Realtime publishers

The Shortcut Guide™ To

Understanding Data Protection from Four Critical Perspectives

sponsored by

CREDANT®

We Protect What Matters

Rebecca Herold

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Introduction to Realtime Publishers i
Chapter 1: What Corporate Business Leaders Need To Know About Data Protection 1
The Importance of Data Protection to Business 2
The Information Security Triad 3
Breaches Are Going to Happen 5
Technology Advances Bring New Information Protection Risks 6
Cloud Computing 6
Mobile Computing 8
Social Networking Technologies 9
Video Meetings and VoIP 11
The List Is Ever-Growing 11
Bad Economic Times Breeds Bad Security 12
Increasing Crimes 13
Increasing Mobility 14
Security Protections and Funding Reduced 15
The Impact of Information Security Incidents and Privacy Breaches to the Business 17
Case Studies 20
Cost of Responding to Breaches 20
ATM Break-In 21
Lose Clear Text PII, Get a Fine 22
Key Business Leader Information Protection Responsibilities 23
#1 Provide Visible Support for Information Security Initiatives 23
#2 Make Personnel Responsible for Protecting Information 25
A Culture of Security Protects the Business 25

Copyright Statement

Chapter 1: What Corporate Business Leaders Need To Know About Data Protection

If handling complex and difficult information protection requirements and issues is not at the top of the priority list for companies maintaining customer and employee information, it should be moving there. Unfortunately, the viewpoints of information protection and the associated issues and activities that are necessary within a business enterprise are often drastically different from area to area.

Why this propensity for widely varied views of the role of information protection within business? There are many reasons. Generally, however, when addressing the many different information protection issues throughout a business enterprise, there are often gaps in communication and coordination activities between the primary information protection decision-making stakeholders throughout the organization, such as the legal and privacy office, the information security office, the auditing and compliance office, and the IT operations areas. These communication gaps create more complexity and bigger challenges for companies to handle and put the organization at greater risk for incidents as well as contractual and regulatory noncompliance.

Successful information protection programs require the viewpoints and goals for information protection within different stakeholder areas to be complementary and integrated throughout all the enterprise, within every business process stage, and at every level within the organization. This guide will provide discussion, practical knowledge, and numerous examples, facts, and case studies to address complex information protection convergence and compliance issues within your organization. The four chapters within this book will discuss the following:

- Chapter 1 explains why executive leaders must be concerned and take an active role in supporting information protection efforts. It also provides the information that CEOs, CFOs, and all other types of CxOs, in addition to lawyers, must know to help make the best possible decisions for information protection activities.

- Chapter 2 provides the information that compliance officers, auditors, and privacy officers need to understand and consider with regard to information protection to help them make the best decisions within their realm of responsibility.
- Chapter 3 helps information assurance professionals to better understand the information protection issues and challenges within information security departments and the associated technologies and activities.
- Chapter 4 speaks directly to IT leaders, IT administrators, developers, architects, and others who are the digital information custodians of the enterprise and responsible for implementing security controls but who usually have very little or limited information protection training or experience.

The Importance of Data Protection to Business

How much are your customers worth to your business? It's pretty safe to say that without them you would not have a business. If you lose the trust of your customers, you face losing them. If you lose your customers' personally identifiable information (PII), or bad things are done with your customers' PII that negatively impacts them, you will lose their trust and chances are pretty good that you will lose their business.

How much are your employees worth to your business? As the adage goes, one of the most important assets an organization has is its employees. What would happen if a breach occurred and your personnel's information was stolen or used for criminal activity? You would lose their trust and likely many of your employees.

Are you effectively protecting your business information assets along with your customers' and employees' PII? If not, your business is at significant risk, and so are you as a business leader. Stop and consider three questions:

- How does your organization protect business information assets, including confidential information and PII?
- Who has access to business information assets?
- Where are business information assets and all business confidential information and customer PII located?

If you cannot answer the previous questions, it is likely you will

- Experience an information security incident,
- Have a privacy breach, and
- Be in non-compliance with multiple laws and regulations.

Any one of these can be costly. All three can be catastrophic to your business. The risks to information, and to your business, are increasing every day.

Businesses are sharing more information than ever before, and they are also outsourcing more business information processing than ever before. This environment creates business risks that never before existed and for which business leaders never even had a need to think of as recent as 10, and even 2, years ago.

> **Note**
>
> A January 2009 Gartner study predicts outsourcing will continue to grow in 2009 despite economic slowdown, further highlighting the need for effective information protection practices.

Information and the associated information infrastructure are key business assets that are very valuable. The availability, integrity, and confidentiality of business information are critical for the continued success of your organization.

The Information Security Triad

CEOs and other executive business leaders must know and understand their industries, customers, current economy and economic outlook, along with their own organization's key operations to be able not only to survive but also to survive and be successful by having a clear and accurate understanding of their enterprise business health. Unfortunately, an often-overlooked component of enterprise health is information security and compliance. This shortcoming is typically attributed to a lack of awareness for what is necessary within an effective information assurance program. It is important for CEOs and other executive business leaders to know and understand that the long-held and accepted triad of necessary information security components is 1) confidentiality, 2) integrity, and 3) availability.

Confidentiality

Maintaining information confidentiality requires protecting information, in all forms, from unauthorized disclosure to those who do not have a business need or perhaps to a competitor or to the press. Confidentiality is not only a component of the security triad; it is also a requirement of numerous laws, regulations, industry standards, and growing numbers of contractual requirements.

