What IT Needs to Know About Compliance

by Rebecca Herold, CISSP, CISM, CISA, FLMI ***June 2006***

Businesses must always be vigilant about data security, particularly in the global information-based economy. Businesses are dependent upon information technology (IT). The risks that are an inherent part of IT make it necessary for IT leaders and IT personnel to know the data protection laws and regulations more than ever before. It is with this knowledge that they can incorporate information security and privacy within all the IT processes, throughout the entire systems development life cycle (SDLC).

Regulations with IT Requirements in the United States

There are many regulations worldwide that have numerous data protection requirements. Some of these regulations directly apply to IT practices, but many indirectly impact IT, and it is important that IT leaders are aware of them. Within the U.S., the regulations that have received the most press and most explicitly define IT requirements include the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). However, other laws that don't explicitly state information security requirements, such as the Federal Trade Commission Act (FTC Act), still profoundly impact information security activities.

GLBA

The Safeguards Rule component of GLBA greatly impacts IT leaders. At a high level, this rule requires IT leaders to:

Establish a security plan to protect the confidentiality and integrity of personal data.

Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

Establish ongoing information security training and awareness.

Implement security for and within information systems, including network and software design and information processing, storage, transmission, and disposal.

Implement methods to detect, prevent, and respond to IT attacks, intrusions, or other system failures.

Design and implement information safeguards to control identified risks and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

Ensure the security of business partners and service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue, and requiring them within your contracts to implement and maintain safeguards.

Regularly evaluate and adjust the information security program based upon the results of the testing and monitoring, material changes to operations or business arrangements, and any other circumstances that might have a material impact on the information security program.

Technology Issues IT Must Address for GLBA

Authentication and identification

Access controls

Awareness and training

Malicious code protection

Risk analysis

Business continuity and disaster recovery

Data disposal

Data retention

Secure data transmissions

Secure data storage

Customer management databases

Procedures supporting your published policies

Third-party data sharing

HIPAA

The Security Rule component of HIPAA also greatly impacts IT leaders. At a high level, this section requires IT leaders to:

Perform a risk analysis for the electronic protected health information (PHI) within the organization and establish appropriate controls based upon the risks.

Ensure the confidentiality, integrity, and availability of all electronic PHI that the organization creates, receives, maintains, or transmits.

Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI.

Protect against any reasonably anticipated uses or disclosures of PHI.

Comply with the Security Rule standards with respect to all electronic PHI.

Review and modify security measures as needed to ensure reasonable and appropriate protection of electronic PHI.

Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule.

Provide ongoing information security training and awareness to all personnel handling PHI.

Ensure business partners have appropriate information security practices for the information your organization has entrusted to them.

Technology Issues IT Must Address for HIPAA

Authentication and identification

Access controls

Awareness and training

Malicious code protection

Risk analysis

Business continuity and disaster recovery

Data disposal

Data retention

Secure data transmission

Secure data storage

Customer management databases

Procedures supporting your published policies

Third-party data sharing

FTC Act

A regulation quickly growing in importance to IT leaders because of increasing compliance efforts, actions, and fines is Section 5 of the FTC Act. This basic consumer protection statute provides that “unfair or deceptive acts or practices in or affecting commerce are declared unlawful.” Although this regulation does not explicitly indicate information security requirements, the lack of security to support promises made to consumers, such as those commonly found in Web site privacy policies, can have significant impact on organizations. IT must implement security not only to support any posted policies and customer and business partner contracts that indicate information security measures exist to protect personal information, but they must also increasingly have such security measures in place as a basic expectation of a standard of due care.

Technology Issues IT Must Address for the FTC Act

Procedures supporting your published policies

Access controls

Third-party data sharing

Firewalls and malicious code prevention

Applications and systems development

Secure data transmissions

Secure data storage

Secure data disposal

International Regulations with IT Requirements

Throughout the world, there are numerous data protection laws that impact the decisions IT leaders make. Technology must be aligned with the requirements of the diverse geographic markets within which you operate.

> ☞ You must look at international information security and privacy differences in terms of what is expected and normal for the country within which you are storing, processing, or transmitting data—not in terms of what is expected and normal in your country of residence.

Just a few of the laws that have had significant impact on companies include Canada’s Personal Information Privacy and Electronic Data Act (PIPEDA), the European Union’s Data Protection Directive, and Japan’s Information Protection Law.

Canada's PIPEDA

Canada's PIPEDA applies to every organization with regard to its use of personal information about Canadian citizens that it collects, uses, or discloses in the course of commercial activities, and about its employee's personal information. IT leaders need to:

Establish safeguards for personal information to ensure only those with a business need can gain access to it.

Establish retention practices to ensure personal information is retained for as long as is necessary to allow individuals access to it for pursuing actions to PIPEDA violations.

