Report *based on* discussions *with the*

VOLUME 3, FALL 2010

Security for Business Innovation Council

An industry initiative sponsored by RSA

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

INSIDE THIS REPORT:

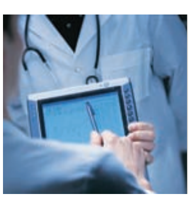
Evidence of four emerging trends in information protection regulations

The rapid shift toward a new era of compliance

Business impact: predictions and analysis

Strategies for aligning compliance programs to the new era

Contents *The Complete Compendium to the New Era*



I. INTRODUCTION

The End of Business As Usual >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>2

II. THE CHANGING COMPLIANCE LANDSCAPE

Strengthened Enforcement >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>4

Global Spread of Data Breach Notification Laws >>>>>>>>>>>>>>>>6

More Prescriptive Regulations >>>>>>>>>>>>>>>>>>>>>>>>>>>>>7

Growing Requirements Regarding Business Partners >>>>>>>>>>>>>8

III. BUSINESS IMPACT

Gets Management Attention >>>>>>>>>>>>>>>>>>>>>>>>>>>>>10

Increases Costs >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>11

Creates Greater Consequences for Data Breaches >>>>>>>>>>>>>>11

Gives Rise to More Third-party Risks >>>>>>>>>>>>>>>>>>>>>>>12

Compliance and the Move to the Cloud >>>>>>>>>>>>>>>>>>>>>>13

IV. RECOMMENDATIONS

① Embrace risk-based compliance >>>>>>>>>>>>>>>>>>>>>>>>>14

② Establish an enterprise controls framework >>>>>>>>>>>>>>>>16

③ Set/adjust your threshold for controls >>>>>>>>>>>>>>>>>>>>>16

④ Streamline and automate compliance processes >>>>>>>>>>>>>18

⑤ Fortify third-party risk management >>>>>>>>>>>>>>>>>>>>>20

Managing cloud service providers >>>>>>>>>>>>>>>>>>>>>>>>>21

⑥ Unify the compliance and business agendas >>>>>>>>>>>>>>>>21

⑦ Educate and influence regulators and standards bodies >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>22

V. CONCLUSION

Get it Right and Reap the Rewards >>>>>>>>>>>>>>>>>>>>>>>>>23

VI. APPENDICES

About the Security for Business Innovation Initiative >>>>>>>>>>>24

Security for Business Innovation Report Series >>>>>>>>>>>>>>>>25

Biographies >>>26

Report Highlights

"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." ROLAND CLOUTIER, Vice President, Chief Security Officer, Automatic Data Processing, Inc.

Recently there have been major shifts in the compliance landscape.

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.

GOING FORWARD IT WILL BE more difficult to hide information security failings wherever organizations do business: legislators are forcing transparency through the introduction of breach notification laws in Europe, Asia and North America as data breach disclosure becomes a global principle.

AS MORE REGULATIONS ARE introduced, there is a trend towards increasingly prescriptive rules. For example, two recent state laws are arguably two of the most prescriptive information protection regulations ever. Any global enterprise that does business in the U.S. today will likely be covered by these regulations.

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.

THE NEW ERA OF COMPLIance creates formidable challenges for organizations worldwide.

FOR MANY, STRICTER COMPLIance could help focus management attention 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.

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.

TODAY, THE NEW ERA IS FORCing all compliance programs to the next level.

AS THE RECOMMENDATIONS reveal, to reach higher levels of maturity, organizations must answer hard-hitting questions about their compliance program such as:

- Have we developed the necessary governance structure and competency in risk management?
- Do we have a consistent controls framework across the entire enterprise?
- Are we able to judge the materiality of risk and determine the appropriate level of controls?
- Can we articulate and defend our risk decisions and controls threshold to auditors?
- Have we streamlined processes enabling a single assessment to produce multiple reports for different purposes?
- Do we have a plan for automation to reduce the number of hours spent on repetitive tasks and manual data collection?
- Would the due diligence we perform in assessing service providers stand up in court?
- Does our vendor oversight program satisfy the rigor of regulation?
- Is compliance fully embedded in our business processes or something we do on the side?
- Are we making sure that the next round of upcoming regulations won't cripple our business?

1 Introduction *The End of Business As Usual*

"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

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 (SEE TABLE 1).

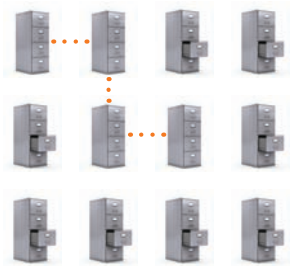
Now regulators around the world are upping the ante, prompted by massive data breaches over the last few years, which have dominated the headlines and caused public outcry. New breach notification laws are spreading across the globe, forcing more transparency for information security failures. Enforcement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

On the litigation front, some of the first test cases and class action lawsuits are making their way through the U.S. courts as consumers, shareholders and business partners are seeking legal retribution from organizations that failed to safeguard data protected by law. Since many more jurisdictions are implementing breach notification laws, there will likely be more incidents disclosed followed by more lawsuits.

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.

Increasingly, even organizations not directly covered by regulation or standards will have to meet the requirements through contracts. Enterprises are becoming more accountable for the information security practices of their service providers. Being able to comply with information security and privacy regulations has become a prerequisite for doing business in the 21st century. More and more companies will be left out of lucrative deals if they are unable to demonstrate compliance with information protection mandates.

Heightened compliance obligations are emerging just as economic conditions motivate organizations to become even more dependent on third parties. Much of today's business innovation involves new business models and IT environments that rely heavily on the use of external service providers and cloud computing.



"COMPANIES ARE *increasingly disqualifying business partners because they're not able to meet the due diligence standards, based on data privacy and other regulatory requirements. So it is certainly impacting business."*

DAVID KENT, Vice President, Global Risk and Business Resources, Genzyme

> *The regulators are moving away from light-touch to more interventionist regulation. That's clear in all senses of society and economy so it's not surprising regulation is tightening up in the data protection field. As I see it, the trajectory of the law here is one way only, which is towards more frequent regulatory intervention, more disputes, more arguments, and more litigation."*
>
> STEWART ROOM, Partner, Privacy and Information Law Group, Field Fisher Waterhouse LLP

TABLE 1: **A DECADE OF REGULATION GROWTH***

DATES	REGULATION OR STANDARD	GEO	APPLIES TO
Late 90s-2005	Data Protection Directive member country implementations	European Union (EU)	All organizations operating in the 27 member countries
2000-04	Personal Information Protection and Electronic Documents Act (PIPEDA)	Canada	All organizations in Canada
2001-03	Gramm Leach Bliley Act (GLBA) FTC and Interagency Rules	U.S.	All financial institutions in the U.S.
2003-05	Healthcare Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules	U.S.	All healthcare organizations in the U.S.
2003	SB-1386 (privacy law with notification)	California	All organizations handling data on Californian residents
2003-05	Personal Information Protection Act (PIPA)	Japan	Government or private entities handling personal info on 5,000+ individuals
2004-05	Sarbanes-Oxley (SOX) Section 404 on Internal Controls	U.S.	All publicly traded companies in U.S. (exemption for smaller reporting companies)
2004-07	Basel II Operational Risk Requirements	Global	All internationally-active banks with assets of $250B+
2004-10	Payment Card Industry Data Security Standards (PCI DSS)	Global	All organizations processing credit card data
2006-10	North American Electric Reliability Council (NERC) Critical Infrastructure Protection Cyber Security Standards	North America	Users, owners and operators of the bulk electric power system
2008-9	IT (Amendment) Act	India	All organizations

**Sampling of regulations with information protection requirements; dates listed are time periods for effective dates and/or compliance deadlines*

And all of this is occurring against a backdrop of escalating threats.

This new era of compliance will have significant impact on business. Organizations not meeting prevailing standards will have to ramp up quickly in order to survive as a player in international business. Enterprises that have been diligent in achieving relatively high standards and building mature compliance programs will need to rapidly address new challenges.

The seventh report of the Security for Business Innovation Council will look at how the changing compliance landscape is raising the bar for organizations worldwide and how to meet the challenges. It offers a set of seven concrete recommendations drawn from discussions with 15 top security executives of some of the world's largest companies as well as one of the world's foremost experts on data protection laws.•

2 The Changing Compliance Landscape

Four emerging trends usher in the new era

After a decade of information protection mandates, compliance is still a major focus for enterprises worldwide. The latest E&Y Global Information Security Survey found 77 percent of IT and security executives rated achieving compliance with regulations as a top priority.[1]

Most large global enterprises today must comply with a lengthy list —even up to hundreds — of regulations and standards with requirements for information protection. An organization's particular list depends on their type of business, vertical industry, and the geographies in which they operate. Every organization's list is continuously getting longer as new regulations appear on the scene. For example, many organizations will be affected by the new "Dodd-Frank Law" in the U.S. or "Solvency II" in the European Union (EU).

Besides the constant flow of new regulations, organizations must now contend with a new era of compliance. Over the past 18 months the compliance landscape has significantly shifted. Specifically, four emerging trends are now ushering in this new era:

- Strengthened enforcement
- Global spread of data breach notification laws
- More prescriptive regulations
- Growing requirements regarding business partners

Strengthened Enforcement

Although enforcement of information protection legislation has been weak in many jurisdictions worldwide, regulators are now

> **"IT GETS** *more and more complex. If you're a public company, you've got SOX. If you take credit cards you've got PCI. Then there are the privacy laws. A company like ours has operations in 37 countries around the world. Global organizations have to comply with all the variations of privacy laws in the US, the EU and Asia — and there are new laws and new requirements all the time."*
>
> DAVE CULLINANE, Chief Information Security Officer and Vice President, eBay

strengthening it through expanded powers, higher penalties and harsh enforcement actions.