For example, the Payment Card Industry (PCI) Data Security Standard (DSS) includes many directives to protect the wide range of business information from unauthorized disclosure. Just a couple of the specifics include "Requirement 4: Encrypt transmission of cardholder data across open, public networks" and "Requirement 7: Restrict access to cardholder data by business need to know" and (Source: PCI DSS at https://www.pcisecuritystandards.org/).

As another example, consider the trend for new legal requirements for businesses to encrypt PII. This trend is specifically to maintain the confidentiality of PII and prevent identity theft and other related crimes. Two states, Nevada and Massachusetts, have enacted laws requiring businesses to encrypt PII, and more states are poised to follow suit.

It is important to note and understand that these laws mandating encryption are in addition to the at least 47 US breach notice laws currently in effect. Breach notice laws provide the requirements that organizations must follow after a breach has occurred, but these new laws that include encryption requirements are aimed at preventing breaches from occurring in the first place.

Resources

Find the Nevada law, NRS 597.970, "Restrictions on transfer of personal information through electronic transmission,: at http://www.leg.state.nv.us/NRs/NRS-597.html#NRS597Sec970.

Find the Massachusetts law, "201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth" at http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf.

Find a list U.S. breach notice laws at http://www.privacyguidance.com/files/USStateandTerritoriesBreachNotificationLaws032209.pdf

Integrity

Maintaining information integrity requires businesses to protect information from unauthorized modification and to ensure information—such as a price list, customer information, and account details—is accurate and complete. Integrity is not only a component of the security triad; it is also a requirement of numerous laws, regulations, industry standards and growing numbers of contractual requirements. For example, one of the multiple integrity requirements within PCI DSS includes, section 11.5: "Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly." As another example, consider that multiple federal and international laws require businesses to have information safeguards in place to ensure integrity.

A major component of the European Union (EU) Data Protection Directive 95/46/EC is to maintain the integrity of PII. This is demonstrated by Article 6 item 1 (d), "Member States shall provide that personal data must be...accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified."

An example of just one of the many laws from the US that requires integrity is the Gramm-Leach-Bliley Act (GLBA) Standards for Safeguarding Customer Information (commonly referenced as the Safeguards Rule). One of the multiple integrity requirements within it includes the directive for businesses to "Protect against any anticipated threats or hazards to the security or integrity of "nonpublic personal information."

Resources

Find EU Data Protection Directive 95/46/EC at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

Find the GLBA Standards for Safeguarding Customer Information at http://www.ftc.gov/os/2002/05/67fr36585.pdf.

Availability

Maintaining availability means that businesses must ensure information is available when needed. Not unlike confidentiality and integrity, availability is also necessary to meet growing numbers of legal, regulatory, and industry standards and contractual requirements.

Once more considering the EU Data Protection Directive 95/46/EC, this minimum requirement law that is enforced throughout all the 28 EU member countries, requires that organizations with customer or employees in the EU must make available to any person on request the corresponding PII in a form appropriate to allow understanding. In addition, HIPAA has an entire section, § 164.524 "Access of individuals to protected health information" dedicated to addressing the need for organizations to make information available.

An effective enterprise information security framework that includes consideration of the security triad is a necessary component for business success and to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image and branding. Business leaders must understand this importance and clearly support information security program efforts to move the business forward.

Breaches Are Going to Happen

Increasingly, organizations and their information systems and networks are faced with information privacy and security threats from a wide range of sources such as criminals who want to commit identity theft, mistakes by personnel, accidents due to lack of knowledge and training, inappropriate business practices, computer-assisted fraud, sabotage, vandalism, fire or flood, just to name a few. Information protection risks such as email schemes, identity theft, fraud, and so on have become more common, more ambitious, and increasingly sophisticated. Organizations have increasing numbers of personnel performing business more often away from the office, while traveling or from within home-based offices, both of which create significant information protection risks that must be addressed. Additionally, the number of privacy-related laws and regulations continues to proliferate at exponential rates throughout the world.

Dependence on information systems, application services, and personnel knowledge of risk makes organizations more vulnerable to information privacy and security threats. Interconnecting public and private networks, the trend to use distributed computing and cloud computing, connections to business partners and third parties, and sharing information resources increases the difficulty of achieving adequate and acceptable information protection and access control.

The large number of laws requiring privacy and security activities can be overwhelming if there is not one person or area responsible for knowing, understanding, and addressing the requirements. Monitoring the laws is necessary to ensure compliance and to prevent being fined or undergoing legal action as a result of noncompliance.

So, could a privacy breach impact your organization? Many businesses have been significantly impacted by privacy breaches. The following examples highlight just a few of the privacy incidents and lawsuits that have occurred and impacted businesses recently.

Technology Advances Bring New Information Protection Risks

Technology evolves quickly, bringing new risks to business that creep into your business facilities and networks and are fully utilized before business leaders even realize it. Just stop for a moment and think about all the comparatively new technologies that exist and how many are being used within your business facilities and on your computer systems and networks. Some are being used for business and others are being used by your personnel for their own personal activities in ways that can put your business at significant risk. Consider just a few of these.

Cloud Computing

One of the most talked and written about trends in the past year is "cloud computing." Gartner predicts that 30 percent of consulting and systems integration revenue will be delivered using cloud computing by 2011.

> **Note**
>
> "Cloud computing" involves sharing and/or storing information on remote servers owned or operated by others and accessed through the Internet or other connections to networks outside of enterprise control. There are many types of cloud computing services, such as data storage sites, video sites, tax preparation sites, personal health record Web sites, photography Web sites, social networking sites, and many more.