Technology Issues IT Must Address for PIPEDA

Individual access requirements

Procedures supporting your published policies

Access controls

Third-party data sharing

Cross border data flow

Applications and systems development

Secure data transmissions

Secure data storage

Canadian provinces have generally been following the BS7799 standards for information security and the OECD privacy principles for many years. By adopting these practices and integrating them into your own IT standards, you will be several steps ahead in facilitating information data flows with Canada.

EU Data Protection Directive

Any person or organization that collects or handles personal information from a citizen of any of the 25 EU nations and transfers the information across the country borders must comply with this regulation. To comply with these requirements, IT leaders must generally:

Establish policies and procedures to keep personal data accurate and up to date, document when a data subject informs you that data is inaccurate, and take reasonable steps to ensure that data is accurate beyond simply asking the subject when the data is collected.

Establish procedures to discontinue use of personal data and dispose of it when it is no longer necessary for the business purpose for which it was collected.

Establish appropriate security technology to prevent personal data from being hacked, lost, damaged, or stolen.

Establish procedures to prohibit the transfer of personal data outside the European Economic Area unless the country to which it is being transferred provides an adequate level of protection.

Keep in mind that there is a traditional European 1-month-long holiday that can start anywhere between mid-July and mid-September. Schedule your IT upgrades and implementations to allow for the possibility that you might not be able to work with your IT counterparts in the EU countries during this time. If you don’t, it could significantly impact your project and security, and potentially result in downtime your organization cannot afford.

Similar to Canada, the EU countries have been following the BS7799 standards for information security and the OECD privacy principles for many years. This should provide even more impetus to adopt these practices and integrate into your own IT standards—helping you to be positioned to successfully address legal requirements within these countries.

You must be aware that each of the EU countries is mandated to have country-specific data protection laws that must, at a minimum, correspond with the EU Data Protection Directive. Some of the country-level laws go beyond the directive requirements.

There are very strict data protection laws within the EU for not only consumer data but also employee data. So, for example, if you are considering the implementation of a U.S.-based centralized SAP solution for all your worldwide offices, it is important to know that in some countries, such as France, the transmission of employee data across country borders is prohibited unless you work out an agreement with each of the applicable country’s privacy commissioner.

Technology Issues IT Must Address for the EU Data Protection Directive

International data flow restrictions

Individual access requirements

Procedures supporting your published policies

Access controls

Third-party data sharing

Applications and systems development

Secure data transmissions

Secure data storage

Secure data disposal

Japan's Personal Information Protection Law

Japan's Personal Information Protection Law broadly provides for the protection of personal information used by the Japanese government, third parties, and the public sector, referenced as "Personal Information Handling Operators," that handle data about more than 5000 persons. As part of the compliance requirements, IT leaders must generally:

- Establish procedures to keep third parties from accessing personal data except as required by law.
- Establish procedures to retrieve personal data for specific individuals upon their request.
- Establish procedures to correct personal data errors and inaccuracies as quickly as possible.
- Establish procedures to discontinue use of personal data as soon as requested.
- Establish safeguards for personal data.

Technology Issues IT Must Address for Japan's Personal Information Protection Law

- Authentication and identification
- Access controls
- Auditing and logging
- Malicious code prevention
- Secure data transmissions
- Secure data storage
- Third-party data sharing

Besides the aforementioned laws, there are literally hundreds of other international and U.S. federal and state-level laws with which organizations must comply. These laws cover not only customer and consumer personal information but also employee information.

More Incidents and More Actions in the U.S.

IT leaders must know that as technology advances, information security lags behind those advances. Diligence is necessary to ensure the security of personal data no matter where it is located. If IT leaders do not participate in data protection efforts, the business is at high risk of being negatively impacted by resulting incidents, non-compliance fines, civil suits, customer loss, diminished stock value, and brand damage.

IT leaders need to be aware of the increasing numbers of information security incidents and regulatory oversight actions. For example:

> As of April 2006, the FTC has filed five data security cases based on deception, which the commission and the courts have defined as a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances. In each of these cases, the commission alleged that the companies made explicit or implicit promises that they would take appropriate steps to protect sensitive information obtained from consumers. Their security measures, however, were grossly inadequate and their promises therefore deceptive. The FTC has also brought 12 other data security cases, 6 spyware and adware cases, more than a dozen financial pretexting cases, and more than 80 spam cases.
>
> As of May 2006, the Department of Health and Human Services has received almost 20,000 noncompliance complaints and launched thousands of HIPAA noncompliance investigations, and two criminal cases have been brought for non-compliance with HIPAA.
>
> The numbers of reported incidents of PIPEDA noncompliance in Canada have steadily been increasing over the past few years. In 2002, Canada launched approximately 1700 PIPEDA investigations. Canadian Federal Privacy Commissioner Jennifer Stoddart warned in a speech made public March 9, 2006 that she will make greater use of her statutory powers to crack down on privacy violations in Canada because organizations are not taking their privacy responsibilities seriously enough, and are not responding appropriately to the Privacy Commissioner's directives following violations.
>
> The numbers of actions taken in EU nations has steadily been increasing over the past several years. As examples, in 2002, the Spanish Data Protective Authority fined approximately US$900,000 against an organization for inappropriately sharing customer data with a subsidiary, and approximately US$1.17 million for disclosing protected personal information to the public.
>
> During the years 2001 to 2002, 483 privacy complaint cases were completed in Hong Kong by the Privacy Commissioner Office.