European Union

Originally issued in 1995, 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.[2] Plans for the new legislation will be published in late 2010 with the new proposed law to be promulgated in 2011.[3] Recommendations for strengthening enforcement include providing Data Protection Authorities with full powers to investigate (e.g. conduct audits), intervene (e.g. halt data processing) and engage in legal proceedings.[4]

Ahead of the EU's planned overhaul of the Directive, some of the individual member countries including Germany[5], the UK[6] and France[7], have recently been strengthening enforcement of their existing national laws (SEE TABLE 2).

TABLE 2: **STRENGTHENED ENFORCEMENT IN EUROPE**

Germany	IN LATE 2009 the Federal Data Protection Act was amended to increase maximum fines for violations and to grant greater powers to Data Protection Authorities.
UK	IN APRIL 2010, the Information Commissioner's Office (ICO) was given new powers that include the ability to hand out significant fines to firms that commit serious breaches of the Data Protection Act, conduct compulsory compliance assessments and the potential to impose civil monetary penalties on data controllers.
	THE STATED OBJECTIVES are to "Take purposeful risk-based enforcement action where obligations are ignored, where codes or guidance are not followed and where examples need to be set or issues clarified."
France	IN MARCH, 2010, the Senate overwhelmingly approved a draft bill which would reinforce the obligations of data processors, expand the powers of France's national Data Protection Authority (known as "CNIL") and double the potential fines for infringements.
	THE STATED GOAL is to update the data protection laws "to better guarantee the right to privacy in the digital age."
	THE DRAFT LAW is currently under review by the National Assembly.

TABLE 3: **STRENGTHENED ENFORCEMENT IN U.S.**

HITECH Act	HIPAA now includes mandatory investigations of complaints, compliance reviews and higher penalties.
	In addition to the Department of Health and Human Services, state attorney generals can now enforce HIPAA.
	In July 2010, Attorney General's Office of Connecticut issued a $250,000 fine and a "Corrective Action Plan" to a company for failing to protect health information.
NERC	NERC is now under statutory authority to enforce compliance among all market participants.
	NERC will monitor compliance using regularly scheduled audits, random spot checks, and investigations.
FTC	FTC investigation of two security incidents determined that Twitter failed to implement adequate security measures.
	Twitter subjected to independent security audits for ten years and FTC oversight for 20 years.
	FTC investigation found that RiteAid failed to protect customer and employee information.
	RiteAid required to establish an information security program and agreed to pay $1 million and is subject to third-party security audits for the next 20 years.

USA

Recently there have also been efforts to tighten enforcement of information protection legislation in the U.S. (SEE TABLE 3). For organizations in healthcare, the HITECH Act of 2009 updated HIPAA's enforcement provisions.[8] This includes expanding enforcement powers to include state attorney generals who can now fine organizations for HIPAA infractions, incentivizing states to enforce HIPAA standards. In July 2010, Connecticut became the first state to use these new enforcement powers.[9]

The energy industry faces a stricter regime as well. By the end of June 2010, covered entities — generally owners, operators and users of any portion of the bulk power system — were expected to prove compliance with all provisions of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cyber Security Standards. NERC and its regional authorities will monitor compliance and have the power to levy fines as well as sanctions.[10] 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[11] and RiteAid[12] were subject to harsh FTC actions that received a lot of media attention. In July 2010, FTC Chairman Jon Leibowitz testified before Congress regarding the FTC's intentions to continue focusing on privacy[13], which likely means more investigations and sanctions in the future.

PCI in Europe and Asia

Global enforcement of the Payment Card Industry Data Security Standard (PCI DSS) is also getting more serious. While the PCI standards have been widely implemented and enforced in the United States, so far compliance in Europe and Asia has been relatively weak. But Visa and MasterCard intend to step up enforcement and are imposing compliance deadlines for European and Asian organizations. The card companies set global 2010 deadlines for all Level-1 and Level-2 merchants worldwide, including annual onsite audits by a Qualified Security Assessor (QSA) and increased fees for non-compliance.[14] Recently the PCI Security Standards Council appointed the first European director specifically to increase awareness and "strongly encourage" European companies to adopt the PCI standard.[15]

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

"TO UNDERSTAND *the impact of breach disclosure you have to understand what breach disclosure is about in a philosophical sense. It's about changing the power relationship between the regulator and the regulated. The classic failure of regulation is that the regulator doesn't know as much about the regulated entity as the entity itself. Breach disclosure is a transparency mechanism that equips the regulator with information and therefore empowers the regulator."*

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

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 (SEE TABLE 4). Requirements vary including who must be notified, the type of data that triggers notification, and if there is a risk-of-harm threshold.

California's landmark SB-1386 set off a wave of state breach notification laws that now cover almost the entire U.S. Recently, this trend has hit the EU. The Privacy and Electronic Communications Directive (e-Privacy Directive) was amended in late 2009 to include data breach notification.[16] It is now mandatory for telcos and Internet service providers in the EU to inform national regulatory authorities of any data security breach. Depending on the effects of the breach, they may also be required to inform subscribers. The deadline for transposition of the Directive by member states is May 25, 2011. The upcoming overhaul of the EU Data Protection Directive is expected to include data breach notification requirements, which would broaden breach disclosure to cover all industries in all 27 member countries in the EU.[17]

TABLE 4: **DATA BREACH NOTIFICATION GOES GLOBAL**

YEAR	COUNTRY	DATA BREACH NOTIFICATION LAWS
2003	*U.S.*	California's landmark SB-1386 sets off wave of state laws
2003-2010	*U.S.*	46 states enact notification laws
2008	*UK*	Information Commissioner's Office issues a best practice guidance requiring notification
2009	*EU*	e-Privacy Directive amended to include notification requirements for electronic communications sector
	Germany	National privacy law amended to include notification
2010	*Austria*	National privacy law amended to include notification
	France	Draft legislation passed in Senate would make notification mandatory
	Canada	National privacy law amended to include notification
	Mexico	New privacy law enacted that includes notification
	Ireland	Code of Practice issued regarding notification
	Hong Kong	Privacy Commissioner issues guidance note on breach notification
	EU	Data Protection Directive under review for revision; proposed law expected by 2011 to include notification requirements for all industries; to be implemented in all 27 EU member countries

Meanwhile, several countries in Europe have proceeded to issue their own legislation or guidance on notification ahead of the EU's planned notification requirement for the updated Data Protection Directive. These include the UK[18], Germany[19], Austria[20], France[21], and the Republic of Ireland.[22] Beyond Europe, other countries have recently enacted new rules including Canada[23], Mexico[24] and Hong Kong.[25]

Breach disclosure laws are considered an effective legal instrument that leverages the powers of the marketplace. Notification not only equips the regulator with the necessary information to exercise statutory powers, but it also provides other stakeholders such as customers and business partners with the necessary information to make decisions regarding further purchasing or partnering, as well as to initiate litigation and compensation claims. One possible drawback to the spread of notification laws is that as more and more breaches are disclosed, the public may just get numb. Today the Privacy Clearinghouse web site already shows that around 500 million people's records have been breached since they started keeping their records in 2005.[26]

However 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. With breach notification becoming an established global principle, it will be difficult to hide information risk management failures no matter where an organization does business.

More Prescriptive Regulations

Another emerging trend is the tendency for legislation to get more prescriptive. Two of the latest examples are new state privacy laws from Massachusetts and Nevada, which became effective in 2010. They are arguably two of the most prescriptive information protection regulations faced by enterprises to date (SEE TABLE 5). These state laws do not just apply to companies based in these states but extend to all organizations that handle personal informa-

"In a regulated environment, you essentially have to vouch for the fact that you've partnered with organizations which can handle the information in a secure fashion, consistent with regulation." *David Kent, Vice President, Global Risk and Business Resources, Genzyme*

tion regarding their residents. Any global enterprise that does business in the U.S. will likely be covered by these regulations.

The Massachusetts law puts forth some of the most comprehensive information security requirements 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 new state privacy laws reflect a growing concern among American state legislators about continued large-scale data breaches and the resulting identity theft. It is widely believed that these more prescriptive state laws are harbingers of things to come. The state of Washington has already followed Nevada's lead in making PCI law.[27] Since there is still no overarching federal information protection legislation in the U.S., the Massachusetts law could influence other states and, like the first state breach notification law enacted by California, have a nationwide affect. Already the state of New Jersey has released its "Pre-Proposal" for similar regulations.[28]

TABLE 5: **PRESCRIPTIVE REGULATION**

EXAMPLES	REQUIREMENTS
Nevada's updated privacy law	Adds expanded encryption requirements for data in transmission and on portable devices
	Makes PCI compliance law for all businesses that accept credit cards
Massachusetts' new privacy law	*Encompasses a lengthy list of security requirements such as:*
	• Written information security program
	• Physical and logical access controls
	• Monitoring of unauthorized access
	• Service provider oversight
	• Encryption of data in transmission and on portable devices (minimum 128-bit)
	• Includes penalties and injunctive relief (i.e. court order can be issued to stop violations)

TABLE 6: **MASSACHUSETTS PRIVACY LAW'S REQUIREMENTS REGARDING THIRD-PARTIES**

- → Select and retain third-party service providers that are capable of maintaining appropriate security measures to protect information consistent with the regulations
- → Contractually obligate third-party service providers to implement and maintain appropriate security measures.

Growing Requirements Regarding Business Partners

Many existing regulations and standards call for organizations to assure that any third-parties that handle protected data employ adequate security measures. A recent wave of regulatory activity goes even further in establishing legal requirements for enterprises as well as their business partners to ensure the security of information.