A report issued by the World Privacy Forum on February 23, 2009, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing," warned that businesses and other organizations considering the use of cloud computing should be aware that cloud computing brings with it significant privacy concerns.

> **Resource**
>
> See the World Privacy Forum report at http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

Any information stored locally on a computer or within any enterprise server could also be stored in the cloud, including such things as email, word processing documents, spreadsheets, videos, music files, photos, health records, tax information, financial information, business plans, presentations, accounting information, advertising campaigns, sales numbers, appointment calendars, address books, and other types of proprietary information.

Even PII is being stored in clouds increasingly more often. What kind of information protection is being provided for this PII in the clouds? It's an important question, but unfortunately is not being asked nearly often enough before blindly dumping huge amounts of valuable data and PII into the clouds, trusting that the necessary information protections will just happen to exist in these silent business partners' networks.

But are those silent business partners securing their servers appropriately, and ensuring appropriate privacy protections to the vast amounts of PII that is being entrusted to them? Is there any need to worry? How does storing data on, and communicating via, clouds impacts compliance? These are all important questions to ask about an increasingly common business initiative to move huge amounts of business data to the clouds.

Resource

For more research and recommendations about cloud computing, see my December 2008 report "Cloudy Privacy Computing" at http://www.privacyguidance.com/files/HeroldCSIDecember2008AlertCloud_Computing.pdf.

In addition to addressing the privacy and information protection issues, business leaders must ensure that moving corporate information to the clouds is not a violation of applicable laws, regulations, industry standards, and contractual agreements. For example, GLBA generally allows financial organizations to share data with services providers. To share PII of customers, though, organizations must provide notice that their PII will be shared with others and then provide an opportunity to customers to deny such sharing. So, how does this apply to storing data within a cloud computing provider? Does notice of such storage need to be provided to customers? Arguably it does. However, this is an important point to ensure your corporate legal counsel provides informed advice about.

Many other laws and regulations also likely impact cloud computing decisions, such as the Fair Credit Reporting Act and its limitations on how credit data is handled, HIPAA and determining whether cloud computing use requires a business associate agreement, and most information protection laws outside of the US that require consent to share PII with other organizations.

> **Note**
> Many information protection laws throughout the world require consent to share PII with other organizations. Just a few of these include the EU Data Protection Directive 95/46/EC, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Australia's Privacy Act, and Japan's Act on Protection of Computer Processed Personal Data.

Mobile Computing

It is almost a given that businesses are now actively involved in mobile computing to support business functions in one or more ways.

> **Note**
> Mobile computing is basically 1) using mobile computers, such as laptops, Blackberrys, and other easily moved computers to perform business activities; 2) using mobile storage devices, such as USB thumb drives and DVDs, to store data and then carrying the devices outside of business facilities; and 3) doing business computing outside of business facilities, such as while traveling or from home offices.

At the beginning of February 2009, Google released software, Google Latitude, that allows folks who use mobile wireless devices to automatically and continually share their physical locations, along with an accompanying handy dandy map to make it even easier, with whomever they want to share with. This is not a new revelation; an application offered by the lesser-known Loopt company has been available for a while. Such a tool can provide great benefits when used appropriately. However, as with all great communications technologies, misused, this could also significantly create some major privacy problems.

There are three privacy issues at the core of using mobile wireless-enabled devices and tools of any kind beyond the previous two examples:

- Individuals basically give away PII when using mobile computing devices through lack of knowing how to use them in a safe and secure manner.
- Some organizations take advantage of the mobile wireless-enabled features without thinking through the privacy issues.
- Some organizations do not even think about the related information security, privacy, and compliance issues involved with allowing their personnel to use these devices for business purposes.

Stop and consider how many folks in your organization use wireless-enabled mobile computers. Do you know? You cannot effectively protect information if you do not know where it is located. If you do not know what mobile computing devices are being used within your organization, how can you effectively protect the PII that is stored upon them or accessed through them? And remember, once people start using new mobile computing devices, even if it is to "just test" them and not to use them for any "business work," chances are those devices will soon have business data and customer PII stored upon them.

How many people within your organization are using mobile computing devices? Considering how many people own mobile computing devices now, it is likely many of them are being used within your business.

> **Note**
>
> Apple sold 6.89 million iPhone units in Q3 2008, and 4.36 million units in Q4 2008.

It is important to realize that most mobile computing devices have the wireless feature enabled out of the package. Most folks using these devices will not even be aware that they have their wireless transmissions enabled. It is very possible that these wireless connections could be used to leak valuable PII, resulting in embarrassing and costly privacy breaches.

Organizations must establish strong information protection policies and procedures for the use of wireless-enabled mobile computing devices, providing targeted information security and privacy training for the folks who use them and ongoing awareness communications about safeguarding them.

Social Networking Technologies

Personnel increasingly want to use technology for personal reasons while they are at work, bringing risks into the office that must be addressed. As just one example, consider the use of Twitter. In 2008, Twitter leaped to the attention of Internet users and was adopted by staggering numbers of individuals. As of the end of February 2009, there were more than 4.5 million Twitter users according to the market-tracking firm HubSpot Inc. It projects there are 5000 to 10,000 new Twitter accounts created every day. Do you know when these accounts are heavily used? Yes, while at work. And many of the posted Twitter messages contain confidential company information; a possibly significant business information leak. Add to this all the other "Web 2.0" technologies, and business leaders truly have some important decisions to make regarding this technology use within their business facilities, computers, and networks.