What IT Leaders Need to Know

Noncompliance with laws and regulations can not only impact organizations significantly as an effect of regulatory fines but also through the greater impact from the potential civil actions and the long-lasting requirements of the regulatory agencies that result in organizations needing to implement more procedures and obtain more resources to demonstrate, for as long as 20 years following a judgment, that they have reasonable security measures in place. Many laws and regulations have requirements for protecting information that IT leaders must be involved with implementing, and in many cases, establishing and managing as an ongoing process to meet the requirements.

Critical to the success of the IT leaders is the visible and demonstrated support and backing of executive management. Executives set the examples their personnel emulate. If business executives are not strong supporters of information security initiatives, IT leaders will have a very difficult time meeting the technology requirements of data protection regulations and laws.

IT Leader Regulatory Compliance Action Plans

IT leaders must establish a unified regulatory compliance action plan tailored to their business to ensure that the business is addressing all technology compliance requirements. This action plan needs to include the following elements, which are explicitly stated components of an effective security program not only within regulations such as HIPAA and GLBA but also by regulatory oversight agencies such as the FTC (Source: http://www.ftc.gov/os/2006/03/P034101CommissionTestimonyConcerningSmallBusinessSecurity.pdf):

Implement effective education programs to stay aware of regulatory requirements; make personnel aware of and provide training about the threats to information systems and the steps all business areas must take to address them.

Develop and communicate information security policies and procedures regarding the appropriate use and security of information and computer systems.

Incorporate security into the systems and applications development life cycle to ensure security is implemented and managed effectively.

Identify and inventory all personal data, including data flows, storage locations, and persons with access to the data.

Implement safeguards, such as encryption and access control technologies, to protect personal data in all locations and while in transit through untrusted networks.

Include security requirements within contracts of business partners entrusted with personal information or that have access to the organization's personal information.

Use malicious code prevention software, intrusion detection and prevention systems, and firewalls.

Establish personal data backup, retention, and disposal policies and procedures that comply with applicable laws, regulations, and contractual requirements.

Establish information privacy and security incident response and breach notification policies and procedures.

Incorporate Information Privacy and Security into the SDLC

Based upon the discussion so far, you should recognize the recurring IT requirements necessary for compliance with the multiple laws and regulations. Look at all the lists as one composite set of requirements; it will unify compliance efforts and address many regulations within one set that should be made part of your regulatory compliance strategy.

IT Must Address the Following Requirements that Are Extrapolated from a Wide Range of Regulations and Laws

Access controls

Applications and systems development

Auditing and logging

Authentication and identification

Awareness and training

Business continuity and disaster recovery

Cross border data flow

Customer management databases

Data disposal

Data retention

Firewalls and malicious code prevention

Individual access requirements

International data flow restrictions

Malicious code prevention

Procedures supporting your published policies

Risk analysis

Secure data disposal

Secure data storage

Secure data transmissions

Third-party data sharing

The most effective way to incorporate these issues consistently into the IT environment is to:

Make them formally documented requirements within your SDLC process

Assign specific positions or personnel with the information security and privacy activities involved to ensure they are addressed sufficiently

> ☞ IT must address information privacy and security throughout the entire SDLC.

Perform information privacy and security risk assessments at key points throughout the SDLC to ensure the related issues have been addressed, and to catch any showstoppers related to privacy or security.

Performing PIAs

The systems development and maintenance teams must ensure privacy impact assessments (PIAs) are performed to help ensure compliance with applicable laws and regulations:

Throughout the SDLC

To determine where PII will be obtained, stored, transmitted, and retired

To determine applicable data protection laws and regulations

To determine who will have access to PII

To map the planned PII data flow

To identify risks throughout the flow

Performing Information Security Risk Assessments

The systems development and maintenance teams must ensure information security risk assessments are performed to help ensure compliance with applicable laws and regulations:

Throughout the SDLC

To identify technical, administrative, and physical risks within the planned system

To identify cost-effective controls to address the identified risks