New obligations

The new Massachusetts privacy law sets up more substantial obligations to engage in pre-contract evaluation and ongoing monitoring of the security practices of third parties than most other previous legislation in the U.S.A and elsewhere[29] (SEE TABLE 6).

Recent modifications to HIPAA, through the HITECH Act, mean that more organizations are now covered by HIPAA: the definition of a business associate has been broadened to explicitly include sub-contractors, providers of health data transmission services, and vendors of personal health records.[30] As well, business associates now have direct responsibility and liability for a breach, including notification and remediation, and are subject to the Act's civil and criminal penalties.

Enforcement action

This concept — that a covered entity is ultimately responsible for the actions of its third parties — is reinforced by a recent FTC enforcement action involving mortgage lender Premier Capital Lending. In that case, the FTC brought an action for, among other things, violating the Safeguards Rule by engaging with a business partner that did not employ "reasonable and appropriate" security to safeguard sensitive data, to access consumer credit reports through Premier's system.[31]

Guidance on cloud service provider

In July 2010, a Data Protection Authority (DPA) in Germany issued the first statement by a regulator regarding assuring cloud computing service providers.[32] According to the guidelines, companies or qualified external third parties must exert "regular control" over whether cloud computing service providers are observing the restrictions of the federal privacy laws in Germany (SEE TABLE 7). This first statement from a regulator provides an indication that organizations will be held legally accountable for assuring that their cloud computing service providers have adequate security. •

TABLE 7: **GERMAN DPA GUIDELINES ON CLOUD SERVICE PROVIDER ASSURANCE**

Exert "regular control" over the cloud vendor's technical and organizational measures used to protect the data.
Two ways to exert "regular control" were suggested: • Obtain an expert opinion in the form of audits or certificates indicating that the service provider is observing the legal restrictions. • Obtain a binding guarantee declaration in which the service provider makes a comprehensive commitment to meet the obligations imposed by the law.

"THE REGULATORS *in general seem to be heading towards more prescriptive regulations. When standards get too prescriptive they can be a hindrance. They start to impose things that may not be relevant to an organization's risk management. The organization may do things in a different way, yet manage risk well. But that wouldn't be acceptable to the prescriptive regulator."*

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

3 Business Impact *Only the Strongest May Survive*

"Heightened scrutiny of other people and by other people is going to cost you. Besides regulators, customers or partners who are working with you are going to demand more of you. That's going to add cost." *Stewart Room, Partner, Privacy and Information Law Group, Field Fisher Waterhouse LLP*

SINCE INFORMATION PROTECTION REGULATIONS first appeared a decade ago, compliance has affected enterprise IT and business strategies. The new era of compliance will add to the already formidable challenges and force a renewed focus on compliance.

Gets Management Attention

A major impact of compliance is that it gets the attention of executive management. The new more stringent regulatory regime may help motivate management in organizations which have not taken security that seriously yet.

In many organizations, compliance has elevated information security to become a C-suite and board-level issue. Compliance often enables the necessary investment in the resources and people required to protect information. It creates a willingness to change business processes and helps drive a cultural change. Ten years ago, many information security organizations did not have the mindshare, funding, or technology they do today. Recent research indicates that 64 percent of IT and security executives surveyed believe regulatory compliance has increased the effectiveness of information security.[33]

But whether compliance helps to improve security depends on an organization's approach. If management simply meets the requirements of the regulation or standard rather than managing risk, information security will not necessarily improve.

> *"Compliance is the best and worst thing that ever happened to security. It's a combination. It gives you awareness. It gives you real life justification for good security practices. But at the same time, especially when regulations get prescriptive, it can make it more difficult to have a truly risk-based program where your highest risk items always get your financial investment."*
>
> DENISE WOOD, Chief Information Security Officer and Corporate Vice President, FedEx Corporation

Information security cannot be treated as a fixed state. It is an ongoing process that must respond to a changing environment.

Increases Costs

In the new era of compliance, costs are sure to rise. In a recent survey, 55 percent of IT and security executives indicated that regulatory compliance costs accounted for moderate to significant increases in their overall information security costs.[34] As the compliance landscape gets more complex, demonstrating compliance gets more time consuming and costly. Enterprises must constantly update their compliance programs to account for new requirements. For a global enterprise, another major struggle is dealing with international laws that actually have conflicting requirements. One country tells you to do one thing; while another tells you can't do that. It makes it difficult to have a global model for compliance. Organizations end up having to duplicate functions across sovereign boundaries to stay compliant, adding costs.

Another reason costs go up is that the number of requests to demonstrate compliance continually increases — not only are requests coming from regulators and auditors, but also from customers and partners. Most organizations continue to rely mostly on manual efforts and reams of paper for data collection and reporting, which consumes inordinate amounts of resources.

Increased responsibility for information security across the extended enterprise also has a significant cost impact on organizations. For example, organizations must undertake exhaustive work to evaluate and oversee service providers' security practices. At the same time, service providers must invest in developing assessment processes so that they can give customers the required assurances.

Generally, if regulations call for a risk-based approach, organizations are investing in security controls based on an analysis of their risks weighed against their appetite for risk. Their investment addresses their business needs to protect information. It is when regulations get more prescriptive that compliance creates additional costs for security controls. Organizations have to spend budget dollars implementing technology specified by regulatory requirements rather than technology which helps to manage risks.

Creates Greater Consequences for Data Breaches

The chances of having a data breach will be much higher for those organizations that ignore risks or do little to mitigate them. But even a diligent organization may experience a breach. If a breach occurs and the data involved is governed by law, there could be regulatory actions and fines. With breach notification now a requirement in more and more jurisdictions, it is increasingly likely that an organization will also have to disclose the breach to authorities and/or those affected.

Generally, it's not the regulatory fines or actions that are the most dreaded consequences of a breach — fines won't push most companies out of business — it's the resulting public stigma. The more significant fallout stems from having to disclose an incident and can include:

- Direct costs of notification, damage control activities and breach investigation and clean-up;
- Damage to reputation caused by negative media;
- Loss of customer, business partner and investor trust;
- Legal costs of litigation;
- Decline in shareholder value;
- Loss of business;
- Heightened scrutiny by business partners and customers through more detailed assessments; and
- Higher costs of meeting future contract requirements.

Some of the first test cases involving data breaches

TABLE 8: **DATA SECURITY BREACH LITIGATION***

TYPE OF LITIGATION	EXAMPLES FROM 2009-2010
Investor law suit	A retailer settled a lawsuit brought by an employees' pension plan alleging that the retailer failed to protect customers' personal data resulting in a breach.
Class action law suits	Five financial institutions filed a class action suit alleging that two acquiring banks should be included as defendants and share responsibility for damages caused by a data breach which impacted millions of credit and debit cards.
	Two class actions were filed against various defendants including a payment processor, arising out of an unauthorized intrusion into the processor's computer systems.
	A bank settled a lawsuit, which alleged that it failed to limit access to and/or adequately safeguard private customer information, agreeing to pay identify theft insurance and free credit monitoring reimbursement for millions of customers.
B2B Law Suits	A lawsuit filed by a manufacturing company alleged that a bank opened the manufacturer's customers to phishing attacks by sending e-mails asking customers to click on a link to update the bank's security software.
	A lawsuit filed by a restaurant chain is seeking compensation from a point-of-sales system vendor and reseller alleging that problems with the system and installation led to a security breach.

**Lawsuits caused by a breach of information protected under privacy legislation or PCI*

are making their way through the U.S. court system (SEE TABLE 8). Many claims of compensation do not make it into the public realm as businesses instead choose to settle out of court. When a breach involves data processed by many organizations along a value chain, there will be disputes about who is to blame. In fact, with more breach notification laws and requirements for business partners, the climate is ripe for commercial litigation.

Monumental or repeated information security failures may actually take down a company. For example, CardSystems, a payment processor, suffered a catastrophic data breach when 40 million credit card records were stolen in 2005.[35] The credit card companies withdrew their business and CardSystems eventually ceased to operate. In the future, the types of companies at greatest risk of failure may be the outsourcers or cloud computing service providers that handle regulated data, have contractual obligations to protect it, but ultimately do not have adequate safeguards.

The fifth annual Ponemon research study, which looked at the costs of data breaches in the U.S., found that 42 percent of all incidents studied involved third-party organizations and these were the most costly due to additional investigation and consulting fees. The study also found that costs in general continue to rise. The average cost per incident in the U.S. was $6.75 million USD, with resolution costs ranging from $750,000 to $31 million. Organizations are also spending more on legal defense costs than in previous years.[36]

In a follow-on study comparing costs of data breaches internationally, it was found that the average cost per incident worldwide was $3.43 million USD. The costs are higher for organizations that suffer a data breach in countries with notification laws compared to incidents that occur in countries without. For example, in the U.S., costs related to lost records were 43 percent higher than in countries without notification laws.[37] Going forward, costs may go up in other countries as other jurisdictions add notification requirements.

Ultimately, in today's relentlessly competitive global marketplace, the judgment to fear most could be the court of public opinion. In July 2010, a leading PC manufacturer had an incident involving the distribution of motherboards infected with malware, which was reported in the press. However the more damaging coverage was the highly critical editorials in the blogosphere. In our ultra-connected society, people now have the means to know what is going on at companies and broadcast their opinions about it to the world.