Note

"Web 2.0 is generally a term, made popular after the first O'Reilly Media Web 2.0 conference in 2004, describing the emerging ways in which World Wide Web technology and Web designs can be used to enhance and make easier information sharing, creativity, and group collaboration. Web 2.0 services and technologies include such things as social networking sites, wikis, blogs, micro blogs, mashups, crowdsourcing, surveillance sites, and folksonomies" (Rebecca Herold, "Web 2.0 Privacy and Security FAQ," http://www.privacyguidance.com/files/CSI_Alert_October_2008.pdf, CSI Alert, October 2008).

Chances are, personnel within your organization are participating in one of the popular social networking Web sites such as Facebook or MySpace. These sites are not inherently bad. However, those using them must consider the opportunities for other people on the sites to do bad things. Used appropriately, these sites can be quite informative and entertaining. Used inappropriately, though, they can be dangerous to not only your business but also your personnel and their family and friends.

Note

According to a March 2007 survey by security firm Clearswift, more than 75% of workers under 30 access social networking sites regularly from their work computers. Half of these say they have discussed their work, employer, customers, or coworkers on social networking sites.

When personnel visit social networking sites from the business network or computer systems, they may unintentionally expose information about personnel, customers, or your business-sensitive documents. How? Others on the site may be using social engineering schemes and malicious code, through the many peer-to-peer (P2P) communications these sites use, to scoop up your valuable business information.

Although your company may have software in place to prevent malicious code from damaging your network, this software may not prevent attacks or damage that can occur through P2P communications, such as instant messaging (IM), file sharing (such as Gnutella), or voice capabilities (voice over IP, or VoIP). It is also easy for other malicious software such as keyloggers and screenscrapers to be loaded on your workstation while communicating with social networking sites. These malicious programs may be able to record every keystroke or use other methods to secretly steal sensitive corporate or customer information.

Organizations must establish strong information-protection policies and procedures for using Web 2.0 technologies and sites while at work and while using business computers and networks. In most businesses, it will be infeasible to just completely ban the use of such technologies; business leaders would likely create a highly disgruntled group of employees as a result. Business leaders must decide what is allowable, and even beneficial, with regard to using Web 2.0 technologies, and implement controls to keep bad things from happening as new Web 2.0 technologies emerge.

Video Meetings and VoIP

Is your business using video meetings? Chances are, they will be soon. According to a late January 2009 report, Gartner predicts that the current and projected bad economy will drive more use of video meetings, making it pervasive within businesses in the next 3 years.

> **Resource**
>
> See the report about telepresence at http://www.networkworld.com/news/2009/012109-video-telepresence-to-be-more.html.

Gartner reports they project video meetings replacing 2.1 million airline seats each year, taking $3.5 billion annually from the US travel and hospitality industry. Related to this is the projection that by the end of 2013, "40 percent of enterprise knowledge workers will have abandoned or removed their desk phone" and businesses will be using VoIP solutions instead.

The technologies used for video meetings, most of which will be deployed via the Internet, and significantly more use of VoIP will result in drastic changes to business networks. Not only will bandwidth and performance be impacted, but many new paths through which sensitive data can be leaked outside the business will be created. Business leaders must ensure the security issues are addressed before using video meetings and VoIP to avoid massive, and possibly business closing, information security incidents and privacy breaches.

The List Is Ever-Growing

These are just a few of the new technologies currently being widely deployed by personnel and business unit management throughout large numbers of business organizations. A few of the other technologies that bring with them information protection, privacy, and compliance concerns include:

- Virtualization
- Collaborative content-management tools
- Storage sharing vendors
- Electronic data recycling
- P2P computing
- Connecting to business partner networks

Business leaders will benefit from staying current with the new trends. Enlist the help of your information security and IT leaders to give you regular reports about new technologies that are planned within your company, the associated information security risks, and how they plan to mitigate the risks.

Bad Economic Times Breeds Bad Security

Incidents can, do, and will continue to occur in a very wide variety of ways. Not just as a result of hackers or stolen computers, which are most widely reported, but also as a result of malicious intent from outsiders, malicious intent from insiders, mistakes made by those who handle PII, and simply lack of awareness of what should be done to protect PII, along with a large number of other unique ways. When the economy is bad, employees worry about losing their jobs. When employees worry about losing their jobs, many will resort to desperate measures, such as stealing information from their current employer to use for identity theft or other crimes in the event they lose their jobs, or to take with them to a new employer to provide a competitive advantage.

There is no doubt that this economy is impacting all companies and most individuals. I've read about and heard from many organizations that, as a result, their information security and privacy budgets are being drastically reduced, or even cut completely, in an attempt to save money during these uncertain times. Throwing out the baby with the bath water in this way is a very bad idea!

As the economy continues to be bad, you are going to see more cybercrime attempts, and more cybercrime successes. All the more reason for business leaders to ensure their personnel stays security aware and practice good security. Now is the time to make smart information security investments. There are many ways in which organizations can have good security without overpaying. It is a good time to review your information security expenditures.

One of the ways is to invest in the comparatively inexpensive information security and privacy training and awareness activities. Humans have always been the weakest link in information security success. Take the time, without the large bucks, to make personnel your best security tool. And, of course, maintain your basic security tools, such as encryption solutions , up-to-date anti-malware protections, and enforced policies, just to name a few.

