InformationShield

A Brief History of Regulatory Time

By David J. Lineman

As security professionals, we live in an increasingly regulated world. As more companies do business internationally, they must be aware of the security and privacy requirements of the countries where they operate. This paper provides a brief history and overview of important legislation that impacts information security. By looking at key trends, we can be better prepare our organizations for future compliance efforts.

Selection Criteria

The regulations outlined in this paper are chosen based on several criteria. First, is overall impact: how many total organizations and/or individuals they affect. Second is historical significance. Some regulations illustrate a new regulatory trend. Even if they are later replaced, they were key milestones at the time. Third is economic impact. For example, laws that regulated the United States Federal government are mentioned because the U.S. Federal Government is the single largest customer of security products and services. While there is a bias toward legislation affecting the United States, every attempt is made to include important international laws as well.

An overview of security-related regulations

There are a couple of important considerations when looking at the world of regulations. First, is the time line. Since information security is a relatively new field, and widespread use of computers is even newer, most regulations are clustered within the last several years. In fact, the pervasive use of the internet is responsible for much of the newest legislation. Figure 1 provides a visual representation of the regulations mentioned in this article.

Second is the legislative framework or structure. This defines the overall categories and types of legislation that affect information security. For example, some legislation, such as Sarbanes-Oxley or Gramm-Leach-Bliley

(GLBA) is far-reaching and has only certain components that affect information security and privacy. Others, such as The Children's Online Privacy Protection Act (COPPA) are directly enacted to affect security or privacy.

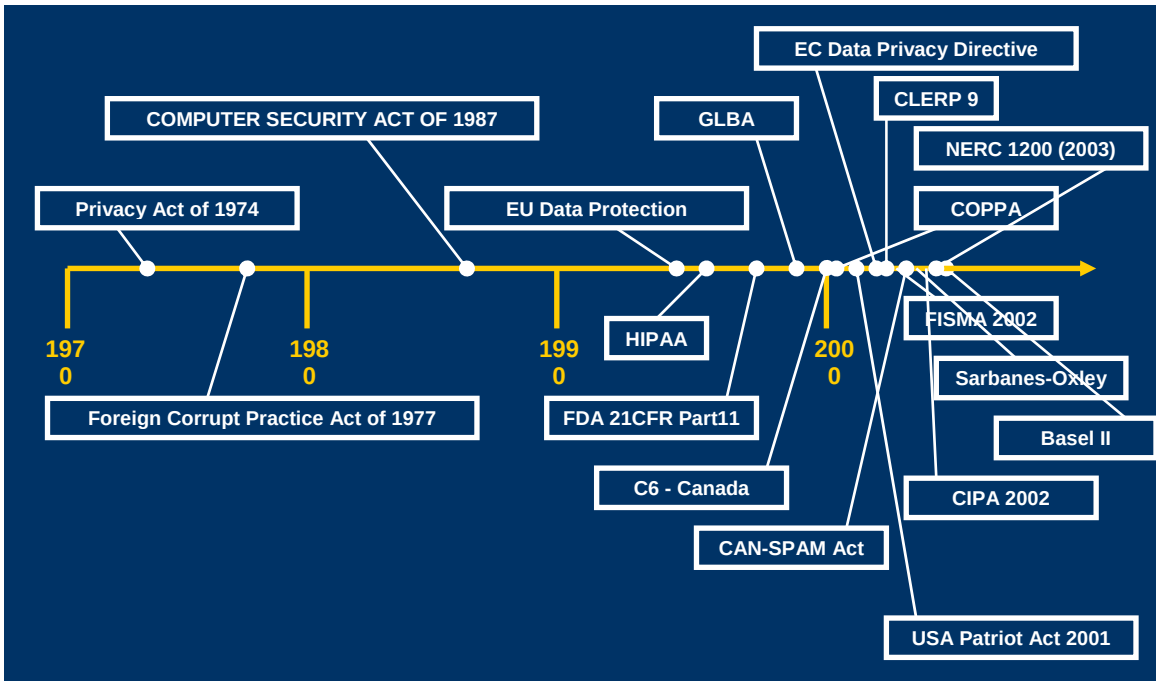

Figure 1: Timeline of security and privacy-related regulations.

