification laws are spreading across the globe, forcing more transparency for information security failures. Enforcement of regulations is on the rise.

Many organizations have embraced existing mandates and have made great strides in developing compliance programs. The shifting compliance landscape now adds urgent new challenges for these players. Other organizations have skated by with lackadaisical efforts because they faced minimal oversight. Those days are gone. Today, a decade into compliance, we are entering a new era characterized by higher levels of scrutiny and greater responsibilities for protecting information.

This report provides a comprehensive set of concrete recommendations from 15 of the world's leading security officers and an expert in data protection to help organizations align their programs to the heightened demands of today's compliance landscape and prepare for tomorrow.

## The Changing Compliance Landscape

Over the past 18 months the compliance landscape has significantly shifted. Specifically, four emerging trends are now ushering in this new era:

- ➔ 1. Strengthened enforcement
- ➔ 2. Global spread of data breach notification laws
- ➔ 3. More prescriptive regulations
- ➔ 4. Growing requirements regarding business partners

### 1. Strengthened Enforcement

Although enforcement of existing regulations has been weak in many jurisdictions worldwide, regulators and standards bodies are now tightening enforcement through expanded powers, higher penalties and harsh enforcement actions.

For example, the EU Data Protection Directive is currently undergoing a complete overhaul. In reviewing the law, the European Commission has stated that strengthened enforcement is one of the major objectives.<sup>1</sup>

In the US, to increase awareness and help enforce compliance with the Federal Trade Commission (FTC) standards, this year the FTC has levied high-visibility sanctions. For example, Twitter<sup>2</sup> and RiteAid<sup>3</sup> were subject to harsh FTC actions that received a lot of media attention.

In Asia and Europe, Visa and MasterCard intend to step up enforcement. The card companies have set global 2010 deadlines for all Level-1 and Level-2 merchants worldwide, including annual on-site audits by a Qualified Security Assessor (QSA) and increased fees for non-compliance.<sup>4</sup>

### 2. Global Spread of Data Breach Notification Laws

Regulators are not just looking at ways to tighten up existing laws; they are introducing new laws aimed at forcing more transparency. Data breach disclosure is becoming a global principle as jurisdictions worldwide adopt privacy and data protection laws that include a general obligation to notify government agencies, individuals, and/or other authorities such as law enforcement of unauthorized access or use of personal data.

<sup>1</sup> Viviane Reding Member of the European Commission responsible for Information Society and Media Privacy: the challenges ahead for the European Union", Keynote Speech at the Data Protection Day 28 January 2010, European Parliament, Brussels

<sup>2</sup> Twitter, FTC settle on charges of data security lapses", InfoSecurity.com, June 24, 2010

<sup>3</sup> Rite Aid Settles FTC Case", WSJ, July 27, 2010

<sup>4</sup> PCI DSS requirements still baffling as compliance deadline approaches", SearchSecurity.co.UK, March 8, 2010



# Business Impact

*"IT'S a very interesting time to be active in this field because so much is changing. An innovative or clever approach to compliance actually gives a competitive advantage, because compliance applies to everyone now and it's really survival of the fittest."*

DR. MARTIJN Dekker, Senior Vice President, Chief Information Security Officer, ABN Amro

Many argue that it was the rise of breach notification that really made a difference in elevating information security awareness and practices in the U.S.A. With breach notification becoming an established global principle, legislators worldwide are sending a message to get serious about data protection.

### 3. More Prescriptive Regulations

As more regulations are introduced, there is a trend towards increasingly prescriptive rules. Two recent state laws from Massachusetts and Nevada are prime examples. The Massachusetts law puts forth some of the most comprehensive data security obligations yet to be imposed on businesses by a legislature. As well, Nevada and Massachusetts are two of the first jurisdictions in the world to mandate encryption of personally identifiable information (PII).

These state laws do not just apply to companies based in these states but extend to all organizations that handle personal information regarding their residents. Any global enterprise that does business in the U.S.A. today will likely be covered by these regulations.