Increasing Crimes

Over the past year, as the US economy along with the economies of most developed countries throughout the world continued to go deeper and deeper into recession, the reports of crimes by business insiders increased. Consider just a few examples that were all reported during the last week in February 2009:

- An assisted living nurse stole the personal information of her elderly patients at a Salisbury retirement community in Maryland and was sentenced to 5 years in prison and must pay in excess of $8000.
- A hospital employee at Johns Hopkins hospital in Baltimore was charged with stealing personal information about patients to obtain credit cards and made $169,390 in fraudulent purchases.
- A hospital worker at the Chandler Regional Medical Center in Arizona was charged with stealing credit cards from elderly patients and running up huge charges on their accounts.
- A 19-year-old Philadelphia woman who worked at the California Pizza Kitchen in the Plymouth Meeting Mall in Philadelphia admitted to stealing at least 50 customers' credit card numbers and giving them to another person to make fake credit cards. They then used the cards to charge more than $78,000 on the accounts. The woman pleaded guilty to felony charges that include theft and identity theft and faces a maximum sentence of 7 to 14 years behind bars.
- A Clayton County Georgia sheriff's department employee was charged with stealing co-workers' personal information including Social Security numbers, driver's license numbers, dates of birth, phone numbers, employee identification numbers, an inmate's medical information, and internal investigation files.

Note

"Almost 60 percent of employees stole company data upon leaving their jobs last year. As the economy worsens and more people are laid off, more insider theft is expected to occur." —ThomasNet Industrial News Room, February 24, 2009

This perceived increase in crime is supported by numerous research reports. For example, the ASIS International 2009 "Impacts of Current Economic Environment on Security" included the following findings:

> General Impacts of the Economic Downturn Results indicate that the need for security has increased in the current economic climate. Indications are stronger among the CSO segment, with 78% reporting an increase, compared to 66% of the managers. The reasons cited for the increased need differ by group, and ostensibly by size of company since the managers tend to work for smaller organizations. General increases in crime and theft, followed by employee lay-offs and furloughs, topped the CSOs' list of reasons. Security managers, on the other hand, reported increases in theft of, and damage to, physical property, as their primary threats."

Resource

See the ASIS International 2009 "Impacts of Current Economic Environment on Security" report at http://www.asisonline.org/membership/economicsurvey.pdf.

Not only do organizations face an increase of insiders doing bad things with the information they have access to but there are also increased risks from folks outside business when they see businesses with large amounts of PII as nice targets to quickly and easily obtain PII to commit crimes if there are insufficient security controls in place.

News agencies from small to large communities are reporting an increase in all types of crimes, including cybercrimes and other types of information thefts as the economy remains dismal. According to a February 2009 report from the FBI, cybercriminals currently have stolen more than $433 billion, or nearly 6 percent of the nation's economy. This crime not only negatively impacts US competitiveness and economic viability. Add to this theft of trade secrets, which represent as much as 85% of a company's value, and you have an even grimmer economic and security threat. The growing mobility of business information and intellectual property make it a huge and valuable target of cyber criminals.

Increasing Mobility

As the economy gets worse, you are going to see more mobile computing. More work is being done away from the office and within home offices in an effort to save on travel and commuting cost, as well as on the time such travel takes. Sensitive information is being stored in multiple locations within today's business enterprise, many of them mobile. Personnel take huge amounts of PII with them when they meet others in public places, while traveling, and in other ways that put PII at risk.

If your company is already struggling economically, the last thing you want to happen is a security incident that could have been prevented. A security incident and/or privacy breach could just be the final nail in the coffin for your organization. Clear-text mobile data represents coffin nails for a lot of organizations.

> **Note**
> "Clear text" data is data that can be read by the human eye. This is in contrast to "encrypted data," which is cryptographically scrambled and would make no sense when viewed with human eyes.

A February 2009 study by the Ponemon Institute reported that 88% of data breaches arose from staff negligence or lack of awareness, resulting in such things as laptops and storage devices being lost or stolen. Encrypting the PII, not only that is in transit through networks but also stored on mobile devices, has a significant impact on preserving privacy. Unfortunately, encryption is still an underutilized security tool.

According to the Ponemon study, information obtained from 720 IT security practitioners and 874 business managers from US-based organizations reveals:

- 92% of IT security practitioners have had a laptop lost or stolen and a data breach has resulted in 71% of these cases. Only 45% were able to prove the data was encrypted.
- 56% of business managers say they have disabled their laptop's encryption solution and 48% admit this is in violation of their company's security policy.
- 59% of business managers sometimes or often leave their laptop with a stranger when traveling.

Previous Ponemon Institute studies have shown that the lost or stolen laptop is the number one cause of data loss. It is no surprise considering how few laptops are using encryption.

Security Protections and Funding Reduced

Too many business leaders are cutting information protection funding and resources during the economic hard times. Since the beginning of 2009, I've asked a dozen CISOs from a variety of industries, including financial, banking, retail, government, education, and technology, whether they have seen an increase or decrease in their information protection funds and resources. Every one of them indicated that they have seen a decrease as well as the number of information protection personnel positions being cut in half. This even though numerous statistics show information security crime and incidents are rising.

> **Note**
> Investments in information protection funding is also down, as revealed by findings from the Dow Jones & Company, which reported that information security venture investment shrunk almost 50 percent from $1.1 billion in 2004 to $566 million in 2007, and then down to $351.5 million as of Q3 2008.

The combined increase in cybercrime and the insider threat, along with the reduction of important information protection activities, positions, and funding creates the perfect storm for a major breach to impact a business. Smart business leaders will see the need for continued information protection diligence and be sure to invest in information protection resources, training, awareness, and tools wisely. Figure 1.1 provides a good list for business leaders to consider and discuss with their information security, IT, and compliance leaders throughout the enterprise.