Specific Regulations by Date

Name:	**Privacy Act of 1974**
Date Enacted: Brief Description:	September 1975 The Privacy Act of 1974 was originally introduces as a "code of fair information practices that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies." However, this first regulatory attempt to define proper guidelines for the protection of personal information was plagued by quick passing, vague wording, and a long history of updates and modifications. The Office of Management and Budget says it best in their 2004 update to the act: "The Act's imprecise language, limited legislative history, and somewhat outdated regulatory guidelines have rendered it a difficult statute to decipher and apply." That being said, this law still sets the basic precedent for federal

	governments protecting private information of individuals. In 2003, the General Accounting Office (GOA) did a review of agency compliance with the Privacy Act of 1974, indicating that most agencies could still use improvement.
Industry Effected:	Federal Government
Country:	United States
Related Regulations:	Freedom of Information Act, Federal Information Security Management Act (FISMA)

Name:	**Foreign Corrupt Practice Act of 1977 (FCPA)**
Date Enacted:	September 1977
Brief Description:	In a very early pre-cursor to Sarbanes-Oxley, the FCPA was designed to restore confidence in American companies doing business overseas. As Sarbanes-Oxley is sometimes referred to as "the Enron legislation", FCPA was in response to several scandals involving bribes of foreign officials. At the time, companies voluntarily admitted to giving over $300 million in corporate funds to foreign government officials, politicians, and political parties. Later deemed to be too restrictive, the Act was modified in 1998.
Industry Effected:	All U.S. Companies
Country:	United States
Related Regulations:	Omnibus Trade and Competitiveness Act of 1988, Sarbanes-Oxley, USA PATRIOT Act

Name:	**COMPUTER SECURITY ACT OF 1987**
Date Enacted:	January 1988
Brief Description:	The Computer Security Act reaffirmed the role of the National Institute of Standards and Technology (NIST) as defining the security standards for protecting non-classified federal data. Not only did it establish security baselines for systems, it required the establishment of security plans for system owners and security awareness training for the operators of systems containing "sensitive information." This is one of the first laws to not only formalize security requirements, but to refer to an external agency for their established guidelines. This basic

	trend continues in various vertical industries, where federal law establishes the requirements for controls, but standards bodies define the detailed requirements.
Industry Effected:	Federal Government
Country:	United States
Related Regulations:	E-Government Act of 2002, Privacy Act of 1974

Name:	**EU Data Protection Directive – 1995**
Date Enacted:	1995
Brief Description:	Data Privacy moved across the pond in 1995. With the establishment of the European Union, protection of private data was deemed critical for cross-border electronic commerce. This Act provides a regulatory framework to guarantee secure and free movement of personal information across national borders of EU member countries, and also establishes a baseline of security controls protecting this information. This Act is effectively mirrored in many vertical industries such as HIPAA for healthcare and Gramm-Leach-Bliley for financial services.
Industry Effected:	All industries
Country:	European Union
Related Regulations:	Privacy Act of 1974, C6-PIPEDA

Name:	**Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
Date Enacted:	August 1996
Brief Description:	The goal of HIPAA was to reform the health insurance market and simplify healthcare administrative processes, while strengthening the privacy and security of health information. The HIPAA security regulations fell into the broad categories of patient privacy and health information security, placing requirements on healthcare providers, health plans, healthcare clearinghouses and insurance companies, collectively referenced as healthcare organizations or “covered entities.” HIPAA took years to go from draft for final rule, with the final Security Rule being effective in February

	2003. But it defines specific requirements for protecting the privacy and security of private health information of individuals. Every time you have to sign those nasty, illegible privacy policies in the doctor's office, you are being affected by HIPAA.
Industry Effected:	Healthcare
Country:	United States
Related Regulations:	Public Health Information Act (Canada), FDA 21 CFR Part 11.