Gives Rise to More Third-party Risks

The sheer volume of external service providers that enterprises must oversee is huge and the number

"TODAY IF *a company suffers a significant data breach, it's going to go viral and stay viral. And once it gets on the web, it doesn't go away."*

BILL BONI, Corporate Information Security Officer, VP Enterprise Information Security, T-Mobile USA

"BEFORE SECURITY *was almost like a pet peeve of the security department. Compliance makes it everyone's responsibility, which makes a huge difference. Now it's easier to go about embedding security into the business."*

DR. CLAUDIA NATANSON, Chief Information Security Officer, Diageo

> *The deficit reduction plan in Europe and the States is going to mean loads of outsourcing. But if you're an outsourced service provider you have no hope of getting government contracts — no hope whatsoever — unless you're able to demonstrate very good systems and operations for security."*
>
> STEWART ROOM, Partner, Privacy and Information Law Group, Field Fisher Waterhouse LLP

continues to grow. One of the main reasons that enterprises are increasing their use of third-parties is because it helps reduce costs. For example, even with the economy slowly turning around, enterprises are aiming to reduce costs through outsourcing. The findings of the "Outsourcing 2010" report by the International Association of Outsourcing Professionals (IAOP) show an upward trend with 70 percent of companies now planning on expanding their future outsourcing programs.[38]

Unfortunately, the increasing use of third-parties is on a collision course with the increasing demands of compliance. Nowadays, enterprises are responsible for the whole value chain — wherever their data goes. With more and more service providers and vendors in the chain, there is an increased chance that one of them will fail; resulting in non-compliance and/or a data breach.

This creates challenges for both sides. For enterprises contracting out to service providers, it means developing effective oversight mechanisms. Although companies in heavily regulated sectors such as financial services firms are accustomed to high-level scrutiny of their suppliers, this burden is something new for many others. For service providers who are not up to the standards required for regulated environments, it will be more and more difficult to do business with large enterprises or government agencies. For some, coming up to speed on compliance will be a matter of survival. Increasingly, organizations are walking away from service providers that cannot meet standards.

An unfortunate casualty may be the smaller service providers that cannot afford high levels of security controls and/or the processes necessary for customer assessments. To reduce the costs of testing for compliance, large enterprises may look to larger providers that can supply multiple services.

Compliance and the Move to the Cloud

When it comes to third-party risk, one of the biggest issues affected by compliance is the use of cloud service providers. Cloud computing is moving from marketing buzz to prime time, as many organizations actively explore solutions. A recent TPI survey of more than 140 global IT decision makers revealed that 18 percent are already in discussions with cloud service providers, and an additional 45 percent plan to do so within the next 6 months.[39] Several Fortune 500 companies have already moved their e-mail systems to the cloud; and according to analysts, many others will be turning to cloud e-mail in droves.[40]

Providing the necessary levels of assurance in cloud environments will be difficult. Even large cloud service providers could have trouble meeting compliance requirements. For example, Google signed a landmark deal to provide e-mail and other applications, such as document archiving and spreadsheets, to the City of Los Angeles. Originally the contract imposed a deadline of June 30, 2010 to have the migration to the cloud completed. But Google is having some difficulty meeting the stringent security requirements set by the state Justice Department and the Los Angeles Police. Therefore the deadline has been extended.[41] It is not surprising that compliance is placing hurdles on the road to the cloud.

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. The EU Directive places limitations as to where data can live and move — i.e., it has to be within the borders of the European Union member states or strict contractual arrangements are required to transfer data outside of the EU. Meeting these requirements may negate the cost savings offered by the cloud. •

④ Recommendations *Best practices go to the next level*

"Security practitioners must link the compliance program to the strategy of the organization. Doing compliance for compliance sake is just using up your resources. Ensure that whatever you're doing for compliance actually derives value for your organization and is not just something which pleases a regulator." *Vishal Salvi, Chief Information Security Officer and Senior Vice President, HDFC Bank Limited*

Over the last decade, many organizations' compliance programs have been evolving and are at various stages of maturity (SEE TABLE 9). Where they are at presently on the maturity curve depends on company size, vertical industry, and level of management attention. Today a confluence of factors is forcing all compliance programs to the next level. This set of recommendations helps organizations to align their programs to the heightened demands of today's compliance landscape and prepare for tomorrow.

1. Embrace risk-based compliance

A risk-based compliance program is an operating model with three main components:

- A governance process
- An information risk management competency
- A data collection and reporting ability

In the past decade, regulations have often provided the impetus for organizations to put these systems in place. Most regulations specifically call for taking a "risk-based approach." However these systems are not exclusively for compliance; rather they address a business need to manage risk and ensure the protection of an organization's information assets.

A governance process establishes oversight, formalizes decision-making and creates organizational structures for approvals. Information risk management is "identifying and measuring the risks to information and ensuring that the security controls implemented keep those risks at an acceptable level to protect and enable the business."[42] An acceptable level of risk is determined by an organization's appetite for risk. In the compliance context, an acceptable level of risk must ensure that all regulatory requirements are met and the controls put in place can be defended as commercially "reasonable and appropriate." A fundamental, expectation of most regulations is that organizations implement "reasonable and appropriate" measures to protect information. Except for the very prescriptive, most regulations don't' specify controls. A risk-based approach is the basis for determining what is adequate.

A data collection and reporting ability is required to demonstrate compliance with internal information security policies as well as external regulations and standards. For most large global enterprises, this is ultimately where the burden of compliance is found; it is not in putting controls in place. At present most large global enterprises have already put in place controls and are adjusting them on an ongoing basis in response to the risk environment. Testing the controls and providing evidence of the controls — over and over — is what takes its toll on the organization.

Often it is the interpretation of an on-site auditor that determines whether an organization is "compliant" or not, but an effective compliance program is not audit-driven. Decisions regarding the implementation of security controls should be focused on risk management, not audits. This requires an organization to engage with the auditor to explain context and to ensure he/she can make the link between

> *As you move up the maturity curve, integrating compliance to become part of business processes is towards the top. The ability to measure it, track it, and report on it outside the context of security alone and making it part of board-level reporting is another obvious sign of maturity."*
> ROLAND CLOUTIER, Vice President, Chief Security Officer, Automatic Data Processing, Inc.

TABLE 9: **COMPLIANCE PROGRAM STAGES OF MATURITY**

First stages	Focus is on building awareness
	Investing in developing competencies, processes, and security controls
	Piecemeal approach to each regulation and standard
	Compliance is viewed as a project and is assessment-oriented
	Audit-driven and reactive: preparing for and responding to audits
	Ad-hoc checklist processes
	Informal management by various silos including information security
More mature stages	Focus is on building ownership across the business
	Streamlining processes and controls, looking for ways to create efficiencies
	Framework approach to multiple regulations
	Risk management-driven and proactive: evaluates risks and determines level of controls based on risk appetite
	Compliance is viewed as a process and is reporting-oriented
	Formalized processes
	Implementing automation of data collection and reporting for select assets or categories of controls
	Governance by a cross-functional information risk or compliance council
	Vendor/partner assurance program
Advanced stages	*Adds to more mature stages:*
	Focus is on building personal responsibility with all stakeholders across the enterprise
	Integrating compliance with business processes
	Implementing automation of compliance processes system-wide
	Achieving continuous-controls monitoring
	Integrating with Enterprise Risk Management and Compliance programs

regulatory requirements and the organization's risk decisions. Auditors should not be dictating what to do, but rather validating that expectations are being met. As an organization's program matures, auditors will expect continuous improvement.

Having someone with an IT audit background on the security team can help frame discussions with auditors including: what is the measurement of control effectiveness, what is the residual risk and what is the level of risk the business has accepted? Someone with an IT audit background can also help the auditor to focus on examining the most critical controls and to understand risk-based scoping. Auditors are important allies working collaboratively with security to ensure that compliance efforts enable rather than hinder business.

In general, an effective compliance program requires the right caliber of personnel: for example technologists who understand nuances of legal requirements and the business/risk environment; and lawyers who are able to understand and articulate particular technology risks. You need people who are comfortable working across the various domains.

Compliance also requires highly adaptive personnel as new regulations come up and new risks emerge. One approach to ensuring the security team has the right skills is to invest in career development and support certifications in various disciplines. This helps to build the team's know-how to re-engineer processes and tweak models to fit the changing environment.

Successfully building a risk-based compliance program requires that executive management is willing to make the necessary investments in people, process and technology. It also requires commitment to achieving higher levels of maturity and an under-

RECOMMENDATIONS

1. Embrace risk-based compliance
2. Establish an enterprise controls framework
3. Set/adjust your threshold for controls
4. Streamline and automate compliance processes
5. Fortify third-party risk management
6. Unify the compliance and business agendas
7. Educate and influence regulators and standards bodies

standing of the challenges at every stage. Early on, the main focus is creating awareness of the need to protect information and how to protect it. Over time the focus evolves to getting the business and stakeholders to take ownership of compliance. A key step is moving from informal management of compliance through siloed activities to formal management by a cross-functional team — typically an enterprise risk or compliance committee.

Information protection regulations are only a small subset of an enterprise's total regulatory regime. Besides regulations governing information protection, organizations must adhere to quality standards, labor rules, safety codes and environmental legislation, etc. To effectively align with business strategy, a compliance program that addresses information protection regulations must integrate with the governance, risk management and reporting efforts that are put in place to address all regulations. An effective enterprise program 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. An effective enterprise program 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

MOST ORGANIZATIONS TODAY FACE MULTIPLE regulations regarding information protection. It is inefficient and unsustainable to manage compliance by maintaining a separate list of requirements for every regulation. Instead, develop one overall list of information security controls that satisfies all of the various regulations and addresses business requirements. The end result should be much more than just a list but an "enterprise controls framework," that encompasses the organization's model of security controls. It is typically a matrix with controls mapped to the various regulations and business needs such as protection of intellectual property. In a converged security environment, it may include not only information security controls but also controls related to physical security, product quality, disaster recovery and business continuity, etc.

At the highest level, the framework often has broad controls such as "Authentication," with sub-controls providing more detail such as "Keep authentication mechanisms effective." It may also have practices such as, "Passwords should be changed at regular intervals."