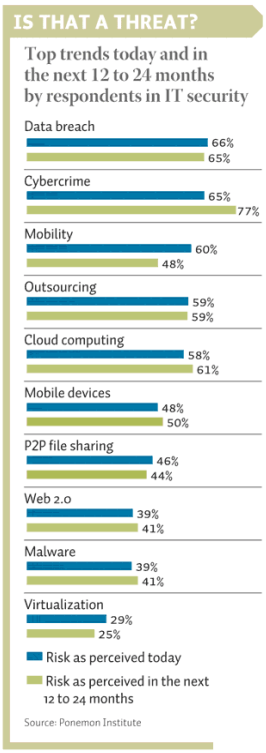

Figure 1.1: Risk trends business leaders must address (Source: Ponemon Institute).

The Impact of Information Security Incidents and Privacy Breaches to the Business

Your security can be breached in a number of ways as demonstrated earlier. The impact of an information security incident and associated privacy breach will likely be far greater than you would anticipate. Not only will the loss of sensitive or critical business information directly affect your competitiveness and cash flow, it could also damage your reputation and have a long-term detrimental effect. It can take your organizations years to establish a good reputation and build an image as a trustworthy and reliable business, but a security incident can destroy the reputation and customer trust in a matter of hours or even minutes. When privacy breaches occur:

- Customer trust is lost
- Customers are lost
- Brand value is lessened
- Breach response activities result in significant costs to the business
- Time involved for breach response will go for years
- Penalties and sanctions could reach into the millions of dollars

Addressing privacy concerns, implementing enterprise security, and ensuring compliance to applicable privacy laws are significant to achieving uninterrupted business processing, demonstrating due diligence, and minimizing risks due to noncompliance. A breach could potentially cost hundreds of thousands to millions of dollars in human resources, communications, and materials expenses in addition to negative publicity, lost business, and legal counsel costs.

According to a 2009 Ponemon Institute study, the average cost to an organization where a breach of PII occurred in 2008 was $202 per compromised record, up 2.5% from $197 per record in 2007. Consider how these costs can be broken down according to specific breach response activities.

As an example, let's examine how a breach could impact a hypothetical business, Company X, for a file containing unencrypted PII for 10,000 customers. Table 1.1 provides, at a high level, an example of some of the activities and associated conservatively estimated costs and times in total personnel man-hours that would have a financial and human resource impact to the organization.

Breach Impact Components	Hours/Cost
Time (in man-hours) to determine and confirm the files within which a breach of PII occurred	40
Time to determine all the individuals impacted	40
Time to collect contact information for impacted customers	60
Time to write and mail letters to notify customers of the breach	60
Time to create and update a web page containing information about the breach	48
Time to answer customer questions about the breach	500
Total Man-Hours	748
Avg. Cost per Man-Hour Cost (include all HR benefit considerations)	$200.00
Total Man-Hour Costs	**$149,600.00**
Customer Credit Monitoring	
Annual cost per individual for credit monitoring	$100
Number of Years to Monitor	3
Total Monitoring Cost for 10,000 Individuals	**$3,000,000**
Potential Legal Damages	
Fines and Fees for Applicable Laws	$250,000
Number of Individuals Bringing Civil Suit	500

Award Per Individual	$500
Total Civil Suit Award	$250,000
Total Fines, Fees and Awards	**$500,000**
Lost Customer Revenue Impact	
Number of Customers Lost as Result of Breach	1000
Value Per Customer	$200
Total Lost Customer Value	**$200,000**
Estimated Cost of Breach Response Materials	
Letter paper and envelopes	1000
Postage ($0.43 * # of individuals)	4300
Total Materials Cost	**$4,300.00**
TOTAL BREACH COSTS	**$3,704,300**

Table 1.1: Privacy Incident Business Impact Example (Source: The Privacy Management Toolkit, Rebecca Herold, Information Shield, 2005).

So, in this case, the breach cost the company an average of $370 per client record. Add to these costs a wide variety of unexpected costs. Although these numbers are significant, there are even more financial impacts than those shown that are associated with information security incidents and privacy breaches. Throughout my research over the past decade, I've identified at least 50 different types of financial impacts that can be involved with a breach, as I've documented within my Privacy Breach Impact Calculator within my Privacy Management Toolkit.

Note

I provide an abbreviated version of the Privacy Breach Impact Calculator at http://www.informationshield.com/privacybreachcalc.html to allow business leaders to provide numbers to see the potential impact of a breach as it would impact their own organizations.

Case Studies

It often helps to consider some actual incidents to see how information security incident and privacy breaches can impact businesses and customers. Consider the following two incidents and consider how similar situations would impact your business.

Cost of Responding to Breaches

Maine's Bureau of Financial Institutions, a division of the Department of Professional and Financial Regulation, conducted a survey at the direction of the state legislature that revealed the costs of Maine's banks and credit unions when responding to breaches. Here are a few of the findings:

- 95% of the 75 responding financial institutions (50 credit unions and 25 banks) were affected by one or more of 20 data breaches identified in the survey
- The cost of investigating all of the data breach incidents was $269,900 or 12.6% of total breach response costs in all categories.
- Providing notice to individuals of all the data breaches cost respondents a total of $304,500 or 14.2% of total breach response costs
- Reissuing credit and debit cards to affected customers cost nearly $1.2 million, representing 54.3% of the total breach response costs
- Undefined "other" costs totaled $68,800 or 3.2% of total costs for the survey respondents
- The total cost of covering fraudulent purchases and transfers was $336,100, or 15.7% of total breach response costs
- A little more than one third (25) of the institutions that reported breaches reported unauthorized or fraudulent transfers as a result of the breaches

Resource

See the full "Maine Data Breach Study" report at http://www.maine.gov/pfr/financialinstitutions/reports/pdf/DataBreachStudy.pdf.