Name:	**Food and Drug Administration 21 CFR Part 11**
Date Enacted:	August 1997
Brief Description:	With the imposing title, "Title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures," 21 CFR Part 11 established a set of technical and procedural controls for dealing with electronic records and electronic signatures. In contrast to most other government regulations, 21 CFR Part 11 was developed in response to the pharmaceutical industry's request to the government to accept new technologies (for example, electronic signatures). Although passed after HIPAA, this was the first law outside of the financial services sector that had some financial impact on an industry. Several pharmaceutical companies had large compliance issues that resulted in fines and delays of major drug development. Many U.S. companies are required to comply with both HIPAA and FDA CFR Part 11.
Industry Effected:	Pharmaceuticals and medical equipment
Country:	United States
Related Regulations:	HIPAA (United States)

Name:	**Personal Health Information Act**
Date Enacted:	June 1997
Brief Description:	The Canadian Health Act of 1984 established the foundation for a publicly administered health insurance system in Canada. The Personal Health Information Act establishes "clear and certain rules for the collection, use and

	disclosure of personal health information." The act establishes the right of individuals in Canada to request and examine the personal health information collected by trustees. The act also places restrictions on healthcare organizations in Canada, including requirements for maintaining the security, accuracy and confidentiality of "Personal Health Information." In addition to these requirements, many individual provinces are establishing their own laws, such as *The Health Information Protection Act* passed in 1999 by Saskatchewan.
Industry Effected:	Healthcare
Country:	Canada
Related Regulations:	HIPAA, Bill C6 (PIPEDA)

Name:	**UK Data Protection Act 1998**
Date Enacted:	July 1998
Brief Description:	The Data Protection Act of 1998 is an example of EU member countries drafting their own data privacy policies to become compliant with the requirements of the EU Data Protection Directive. This is a common theme in regulatory history. We often see vertical industries (like healthcare) or certain member states or provinces leading the way in data protection measures that are later adopted at the national level. This law represents the process in reverse, as member counties enable laws to comply with international standards.
Industry Effected:	All industries
Country:	United Kingdom
Related Regulations:	EU Data Protection Directive

Name:	**Children's Online Privacy Protection Act (COPPA)**
Date Enacted:	October 1998 (Modified April 2000)
Brief Description:	Leading the regulatory process for protecting children in the age of the internet, COPPA prohibits unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personally

	identifiable information from and about children under age 13 on the Internet. The rules spell out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online. Several United States companies have been fined for violation of the provisions of COPPA.
Industry Effected:	All industries collecting person data.
Country:	United States
Related Regulations:	Children's Internet Protection Act (CIPA)

Name:	**Gramm-Leach-Bliley Act – Title V (GLBA)**
Date Enacted:	November 1999
Brief Description:	Also knows as The Financial Modernization Act of 1999, GLBA was designed to modernize the United States' financial services industry by removing historical barriers between sectors, such as banking, insurance and securities brokerage. In addition, Title V of the law directed the Federal financial institution regulators, the SEC and the Federal Trade Commission (FTC) to create new regulations that address the privacy and security of customer information. This law is a good example of how a very broad legislation can trigger very specific information security requirements. Basically, GLBA changed the definition of a "bank", and required an entirely new group of organizations to adopt the security and privacy requirements of the banking industry. It also added new privacy and disclosure requirements to protect personal financial information of consumers. Every time you get one of those letters from your bank or brokerage telling you about their privacy policies, you are experiencing GLBA.
Industry Effected:	Financial Services
Country:	United States
Related Regulations:	Fair Credit and Reporting Act, HIPAA

Name:	**BILL C-6: PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)**
Date Enacted:	April 2000
Brief Description:	In this Act, the privacy guidelines for health information expand to all personal information and all industries in Canada. The Act establishes rules for the management of personal information by organizations involved in commercial activities. According to the Act, businesses must obtain the individual's consent when they collect, use or disclose personal information. The Act further stipulates that Canadian's have the right to inquire as to accuracy and the use of their personal information. (It is interesting to note that the United States has no law of this magnitude, but instead regulates specific industries such as healthcare and financial services.)
Industry Effected:	All organizations in Canada or collecting private information from Canadian citizens.
Country:	Canada
Related Regulations:	Privacy Act of 1974, EU Data Privacy