As a basis for developing a customized controls framework, many organizations use standards such as:

- Control Objectives for Information and related Technology (COBIT) from the Information Systems Audit and Control Association (ISACA);
- ISO 27001/2 Information Security Management System and Code of Practice Standards from the International Standards Organization; and
- The Standard of Good Practice for Information Security from the Information Security Forum (ISF).

Developing a controls framework to create a consistent set of controls across an entire enterprise can be an immense task. It is a cross-organizational, cross-functional effort often driven by the information security team with oversight by the enterprise risk or compliance committee. Once an initial framework is established, this committee keeps track of changes to regulatory or business requirements and determines any necessary modifications to the control framework.

With this method, many large enterprises are able to track pending legislation and upcoming requirements and then implement changes ahead of regulatory mandates, achieving compliance pre-regulation. The more mature compliance programs often require only minor modifications to their existing controls when a new law comes out because they have already implemented the relevant security measures based on their risk analysis and business requirements.

3. Set/adjust your threshold for controls

IN A RISK-BASED COMPLIANCE PROGRAM, CONtrols are applied to particular classes of information assets based on an assessment of risk. Different classes of risk might include internal information, confidential data, or customer records. How does an organization determine what level of security control is appropriate for a particular level of risk? For example, what's the "right" level of authentication when a call center employee is accessing customer records over the local network? Or a contractor is accessing corporate data from his home PC? Or a service provider is accessing credit card data over a Virtual Private Network? Is the "right" level a password? A smart card? A biometric? What's the "right" level of encryption to apply? Encrypt all data transmissions?

> *Implementing baseline controls around the systems that process credit card or customer-sensitive information to achieve compliance is not sufficient to achieve security. It's necessary but not sufficient. Compliance is typically a subset of the necessary controls. Legislation lags the state of technology and threats because the institutional and bureaucratic operations that codify the standards take so much time."*
>
> BILL BONI, Corporate Information Security Officer, VP Enterprise Information Security, T-Mobile USA

Using 128-bit encryption? Should it be higher for some transmissions?

Determining the "right" level of security controls to meet compliance requirements and business objectives is complex. Where does an organization set its threshold? Ultimately it is a judgment call that considers security and legal risks. A critical aspect of these decisions is asking what would be deemed commercially "reasonable and appropriate." The enterprise must take a position on the current industry standard. In other words, "What is the prevailing standard of practice in the industry given the current risks and costs?" Of course organizations cannot be expected to implement such a high level of security controls that they can no longer compete in their industry.

The "industry standard" is not going to be conveniently laid out in a manual nor located on a web site. Security officers and information risk managers will need to get a sense of the prevailing standard by networking with peers from other companies to find out what everyone else is doing, as well as by understanding the relevant trends. Over time as expectations rise, the threshold will need to be reset. Generally in every industry the baseline for security controls will likely continue to go up. The threshold is pushed up because of advances in technology, improvements in the practice of security, escalating threats and increased data sharing with third-parties.

In some jurisdictions such as India, companies have been given more specific direction regarding how to determine the "industry standard." The "IT (Amendment) Act", which came into effect in 2009, calls for organizations to take "reasonable security practices and procedures" to protect information, and specifically mentions that this would be prescribed in consultation with the concerned professional bodies or associations, such as the "Confederation of Indian Industry" and the "Data Security Council of India".

What are the consequences of not keeping up with the industry standard? An audit may find that controls are not sufficient, resulting in a fine by a regulator or creating a dispute with a business partner. Not keeping up with an industry standard also puts the organization at greater risk for a data breach. Should a data breach occur, it leaves the organization with a less legally-defensible position if the company is pulled into court.

Organizations need to set the threshold high enough to guard against the current threat level. Compliance does not equal security and being compliant does not eliminate risk. Doing the bare minimum to meet compliance requirements will be setting a threshold for security controls that is more than likely going to be "behind-the-times."

When dealing with multiple regulations, one approach is to set the threshold based on the strictest regulation. As other jurisdictions issue requirements to match, the organization will already be covered. For example, Massachusetts' new encryption requirements call for 128-bit encryption when personal

information regarding Massachusetts residents is transmitted. Many organizations are implementing these types of encryption controls not only for data pertaining to Massachusetts residents, but also for residents of other states. Some organizations are setting this threshold globally. Other organizations make these encryption controls available globally as a service to be used at the discretion of business units. Where the organization sets the threshold depends on their risk assessment and business objectives.

4. Streamline and automate compliance processes

ORGANIZATIONS ARE INCREASINGLY CALLED UPON to prove compliance to regulators, internal and external auditors as well as customers and business partners. How do organizations prove compliance? Essentially by proving that information security controls exist and that they are effective. This involves:

- Documenting the compliance program, including policies and processes;
- Monitoring, measuring and testing the security controls;
- Collecting all of the data on the controls; and
- Generating reports on the controls with respect to the requirements of regulations and standards and in the context of the organization's risk decisions.

Filling out self-assessment questionnaires is a common way to demonstrate compliance. Another is to have an auditor come on site to read documentation; actually look inside applications and networks; and possibly test controls. Whatever the method, for most organizations today, even those with relatively mature compliance programs, it is a huge, time-consuming and labor-intensive task to maintain the documentation, collect the data and create the reports.

And costs continue to rise as the compliance landscape gets more complex and organizations are subject to a growing number of requests to prove compliance. Typically as a compliance program matures, organizations aim for creating efficiencies, streamlining processes and using more automated

> *"To provide evidence of compliance for all of the regulations, it's the same data pool. It's the same information about your controls; you just have to produce different reports for different regulators. It makes sense to combine your efforts for compliance, security and risk. Not only is that approach more efficient, the outputs will also be of higher quality due to cross pollination."*
>
> DR. MARTIJN DEKKER, Senior Vice President, Chief Information Security Officer, ABN Amro

methods. At present most organizations still struggle with manual efforts. Moving to more automated methods can help not only reduce costs, but also increase consistency in reporting.

Automation involves multiple stages. It often begins by replacing disparate spreadsheets, file shares and binders with a content management system. A central repository is used for:

- Policies
- Regulatory requirements
- Enterprise control framework
- Control testing processes
- Inventory of assets with classification
  - *Mapped to organizational structure (i.e. asset owners, business process owners)*
  - *Possibly including third-party systems*
- Risk assessments
- Self-assessment questionnaires
- Audit results and remediation plans

The next stage is adding a work flow engine to develop and maintain the content; including approvals and escalation. The objective is to have an integrated view of all this information so you can look at and manage your governance, risk management and compliance program in a holistic way.

This approach requires investment in training in order to ensure data quality. Staff members who are required to input information into the system should understand the rigor required for data quality. Careful planning is also necessary to keep the management load to a minimum. Developing or deploying a technology solution will only save time if in conjunction, organizations think through all of the various processes involved in substantiating compliance and develop a plan to streamline them. Understand what can be automated and what will still require human intervention.

Often the vision for the third stage is to automate data collection and report generation. The goal is to answer questions via automatic system queries rather than have application owners manually input the information. For example, consider the question — "Have access rights for terminated employees been removed from the system?" In this case, a list of terminated employees would be checked against a database of access rights and a report automatically generated.

Achieving a level of automation whereby all the necessary data is harvested through system queries to produce a specific metric that demonstrates compliance is a massive data integration, correlation and business intelligence problem. Ultimately the objective is "continuous controls compliance" — continuously monitoring effectiveness of controls and highlighting compliance exceptions. It is often a multi-year project to get to this kind of "hands-off" automation of control validation and the majority of organizations have not attained this level yet. In a recent survey, only 36 percent of organizations had deployed a solution for continuous monitoring of security controls.[43] But many are working towards it, with the expectation that investments in automation will help reduce costs and improve compliance posture over the course of the long term.

The approach to automation depends on the organization's needs. Some opt to build their own custom-designed solution while others turn to an off-the-shelf "Enterprise Governance, Risk and Compliance" (eGRC) platform. This platform ties into enterprise applications and infrastructure, consolidating all of the information necessary to manage risk and compliance. For many organizations, the objective of an eGRC deployment goes beyond managing risk and compliance related to information protection. An eGRC platform can help integrate information from all of the various risk and regulatory domains to provide a complete picture of risk and compliance across the entire enterprise.

By providing a "CISO dashboard" and creating quarterly reports that go out to business units on the status of security, an eGRC platform can deliver the kind of visibility into compliance that is needed for the business to take ownership. Ideally, implementing eGRC technology can help provide a common methodology, thought process and language for all compliance stakeholders.

One of the challenges of automated data collection will be interoperability across different applications and platforms. Taking data feeds in from a huge number and variety of systems is a tall order. All the data formats from all of the various feeds have to be readable by the eGRC platform and consumed and presented in a useful format. Open standards might help solve some of these issues.

Implementing an eGRC platform, either through a custom-built or an off-the-shelf solution, will need to done be in multiple steps. Given the number of systems that need to feed into an eGRC platform, it is typically not feasible to integrate every individual data source. Standard middleware is often required which allows feeds from a whole series of systems like security management, configuration management, privilege management and access control systems, etc.

For a single information asset, there may be 20 controls; an organization can start by automating one or two of them and then automate more over time. Another approach is to look at the common sets of requirements that run across all regulations and business needs, such as identity and access management. Implement automation for one set of requirements then the next.