### 4. Growing Requirements Regarding Business Partners

Of late, regulators are also making it clear that enterprises are on the hook for ensuring the protection of their data when it is being processed by a business partner - including cloud service providers.

For example, in July 2010, a Data Protection Authority (DPA) in Germany issued the first statement by a regulator regarding assuring cloud computing service providers.<sup>5</sup> According to the guidelines, companies or qualified external third parties must exert "regular control" to ensure cloud computing service providers are observing the restrictions of the federal privacy laws in Germany.

<sup>5</sup>"Cloud computing may violate German data privacy laws", *Lexology*, July 20, 2010

## Business Impact

The new era of compliance creates formidable challenges for organizations worldwide.

For many, stricter compliance could help improve management focus on security but if they take a "check-list approach" to compliance it will detract from actually managing risk and may not improve security.

The new compliance landscape will drive up costs and risks. For example, it takes time and resources to substantiate compliance. Increased requirements for service providers gives rise to more third-party risks.

With more transparency, there are now greater consequences for data breaches. For example, expect to see more litigation as customers and business partners seek compensation for compromised data. But the harshest judgments will likely come from the court of public opinion - with the potential to permanently damage an enterprise's reputation.

When it comes to third-party risk, one of the biggest issues affected by compliance is the use of cloud service providers. Providing the necessary levels of assurance in cloud environments is proving to be difficult. For some jurisdictions, compliance strikes at the very heart of the cloud service provider's business model in which data processing moves around to the physical locations where the lowest-cost capacity is available. For example, the EU Directive places limitations as to where data can live and move.





# Recommendations

*“IN A way, because regulations mandate organizations to mitigate risks, regulators are actually providing opportunities for innovation. When you build core strength in risk management, it enables you to, for example, be first movers in an industry with a new business line. You’re already prepared to manage any new risks.”*

FELIX MOHAN, Senior Vice President, CISO & Chief Architect, Bharti Airtel Ltd.



The council report offers recommendations to help organizations align their programs to the heightened demands of the new compliance landscape. Specific guidance and “how to” strategies include:

- ➔ 1.) **Embrace Risk-Based Compliance:** Build an effective enterprise program that provides everyone in the chain – from individual business process owners to the board of directors – with all of the multi-faceted information needed to make risk decisions.
- ➔ 2.) **Establish an Enterprise Controls Framework:** Create a consistent set of controls across your enterprise that is mapped to regulatory requirements and business needs.
- ➔ 3.) **Set/Adjust Your Threshold for Controls:** Determine the “right” level of security controls and gauge the prevailing industry standard to meet the legal requirement for “reasonable and appropriate” security measures.
- ➔ 4.) **Streamline and Automate Compliance Processes:** Establish an Enterprise Governance, Risk and Compliance (eGRC) strategy that consolidates all of the information necessary from across the organization to manage risk and compliance and provide visibility into controls.
- ➔ 5.) **Fortify Third-Party Risk Management:** Move away from “boilerplate” security agreements and toward comprehensive third-party strategies that focus on: diversification, due diligence, rigorous contractual requirements, consequence management and governance.
- ➔ 6.) **Unify the Compliance and Business Agendas:** “Operationalize” compliance and develop the organizational structure required to fully embed compliance into the business and align it with the organization’s highest-priority goals.
- ➔ 7.) **Educate and Influence Regulators and Standards Bodies:** Educate legislators and constructively affect regulation to avoid overly prescriptive rules that will cripple business.

## 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 top security leaders from around the world to drive an industry conversation and chart the way forward.

## Conclusion

Compliance does not have to be a hindrance to business innovation. If it is done right, it won’t be a drag on resources. If organizations focus compliance efforts on building core risk management strength, compliance can actually enable innovation. The key is to have a risk-based compliance program that puts fewer resources towards non-productive compliance activities and leaves more for an organization to invest in business innovation.



The Security Division of EMC

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

©2010 EMC Corporation. All rights reserved. EMC, RSA and the RSA logo are registered trademarks or trademarks of EMC Corporation in the U.S. and/or other countries. All other trademarks mentioned herein are the property of their respective owners.

CISO7 SYN 1010