Name:	**Children's Internet Protection Act (CIPA)**
Date Enacted:	December, 2000
Brief Description:	This is legislation designed to protect children by hitting organizations where it counts: in the budget process. CIPA requires any public institutions (such as schools or libraries) that provide internet access to children to implement security policies and content filtering technologies Any organization that uses funding under the Library Services and Technology Act (a.k.a. "The E-rate Program") must comply with CIPA. In this regard, CIPA is similar to FISMA, which requires security assessments for Federal agencies before their budgets are approved by the OMB.
Industry Effected:	Public institutions proving internet access.
Country:	United States

Related Regulations:	Children's Online Privacy Protection Act (COPPA)

Name:	**USA PATRIOT Act**
Date Enacted:	October 2001
Brief Description:	The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) was enacted to help prevent, detect and prosecute money laundering and the funding of terrorism. This act is interesting because it modifies the provisions of several existing laws, such as the Bank Secrecy Act, making it very hard to decipher. Basically, the Act requires financial institutions to establish a Customer Identification Program (CIP) that follows appropriate policies and guidelines for verifying the identity of individuals. Any time you are required to provide your driver's license when you are applying for a bank account or any type of credit, you are experiencing the USA PATRIOT Act.
Industry Effected:	Financial
Country:	United States
Related Regulations:	Bank Secrecy Act (United States), GLBA

Name:	**Sarbanes-Oxley Act (SARBOX)**
Date Enacted:	August 2002
Brief Description:	The Sarbanes-Oxley Act of 2002 was enacted to address corporate governance, financial reporting and internal control issues in the aftermath of public company collapses such as Enron and Worldcom. Section 404 of the Act mandates, among other reporting and audit requirements, that companies establish a system of internal controls to insure adequate financial reporting. Sarbanes-Oxley is a classic case of a far-reaching law that leaves companies scrambling to figure out the details. Most organizations are using the COSO Framework to define their control objectives and the CobIT (Control Objectives for Information Technology) framework to determine the specific

	operational requirements. Basically, the frameworks require appropriate levels of security, but the detailed security requirements can vary widely among various companies. While the compliance deadlines are still rolling in for companies, Sarbanes-Oxley defines the major trend of "financial risk reduction through corporate governance."
Industry Effected:	All publicly-traded companies
Country:	United States
Related Regulations:	The New Basel Accord (Basel II), Corporate Law Economic Reform Program (CLERP 9)

Name:	**Corporate Law Economic Reform Program (CLERP 9)**
Date Enacted:	2002
Brief Description:	The United States wasn't the only country with collapsing companies and outrage at financial markets. CLERP 9 is Australia's version of Sarbanes-Oxley. (Or Sarbanes-Oxley is America's version of CLERP 9, depending on how big your knife is.)
Industry Effected:	Financial Services
Country:	Australia
Related Regulations:	The New Basel Accord (Basel II), Sarbanes-Oxley

Name:	**Homeland Security Act of 2002**
Date Enacted:	December 2002
Brief Description:	In response to the terrorist attacks on the United States, the Homeland Security Act of 2002 established the department of Homeland Security, which enabled a massive restructuring of the federal agencies that perform security functions. At the same time, the government published its "National Strategy to Secure Cyberspace" which outlined several programs that later translated into specific regulations. Two if its primary goals are to establish federal standards to protect government data and critical infrastructure from cyber attacks. It also outlines border protection and emergency response requirements.
Industry Effected:	Federal Agencies

Country:	United States
Related Regulations:	FISMA, NERC 1200, C-TPAT, USA PATRIOT Act