Today there is still no "plug-and-play" eGRC tech-

"YOU NEED *a whole process set up for evaluating vendors. In every organization, business units are contracting out data processing to service providers all of the time. So it's very hard to keep track of it all. You have to work with your purchasing department and put a system in place to ensure that you know which vendors are getting customer information."*

DAVE CULLINANE, Chief Information Security Officer and Vice President, eBay

nology; solutions must be customized and tailored to an organization's business processes. However, commercial solutions are available that provide out-of-the-box policies and workflows mapped to specific regulations so that organizations don't have to start from scratch. Over time eGRC technology will continue to evolve, possibly making integration easier and masking the complexity. One route the technology may take is vertical industry-based toolsets which build in functionality for the specific business processes of a particular sector. Another is appliances which cover multiple functions in one device such as appliances for unified threat management. It should be noted that even as the technology evolves, compliance will never be completely automated simply because people will always be involved at some level of decision-making.

5. Fortify third-party risk management

WITH REGULATIONS AROUND THE WORLD EXTENDing responsibility for the security of data across the value chain, organizations need to develop a solid third-party strategy for mitigating risks throughout the extended enterprise. A common approach in the past has been to develop "boilerplate" security requirements for service provider contracts and leave it at that. But given the increased risk, enterprises can no longer rely solely on agreements and contracts and must take a more active role in verifying that their partner's capabilities are up to the required standards.

A comprehensive third-party strategy would include the following components:

Diversification

- Using multiple service providers to handle different aspects of a business process
- Not giving all the data to one service provider to process

Due Diligence

- Taking a potential partner through an extensive review, with an on-site audit and rigorous line of questioning regarding security policy, architecture and controls
- Possibly have the on-site audit done by an expert third-party assessor
- Possibly require certifications like ISO 27001/2 or SAS 70

Thorough contractual agreement

- Detailed requirements for meeting regulatory compliance and reaching a certain standard with respect to security controls
- Reporting requirements
- Contracts contain "right to audit" clause
- Contractual indemnification — liabilities if there is a data breach
- Breach notification requirements and process
- Incident management procedures

Consequence management

- Extending disciplinary processes into partner's organization

Governance including regular reviews and surprise audits

- Service providers should be regularly audited; how often and how deep into the infrastructure the customer's examination will go should be discussed during contract negotiations

Sharing information on security with business partners is paramount to a successful relationship. On the one hand, service providers are reluctant to reveal detailed information about their security policies and procedures because this information may be misused. On the other hand, data owners cannot rely on imprecise descriptions of security measures from service providers. Achieving an appropriate balance is crucial.

It is important for enterprises in both positions (as data owners and/or service providers) to find an effective way to ensure that their contractual relationships satisfy the required regulations. For managing service providers, organizations should consider creating a "community of practitioners," with a goal of creating consistent practices across the whole extended enterprise. For performing assessments, an alternative is the retention of reputable independent auditors to analyze service provider security practices. As the number of service providers continues to climb for most enterprises, at a certain point having an internal team do all of the required assessments may no longer be sustainable.

A challenge faced by many organizations is that service providers are often contracted outside of the standard purchasing process — for example a busi-

ness unit sends employee data to an HR outsourcing company without going through the standard process. With the expanded regulatory requirements for service providers, security officers will now have the added weight of compliance to help create more awareness and oversight capability for those stray systems that were previously outsourced without proper information security assessments. This may ultimately reduce risks.

Managing cloud service providers

Adoption of cloud services has begun, albeit initially primarily for non-regulated data processing. However, cloud computing offers an attractive business and operational proposition for companies to process large volumes of data, including regulated data. Many companies are aiming to use cloud services even for data subject to compliance obligations.

As a "new" member of the portfolio of third-party providers, organizations need to put cloud providers through the same rigorous due diligence and auditing strategies described above. In addition, they will need to deconstruct the architecture around who's responsible for data, maintenance, access, privileged use, etc. to determine how many layers on which to conduct due diligence.

On their end, cloud providers will need to establish processes and controls that generate legal and regulatory confidence. Ideally they need an "attestation" process that proves they have the right controls in place. The Trusted Cloud Initiative (within Cloud Security Alliance) is creating a reference architecture to enable cloud vendors to have an outside auditor attest to the fitness of their controls (similar to a SAS70 type of certification for a cloud service provider).

Many other initiatives are aimed at solving the cloud assurance problem. "A6", which stands for Automated Audit, Assertion, Assessment, and Assurance API, also known as CloudAudit, is led by Cisco. The Common Assurance Maturity Model (CAMM) is a 24-member consortium of mostly vendors which also includes the European Network and Information Security Agency (ENISA). The Federal Risk and Authorization Management Program (FedRAMP) is co-chaired by NIST. It intends to provide joint authorizations and continuous security monitoring of shared IT services for federal departments and agencies that enter contracts with outside providers. [44]

The lack of a consistent way to assess IT service providers has been a problem for at least a decade. The cloud may force the whole industry to solve this problem. As more and more companies move to a common set of cloud service providers, shared accreditation will be an obvious requirement.

There are interesting possibilities for approaching a "compliant cloud." One possible model, based on market acceptance, will see cloud providers proactively invest in the ability to host large volumes of data with specific controls and assurance to meet a particular regulation. This model is already emerging, with clouds such as the recent introduction of Google's FISMA compliant cloud for the federal government.[45] Other such clouds, like a "HIPAA cloud", etc, may follow.

Another developing model is a "hybrid" or "multi-zone" environment, in which sensitive data will reside within the customer's physical premises or under contractual control in a hosted separate datacenter, while non-critical data will reside where there is the lowest-cost capacity. Another route that many organizations are taking is using a "private cloud" model which gives control over where the data will travel within the enterprise datacenter.

Security organizations need to work closely with their cloud providers and adopt a cloud model that matches the organization's risk profile. They need to incorporate cloud providers into their third-party management strategies to mitigate the risk of the extended enterprise.

6. Unify the compliance and business agendas

IN THE PAST, COMPLIANCE WAS OFTEN SEEN AS the security and compliance teams' responsibly and it was an isolated function. Now a fundamental shift is taking place in many organizations. Compliance is increasingly recognized as an essential component of doing business.

More and more, compliance teams are being invited to the table at the start of a project. Compliance

> *"We need an open-standards way for cloud computing providers to measure their controls. The idea is for the providers to measure how well they are complying against certain requirements and then display the results publicly on their websites. This could eventually reduce the need to measure those particular controls."*
>
> PETRI KUIVALA, Chief Information Security Officer, Nokia

"COMPLIANCE REQUIRES *an organization to establish a cultural change. People themselves should be able to distinguish compliant behavior and incompliant behavior. Compliance will always be there. There will always be regulation. It's not an incident that you can just react to and then it's gone. Compliance should be considered part of doing business-as-usual."*

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

is more often integrated into business innovation processes early on, for example when a business begins an M&A due diligence. Business process owners are recognizing that compliance should be dealt with in the same way as other business risks; up front and not at the 11th hour, in order to ensure proper assessment, planning and funding.

Organizationally, having a compliance function within each business unit is crucial to aligning compliance to business. The responsibility for compliance should not rest solely within the information security and compliance departments; it should be moved out to the business-line and division mangers. With the right check and balance structure, the corporate compliance group establishes the standards; while the business units, which have profit and loss responsibility, implement the standards. This way the right trade-offs can be made between the business needs and the enterprise legal risks.

A central feature of a relatively mature compliance program is a corporate risk or compliance committee made up the Head of Compliance, the General Counsel, Chief Security Officer (or Risk Officer), Chief Auditor, and the Controller's Office. This group often reports to the Head of Finance or the Chief Administrative Officer. This committee manages risk and compliance issues across the enterprise in the context of business strategy.

Besides the right organizational structure, to embed compliance into the business you also need everyone in the enterprise at every level — from executives to staff members and contractors — to fully understand their role in compliance. The challenge is that the topic of compliance is so huge; there are so many regulations and it's a complex landscape. It is not feasible to have everyone read and understand all the laws. Find ways to ensure people know a sufficient amount. Then focus on creating processes for them to follow that have compliance built-in. Compliance should just be part by-product of people following procedures, acting in a professional manner and doing their jobs properly. For example, HR managers should understand that they an important role in compliance by conscientiously keeping the HR database up to date.

Although compliance creates challenges many organizations have found that it can also provide benefits. The goal of compliance initiatives is improved information practices; but the end result can often also deliver improved IT operations and business processes. For example, without the urging of regulations, many organizations would not have adopted better systems to manage identity and access management or patch management. Now organizations can reap the benefits of efficient on-boarding and off-boarding of employees and contractors; and more reliable IT systems.

7. Educate and influence regulators and standards bodies

IT IS WIDELY RECOGNIZED THAT ALTHOUGH REGULATORS for the most part have benign intentions as they develop and fine tune the rules, they don't understand the "real world" environment and the complexity of implementation. After a decade of experience complying with information protection regulations, organizations have a wealth of knowledge of what works and what is not effective. It is critical that security leaders are part of the conversation as a whole host of new legislation regarding identity theft, privacy and critical infrastructure is entering the scene (SEE TABLE 10).

Security and business leaders need to develop credible ways to educate legislators and constructively affect regulation. Internally they need to work closely with the Government Affairs function and join forces with them. Externally they need to participate in groups like TechAmerica's information security council, which gives companies an opportunity to provide insight into legislation. •

TABLE 10: **EXAMPLES OF CURRENT LEGISLATIVE INITIATIVES**

National Strategy for Trusted Identities in Cyberspace 2010
Data Security Act of 2010
Data Security and Breach Notification Act of 2010
The Protecting Cyberspace as a National Asset Act of 2010
2010 Dodd-Frank Wall Street Reform and Consumer Protection Act
2010 European Union Reference Network for Critical Infrastructure Protection (ERN-CIP)
2010 European Union Digital Single Market Initiative
2010 European Union Solvency II Directive

5 Conclusion

Get it right and reap the rewards

A successful compliance program in a large global enterprise today takes a holistic approach to meeting the requirements of multiple regulations. A successful program embeds compliance in business processes. It uses automation as much as possible; and has the risk management competency to make defensible decisions about materiality of risk. Leveraging continuous compliance monitoring technologies will allow organizations to reduce the amount they spend demonstrating compliance. This will enable organizations to reduce their overall security investment and/or focus it on more value-added information security services.