Of the 75 survey respondents, 71 reported being affected by a data breach since January 1, 2007 and incurring expenses reported at $2.1 million. As documented in the report, "The Hannaford breach had the largest impact, affecting the most institutions (71), the highest number of affected account holders (243,599), and had the largest dollar cost ($1.6 million)."

In this survey, the cost of re-issuing credit cards was significant because of the high numbers of individuals impacted. Collectively for the 71 impacted institutions, 246,479 cards had to be reissued.

It is interesting to note that the majority of the financial institutions responded that they first learned of each breach through the Compromised Account Management System (CAMS) alerts that they receive. A CAMS alert is an email sent out by a card issuer, such as Visa, after it has verified that an account compromise potentially has occurred. They did not hear about it from their business partners, nor did they have any internal processes in place to identify the breach activities themselves.

This example provides insights into the complexities of privacy breach response and how many costs can be accumulated by the impacted organizations. It also demonstrates that when breaches occur within business partners, such as TJX and Hannaford, it can have significant detrimental and costly impacts to other organizations. Your business partners' breaches can have significant costly impacts to your organization.

ATM Break-In

On November 8, 2008 more than 130 ATMs in 49 cities throughout the world were hit by a group of apparently well-organized cyber criminals during a 30-minute period. The ATMs were all part of the RBS Worldpay system. The company put out a press release about this gigantic breach on December 23, 2008. The hacker(s) somehow got into the application code and removed the daily withdrawal limits on the ATM cards. They stole $9 million dollars through 100 cards during that 30-minute period.

Even if your organization does not have ATM systems, the concepts involved apply to all types of networks. Consider the following:

- How was the hacker(s) able to lift the limits? Does your organization have controls in place to prevent such hacks?
- What security controls should have been in place to prevent such a hack? Do you have enough security controls in place around your business applications?
- What controls were in place to protect the customer information? What controls are in place to protect your organization's customer information?
- What types of intrusion detection systems (IDS) could help detect such an attempt into a system? Are you using IDS within your own organization?
- What types of audit logs should be generated on systems? Do you have sufficient audit logs generated for your own business applications?

It is worth noting that all these are activities also support the Red Flags Rule requirements to have protections in place to prevent such types of fraudulent activity.

> **Note**
>
> The Red Flags Rule was created as a result of the Fair and Accurate Credit Transactions (FACT) Act of 2003. This rule requires financial institutions and creditors with covered accounts to have identity theft prevention programs and supporting processes in place to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

Lose Clear Text PII, Get a Fine

The US HHS applied the very first HIPAA noncompliance sanction on July 17, 2008 against Seattle-based Providence Health & Services (Providence). On several occasions between September 2005 and March 2006, backup tapes, optical disks, and laptops, all containing unencrypted electronic protected health information (PHI), were removed from the Providence premises and were left unattended. The media and laptops were subsequently lost or stolen, compromising the PHI of over 386,000 Providence patients. HHS received over 30 complaints about the stolen tapes and disks, submitted after Providence informed patients of the theft, as required by multiple state notification laws. Providence also had reported the stolen media to HHS. Under the sanction, Providence agreed to pay $100,000 and implement a detailed Corrective Action Plan to ensure that it will appropriately safeguard identifiable electronic patient information against theft or loss.

> **Note**
>
> This first HHS sanction is in addition to the October 2006 agreement Providence made with the Oregon Department of Justice to pay $95,764 to the Department of Justice Consumer Protection and Education Revolving Account for these same personal data theft incidents

The fact is that any type of PII that moves, either through networks or on the legs of individuals carrying mobile computers and storage devices, is at much greater risk of having bad things happen than the PII stored more securely on centralized servers deep within the layers of network security defenses within your corporate network. Business leaders must ensure that all types of mobile PII are strongly safeguarded. To demonstrate your due diligence for this PII protection, regardless of your industry, ask your information security and privacy officers the following questions:

- What kind of PII does your organization collect, manage and store?
- Where is all this PII stored?
- What safeguards are protecting the PII?
- Is mobile PII encrypted to most effectively protect it?

Key Business Leader Information Protection Responsibilities

Virtually every organization today obtains and maintains information in many different ways using an ever-growing number of technologies. These expanded quantities of information and technologies bring not only new business opportunities but also increased business risks. As a result business leaders have many more information protection responsibilities than ever before. A few of these include:

- Being in compliance with growing numbers of regulatory and legal requirements and emerging legal issues. More data protection laws exist worldwide than ever before, and more will be implemented. Business executives are ultimately responsible for ensuring their organizations are in compliance.
- Demonstrating due diligence and standard of due care for information protection and sufficiently supporting and funding information security programs.
- Providing visible and strong sponsorship of information security and privacy initiatives.
- Addressing the growing personnel demands to use new technologies while at work; not only for business purposes but also for personal activities such as email, instant messaging, and blogging.
- Ensuring the existence, awareness, and consistent support throughout the enterprise of information security policies and supporting procedures by endorsing regular training and ongoing awareness communications and activities.
- Understanding the business impact of not protecting data and taking responsibility for ensuring appropriate safeguards exist throughout the enterprise.
- Staying up-to-date with new and emerging information protection challenges.