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.

"ON BALANCE *I don't think compliance hinders innovation. Compliance just changes the game a bit. It offers an opportunity to innovate in a new more compliant space. It offers new challenges to do what we do more securely."*

DENISE WOOD, Chief Information Security Officer and Corporate Vice President, FedEx Corporation

"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.

6 Appendices

About 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 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. 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.

RSA has 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 conducting a series of in-depth interviews with the Council, publishing their ideas in a series of reports and sponsoring independent research that explores this topic. RSA invites you to join the conversation. Go to **www.rsa.com/securityforinnovation/** to view the reports or access the research. Provide comments on the reports and contribute your own ideas. Together we can accelerate this critical industry transformation.

BUSINESS INNOVATION DEFINED

Enterprise strategies to enter new markets, launch new products or services, create new business models, establish new channels or partnerships, or transform operations

Security for Business Innovation Report Series

Go to www.rsa.com/securityforinnovation

The Time is Now: Making Information Security Strategic to Business Innovation
Recommendations from Global 1000 Executives

Mastering the Risk/Reward Equation: Optimizing Information Risks to Maximize Business Innovation Rewards
Recommendations from Global 1000 Executives

Driving Fast and Forward: Managing Information Security for Strategic Advantage in a Tough Economy
Recommendations from Global 1000 Executives

Charting the Path: Enabling the "Hyper-Extended" Enterprise in the Face of Unprecedented Risk
Recommendations from Global 1000 Executives

Bridging the CISO-CEO Divide
Recommendations from Global 1000 Executives

The Rise of User-driven IT: Re-calibrating Information Security for Choice Computing
Recommendations from Global 1000 Executives

Contributors

Top information security leaders from Global

ANISH BHIMANI, CISSP, Chief Information Risk Officer, **JPMORGAN CHASE**

ANISH HAS *global responsibility for ensuring the security and resiliency of JPMorgan Chase's IT infrastructure and supports the firm's Corporate Risk Management program. Previously, he held senior roles at Booz Allen Hamilton and Global Integrity Corporation and Predictive Systems. Anish was selected "Information Security Executive of the Year for 2008" by the Executive Alliance and named to Bank Technology News' "Top Innovators of 2008" list. He authored "Internet Security for Business" and is a graduate of Brown and Carnegie-Mellon Universities.*

BILL BONI, CISM, CPP, CISA, Corporate Information Security Officer, VP Enterprise Information Security, **T-MOBILE USA**

AN INFORMATION *protection specialist for 30 years, Bill joined T-Mobile in 2009. Previously he was Corporate Security Officer of Motorola Asset Protection Services. Throughout his career Bill has helped organizations design and implement cost-effective programs to protect both tangible and intangible assets. He pioneered the application of computer forensics and intrusion detection to deal with incidents directed against electronic business systems. Bill was awarded CSO Magazine's "Compass Award" and "Information Security Executive of the Year – Central" in 2007.*

ROLAND CLOUTIER, Vice President,Chief Security Officer, **AUTOMATIC DATA PROCESSING, INC.**

ROLAND HAS *functional and operational responsibility for ADP's information, risk and crisis management; and investigative security operations worldwide. Previously, he was CSO at EMC andheld executive positions with consulting and managed services firms. He has significant experience in government and law enforcement, having served in the U.S. Air Force during the Gulf War and later in federal law enforcement agencies. Roland is a member of High Tech Crime Investigations Association, State Department Partnership for Critical Infrastructure Security and Infragard.Universities.*

DAVE CULLINANE, Chief Information Security Officer and Vice President, **EBAY**

DAVE HAS *more than 30 years of security experience. Prior to joining eBay, Dave was the CISO for Washington Mutual and held leadership positions in security at nCipher, Sun Life and Digital Equipment Corporation.Dave is involved with many industry associations including as current Past International President of ISSA. He has numerous awards including SC Magazine's Global Award as CSO of the Year for 2005 and CSO Magazine's 2006 Compass Award as a "Visionary Leader of the Security Profession."*

PETRI KUIVALA, Chief Information Security Officer, **NOKIA**

PETRI HAS *been CISO at Nokia since 2009. Previously he led Corporate Security operations globally and prior to that in China. Since joining Nokia in 2001, he has also worked for Nokia's IT Application Development organization and on the Nokia Siemens Networks merger project. Before Nokia, Petri worked with the Helsinki Police department beginning in 1992 and was a founding member of the Helsinki Criminal Police IT- investigation department. He holds a degree in Masters of Law.*

DAVE MARTIN, CISSP Chief Security Officer, **EMC CORPORATION**

DAVE IS *responsible for managing EMC's industry-leading Global Security Organization (GSO) focused on protecting the company's multibillion dollar assets and revenue. Previously, he led EMC's Office of Information Security, responsible for protecting the global digital enterprise. Prior to joining EMC in 2004 Dave built and led security consulting organizations focused on critical infrastructure, technology, banking and healthcare verticals. He holds a B.S. in Manufacturing Systems Engineering from the University of Hertfordshire in the U.K.*

FELIX MOHAN, Senior Vice President, CISO & Chief Architect, **BHARTI AIRTEL LTD**

AT AIRTEL, *Felix ensures information security and IT aligns with changes to the risk environment and business needs. Previously he was CEO at a security consulting firm, an advisor with a Big-4 consulting firm, and head of IT and security in the Indian Navy. He was a member of India's National Task Force on Information Security, Co-chair of the Indo-US Cybersecurity Forum, and awarded the Vishisht Seva Medal by the President of India for innovative work in Information Security.*

DR. CLAUDIA NATANSON, Chief Information Security Officer, **DIAGEO**

CLAUDIA SETS *the strategy, policy and processes for information security across Diageo's global and divergent markets. Previously, she was Head of Secure Business Service at British Telecom, where she founded the UK's first commercial globally accredited Computer Emergency Response Team. Claudia is Chair of the Corporate Executive Programme of the World Forum of Incident Response and Security Teams. She holds an MSc. in Computer Science and a Ph.D. in Computers and Education.*

1000 enterprises

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

MARTIJN WAS *appointed Chief Information Security Officer of ABN Amro in early 2010. Previously he held several positions in information security and IT including Head of Information Security and Head of Technology Risk Management in the Netherlands. Other positions included IT Architect, Program/Portfolio Manager, and IT Outsourcing/Offshoring Specialist. Martijn joined ABN Amro in 1997 after completing his Ph.D. in Mathematics at the University of Amsterdam and a Masters of Mathematics at the University of Utrecht.*

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

PAUL IS *engaged in consultancy,training and research to help vendors, end-user companies and governments in developing their security strategies. Before founding CSO Confidential, Paul was responsible for IT Security and Information and Records Management at BP. Previously, he ran security and risk management at Morgan Grenfell and Barclays Bank. Paul was a founder of the Jericho Forum, is Chairman of the Institute of Information Security Professionals and a Visiting Professor at Royal Holloway College, University of London.*

RENEE GUTTMANN,
Vice President, Information Security & Privacy Officer, **TIME WARNER INC.**

RENEE IS *responsible for establishing an information risk management program that advances Time Warner's business strategies for data protection. She has been an information security practitioner since 1996. Previously, she led the Information Security Team at Time Inc., was a security analyst for Gartner and worked in information security at Capital One and Glaxo Wellcome. Renee received the 2008 Compass Award from CSO Magazine and in 2007 was named a "Woman of Influence" by the Executive Women's Forum.*

DAVID KENT,
Vice President, Global Risk and Business Resources, **GENZYME**

DAVID IS *responsible for the design and management of Genzyme's business-aligned global security program, which provides Physical, Information, IT and Product Security along with Business Continuity and Crisis Management. Previously, he was with Bolt Beranek and Newman Inc. David has 25 years of experience aligning security with business goals. He received CSO Magazine's 2006 "Compass Award" for visionary leadership in the Security Field. David holds a Master's degree in Management and a Bachelor of Science in Criminal Justice.*

{ GUEST CONTRIBUTOR

STEWART ROOM,
Partner, Privacy and Information Law Group, **FIELD FISHER WATERHOUSE**

WITH 19 *years experience as a litigator and advocate, Stewart is a recognized expert in data protection; ranked at the forefront of this field by the legal directories Chambers UK and Legal 500. He is also President of the National Association of Data Protection Officers and a Director of Cyber Security Challenge UK. Stewart was Financial Times Legal Innovator of the Year 2008 and is the author of several books including his latest Data Security Law and Practice.*

VISHAL SALVI, CISM
Chief Information Security Officer and Senior Vice President, **HDFC BANK LIMITED**

VISHAL IS *responsible for driving the Information Security strategy and its implementation across HDFC Bank and its subsidiaries. Prior to HDFC he headed Global Operational Information Security for Standard Chartered Bank (SCB) where he also worked in IT Service Delivery, Governance & Risk Management. Previously, Vishal worked at Crompton Greaves, Development Credit Bank and Global Trust Bank. He holds a Bachelors of Engineering degree in Computers and a Masters in Business Administration in Finance from NMIMS University.*

CRAIG SHUMARD,
Chief Information Security Officer, **CIGNA CORPORATION**

CRAIG IS *responsible for corporatewide information protection at CIGNA. He received the 2005 Information Security Executive of the Year Tri-State Award and under his leadership CIGNA was ranked first in IT Security in the 2006 Information Week 500. A recognized thought leader, he has been featured in The Wall Street Journal and InformationWeek. Previously, Craig held many positions at CIGNA including Assistant VP of International Systems and Year 2000 Audit Director. He is a graduate of Bethany College.*

DENISE WOOD,
Chief Information Security Officer and Corporate Vice President, **FEDEX CORPORATION**

DENISE IS *responsible for security and business continuity strategies, processes and technologies that secure FedEx as a trusted business partner. Since joining in 1984 she has held several Information Technology officer positions supporting key corporate initiatives, including development of fedex.com; and was the first Chief Information Officer for FedEx Asia Pacific in 1995. Prior to FedEx, Denise worked for Bell South, AT&T and U.S. West. Denise was a recipient of Computerworld's"Premier 100 IT Leaders for 2007" award.*

References

1 "Outpacing Change", Ernst & Young's 12th Annual Global Information Security Survey Report

2 "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

3 "Commission defends data protection review timetable", The Register, August 10, 2010

4 "Data Protection in the European Union: the role of National Data Protection Authorities", FRA European Union Agency for Fundamental Rights, 2010

5 "Germany Strengthens Data Protection Act, Introduces Data Breach Notification Requirement", Jones Day, Oct 2009

6 "Firms unprepared for new ICO powers", V3.co.uk, April 4, 2010

7 "French Senate's proposed Bill to amend Data Protection Act", dataprotectionlaw&policy, Feb 2, 2010

8 "United States: HIPAA Privacy, Security, and Enforcement Rules Modified Under the HITECH Act", Mondaq, July 20, 2010

9 "Connecticut Attorney General Reaches First State HIPAA Settlement with Health Net", Security, Privacy & the Law, July 7, 2010

10 What is NERC CIP, and IT's role in critical infrastructure protection?", SearchCompliance.com

11 "Twitter, FTC settle on charges of data security lapses", InfoSecurity.com, June 24, 2010

12 "Rite Aid Settles FTC Case", WSJ, July 27, 2010

13 "FTC Testifies on Efforts to Protect Consumer Privacy", Smart-Grid, July 28, 2010

14 "PCI DSS requirements still baffling as compliance deadline approaches", SearchSecurity.co.UK, March 8, 2010

15 "Exclusive PCI DSS news: EU regional director rallies UK merchants", SearchSecurity.co.UK, July 9, 2010

16 "European Commission passes new e-Privacy Directive requiring mandatory data breach notification by public communications providers", Lexicology, February, 2010

17 "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

18 "Guidance on data security breach management", ICO, March 27, 2008

19 "Germany Strengthens Data Protection Act, Introduces Data Breach Notification Requirement", Jones Day, October 2009

20 "New data breach notification duty introduced in the 2010 Amendment to the Data Protection Act", Preslmayr Rechtsanwa Lte., March 2010

21 "French Senate's proposed Bill to amend Data Protection Act", dataprotectionlaw&policy, Feb 2, 2010

22 "Irish Data Protection Commissioner introduces draft code of practice on breach notification", SC Magazine, June 10, 2010

23 "Canada's newly introduced data breach law is a start, but it lacks teeth", SC Magazine

24 "Mexico passes new law aimed at data-leak prevention for individuals and private companies", Security & Compliance News, July 19, 2010

25 "Privacy Commissioner Publishes Guidance Note on Data Breach Handling and the Giving of Breach Notifications", Privacy Commissioner for Personal Data (PCPD) Hong Kong Media Statement, June 21, 2010

26 "500 Million Sensitive Records Breached Since 2005", Privacy Rights Clearinghouse, August 26, 2010

27 "FAQ on Washington State's PCI Law", INFORMATIONLAWGROUP, March 24, 2010

28 "New Jersey Publishes Pre-Proposal of Rules Protecting Personal Information", Privacy & Data Security Law Journal, April 2009

29 "Enterprises Should Beware the Pitfalls of Compliance with the Massachusetts Information Security Regulations", Hogan Lovells Chronicles of Data Protection, March 2, 2010

30 "United States: HIPAA Privacy, Security, and Enforcement Rules Modified Under the HITECH Act", Mondaq, July 20, 2010

31 "FTC Consent Decree Alleges Mortgage Lender Failed to Ensure the Data Protection of Consumer Information Provided to a Third Party", Global Financial Market Watch Blog, January 28, 2009

32 "Cloud computing may violate German data privacy laws", Lexology, July 20, 2010

33 "Outpacing Change", Ernst & Young's 12th Annual Global Information Security Survey Report

34 "Outpacing Change", Ernst & Young's 12th Annual Global Information Security Survey Report

35 "Visa cuts CardSystems over security breach", The Register, July 19, 2005

36 "Ponemon Study Shows the Cost of a Data Breach Continues to Increase", Ponemon Institute, January 25, 2010

37 "Infosecurity Europe 2010: Survey says US boasts highest data breach costs", InfoSecurity, April 28, 2010

38 "Outsourcing 2010: Summary of Findings from IAOP's State of the Industry Survey", IAOP Accenture Report

39 "TPI Index — An Informed View of the State of the Commercial Outsourcing Market — Second Quarter 2010", TPI, July 26, 2010

40 "Enterprises Ready to Turn to Cloud E-Mail", CIO, August 18, 2010

41 "Google-City of Los Angeles deal delayed", American Public Media Marketplace, July 26, 2010

42 "Mastering the Risk/Reward Equation: Optimizing Information Risks to Maximize Business Innovation Rewards", Security for Business Innovation Council Report

43 "Outpacing Change", Ernst & Young's 12th Annual Global Information Security Survey Report

44 "Cloud computing risks and how to manage them Issue", Information Security Magazine, June 2010

45 "Google Receives FISMA Certification for Cloud Services", ExecutiveGov, July 27, 2010

Quotable *Highlights from the ongoing conversation*

Bill Boni, Corporate Information Security Officer, VP Enterprise Information Security, T-Mobile USA

"WE HAVE *a legal and regulatory system that is accustomed to things like physical presence and visible control. For cloud-based solutions, developing equivalent levels of confidence within legal and regulatory bodies is going to be challenging. The providers of new cloud solutions have to embrace the level of rigor required by regulation and need to better understand what auditors are asking them in order to demonstrate compliance."*

Dave Cullinane, Chief Information Security Officer and Vice President, eBay

"YOU NEED *a broad perspective of all of the various legislation in the US and elsewhere. Legislators and people in Congress don't often understand the nuances of things like identity theft. They might pass all sorts of legislation that's actually not going to reduce identity theft but just create a whole bunch of requirements. It's important for security officers to be participating in that conversation and provide insight into draft legislation."*

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

"THE FACT *that the compliance issues extend along the supply chain means that people are becoming very sensitized to the compliance implications of using third parties. It actually restricts certain third parties from being suppliers, because they can't reach the high compliance threshold required of the end-customer company."*

"YOU NEED *a process that substantiates your decisions to the auditor. You need complete and defensible clarity about the risk decisions you've taken. A good compliance team is therefore able to fully articulate the issues to create a defensible position."*

Petri Kuivala, Chief Information Security Officer, Nokia

"IF YOU *have implemented your security procedures by following for example, the ISF Standard of Good Practice or some other common methodology, whenever there is a question with regards to whatever new law, you can answer that question based on your current approach."*

Dave Martin, Chief Security Officer, EMC Corporation

"CONTINUOUS CONTROL *monitoring is going to become vital in cloud-based datacenters. It'll be essential for putting regulated data in the cloud. Stuff's going to be moving around. You're going to need the ability to constantly make sure that your regulated data is in the right place with the right controls."*

"YOU DEVELOP *effective controls by working with the business, understanding the details of the process and building in compliance instead of bolting it on. But the process owners have to have a willingness to improve their process to ensure compliance. Make sure they've got some skin in the game."*

Felix Mohan, Senior Vice President, CISO & Chief Architect, Bharti Airtel Ltd.

"THERE ARE *many regulations and internal policies; and these will keep increasing. If you look at them closely, they are all basically addressing a similar set of risks. Put in place a framework based on best practices like ISO 27001/2 to address the risks and you can map your framework to any new regulation that comes along."*

Dr. Claudia Natanson, Chief Information Security Officer, Diageo

"AN ORGANIZATION *will never, ever achieve compliance unless the "I" is part of it. So every person in the organization must know the part they must play to be able to achieve true compliance."*

Stewart Room, Partner, Privacy and Information Law Group, Field Fisher Waterhouse LLP

"THERE WILL *be commercial contracting consequences that flow from you being named, shamed and 'outed' for bad data handling. Organizations might seek tighter indemnities from you or they might refuse to work with you."*

Vishal Salvi, Chief Information Security Officer and Senior Vice President, HDFC Bank Limited

"REGULATION HAS *been a primary driver for the implementation of information risk management and it has made a significant impact. For example if you look at the various sectors that are highly regulated — like financial services or telcos — their security practices are more mature than those in general industry."*

Craig Shumard, Chief Information Security Officer, CIGNA Corporation

"THE IMPACT *of HITECH is just beginning to be felt. For example outsourcers have really gotten a wake-up call in the last year. They've started to realize the impact the extension of the business associate in HIPAA is going to have on their business."*

"FROM A *business standpoint for example, protecting our customers' identities is important to us. Protecting our business pricing information is important to us. There are a lot of corporate objectives that are also met with the security controls that get put in place to satisfy the regulations."*

Successfully building a risk-based compliance program requires that executive management is willing to make the necessary investments in people, process and technology.

"IT'S NOT *enough to hold people responsible for compliance; you need to make them truly accountable. To do this you need visibility into the controls through real-time monitoring. You need to go from asking people to show you that their systems are compliant at a point-in-time to proactive alerting of compliance gaps in real-time."*

DAVE MARTIN, Chief Security Officer, EMC Corporation

RSA®
The Security Division of EMC