Business leaders must make it a point to do at least two things to instill a culture of information security throughout the enterprise to protect business information assets as well as meet legal, regulatory, and industry standards and contractual requirements.

#1 Provide Visible Support for Information Security Initiatives

The most important ingredient for information protection success within business is having clearly visible, strong, and consistent executive management support. Over the years, I have seen a consistent common denominator within organizations that have successful information security, privacy, and compliance programs. They have visibly strong and consistent management support. Every organization I have seen without such support have had ineffective information assurance programs, resulting in ineffective privacy preservation, and their information assurance professionals then face great challenges, and frustrations, in not being able to be effective in their efforts.

> **Tip**
>
> Personnel in general really do follow the examples of their leaders and emulate them to a large degree.

This observation is validated through many studies. For example, consider a report released in late October 2006 sponsored by the International Information Systems Security Certification Consortium (ISC) and conducted by IDC. The study obtained feedback from 4016 information security professionals located in 100 countries. The most critical factor identified by these professionals for having a secure enterprise with effective information security policies and processes was having clear management support of their efforts. This emphasis upon the importance of management support for information security also supports the need for management support of privacy initiatives.

Standards Call for Strong Management Support of Security

Multiple NIST publications reinforce the need for management support of information safeguard efforts. For example, NIST SP 800-100 emphasizes the need for executive managers to regularly deliver messages to staff regarding security, such as through staff meetings, broadcasts to all users by the organization's leader, and other communications, and to champion the program and demonstrate support for training by committing financial resources to the program.

> **Resource**
>
> NIST SP 800-100, "Information Security Handbook: A Guide for Managers" is located at http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.

Laws and Regulations Call for Strong Management Support of Security

Multiple international information protection laws, such as the EU Data Protection Directive 95/46/EC and Canada's PIPEDA, require management support of information protection initiatives.

Good Leaders Set a Good Security Example

Personnel truly do follow their executive management's lead and example. I have seen evidence of this firsthand in the first half of the 1990's when I performed after-hours security reviews within a large multinational financial organization. I would lead a team of information security, physical security, audit, and compliance personnel through a specific business unit work area after normal work hours, typically after 7pm, to see what information security risks existed, such as passwords posted on sticky notes on monitors or under keyboards, documents containing PII laying out in clear view on their desktops, checks from customers laying out in the open, computers still logged into the network and unsecured, and so on.

In the areas where the management demonstrated these poor information security practices within their own workspaces, their personnel also exhibited these same behaviors. Always. It never failed to be the case. However, in the areas where management demonstrated exemplary information security practices, such as securing confidential papers, keeping their work areas secured, and so on, their personnel overwhelmingly also exhibited these same security practices.

When business leaders walk the security and privacy walk, actively and visibly protecting information, their staff will follow suit. Leading by example is a powerful way to promote security and ensure privacy is protected.

> **Tip**
> Organizations must have strong top management support to be successful in safeguarding PII and preserving privacy.

Every successful information security officer and privacy officer I know, and have read about, has the strong support and backing of their top business leaders. Every struggling security and privacy officer I know, and in organizations that have had significant and publicized privacy incidents and noncompliance penalties, have basically non-existent CEO and top business leader support.

#2 Make Personnel Responsible for Protecting Information

Organizations must also make personnel responsible for safeguarding sensitive information and PII. Personnel must know that there will be consequences for not being careful with PII. They must be motivated to safeguard and preserve the privacy of PII. Personnel must have information security and privacy as part of their job performance appraisal process.

When personnel are formally made responsible for documented activities and goals, they are more motivated to meet those goals and follow those activities than if they are just asked to do specific actions without having any consequence associated with the actions. During the course of a workday, it makes sense that personnel will perform the activities they know they are going to be evaluated against, and will have the most impact on their job, before they do other activities that they perceive as having no impact on their professional success as a consequence of not being documented or measured.

A Culture of Security Protects the Business

Institutionalizing information protection throughout the enterprise by involving leadership from every line of business will not only improve information protection efforts overall, it also is a cost-effective way to significantly improve the security of valuable business information. Making all business leaders accountable for information protection by including it as part of their job responsibilities will increase information security and privacy awareness and make all areas of the company more diligent in safeguarding information.

Business leaders must ensure data protection due diligence actions occur for many reasons. Successful business leaders understand that:

- Data protection is necessary for successful business. Protecting PII is necessary to prevent privacy breaches, and subsequently retain customers and employees.
- Data protection consists of three components; 1) maintaining the confidentiality of PII and other sensitive information, 2) maintaining the accuracy and integrity of PII and other mission critical information, and 3) ensuring PII and other business information is available to employees to use for job responsibilities, as well as to customers who want access to review their corresponding PII.
- Multiple laws, regulations, industry standards, organizational policies and contractual agreements require safeguards to be in place to protect PII and other business information.
- New technologies, such as cloud computing, peer-to-peer connections, VoIP, and Web 2.0 tools, present new risks that must be mitigated using new and more effective safeguards.
- Mobile PII and other sensitive information must have additional safeguards to address the increased risks. Encrypting mobile PII is one of the most effective safeguards possible.
- The bad economy, along with increasing crimes and higher levels of insider threats, has created more urgency to protect PII and eliminate enterprise vulnerabilities that put information at risk.
- Privacy breaches can significantly damage business through fines, civil penalties, lost trust and resulting lost customers and employees.

And last, but most importantly,

- Business leaders must recognize and strongly and visibly support information security and privacy initiatives throughout the entire enterprise, at every level.