Name:	**E-Government Act of 2002 (Title III – FISMA)**
Date Enacted:	December 2002
Brief Description:	The Federal Information Security Management Act (FISMA) was approved in December 2002 as Title III of the broad-based E-Government Act of 2002. Under FISMA, which supersedes the Government Information Security Reform Act of 2000 (GISRA), federal agencies are required to assess the state of their security before being approved for budget items by the OMB. This is the first federal law to tie security assessments with budget approval. FISMA requires federal agencies to assess the security of both classified and non-classified systems and to include risk assessment and security needs with each new budget request. The Act requires the National Institute and Standards and Technology (NIST) to establish the detailed security requirements used to evaluate each agency under FISMA. NIST Special Publication 800-26 defines 17 security control areas that provide a framework for assessing the security of federal systems.
Industry Effected:	Federal Government
Country:	United States
Related Regulations:	Homeland Security Act of 2002, Computer Security Act of 1987.

Name:	**NERC 1200 Urgent Action Cyber Security Standard**
Date Enacted:	August 2003
Brief Description:	Commonly called NERC 1200 UAS, the purpose of this standard is to reduce the overall vulnerability of the bulk electric systems to cyber threats. The cyber security standard defines requirements in 14 control areas. These guidelines are in response to the Homeland Security Act of 2002 which establishes the requirements for protecting Critical Infrastructure

	Information (CII). To the layperson, this means our energy infrastructure. While most guidelines focus on information security, these guidelines focus on process control or "SCADA" systems. Energy and Electricity Providers
Country:	United States
Related Regulations:	Homeland Security Act of 2002, FISMA

Name:	**Customs-Trade Partnership Against Terrorism (C-TPAT)**
Date Enacted:	April 2003
Brief Description:	As part of Homeland Security, US Customs has the right to hold and inspect shipping containers. While not a regulation, C-TPAT is a voluntary program for organizations involved in international cargo shipping. By enrolling in C-TPAT, organizations agree to establish a system of security controls that reduce risks to cargo shipments. Basically, companies that establish better security will benefit from less inspections and better shipping times. This is an example of how the concept of "Homeland Security" in the United States had trickled into all aspect of information and physical security, as the Homeland Security Act folded the US Customs Agency under the Department of Homeland Security. It also falls in the category of "self-regulated" internal controls for economic benefit, similar to Basel II.
Industry Effected:	All industries that ship or export goods.
Country:	United States
Related Regulations:	Homeland Security Act, Basel II, Sarbanes-Oxley

Name:	**Basel II Accord (EU)**
Date Enacted:	2003/2004
Brief Description:	Currently under final development, the New Basel Capital Accord (also known as Basel II) introduces important modifications to the way banks define risk-weighted assets. Basel II modifies the basic risk equation, defined in the original Basel Accord, to include operational risk in addition to credit risk and market risk when computing requirements for reserve capital.

	Basically, Basel II allows banks to reduce their overall reserve cash position set aside for credit risk by adopting a set of internal controls to reduce operational risk. Although adopted for different reasons, the Basel II accord follows the trend it overall operational risk reduction through corporate controls represented in the Sarbanes Oxley Act.
Industry Effected:	International Financial Services
Country:	European Union
Related Regulations:	Sarbanes-Oxley Act (United States), Corporate Law Economic Reform Program, CLERP 9. (Australia)

Name:	**California Individual Privacy Senate Bill - SB1386**
Date Enacted:	July 2003
Brief Description:	California SB1386 is another example of states setting privacy standards that are greater than those at the Federal level. Among other requirements, organizations experiencing a security breach that may have revealed the "private information" of California residents must notify each of these individuals. This law brings up the nasty idea of trying to segregate data protection based on the customer's location. What it does, in effect, is raise the bar on data privacy and disclosure. Since most companies doing business in North America will have customers in California, who will able to do anything beyond treating all customers with the same policies?
Industry Effected:	All industries with customers in California
Country:	United States
Related Regulations:	BILL C-6: (PIPEDA), EC Data Privacy Directive.

Name:	**CAN-SPAM Act of 2003**
Date Enacted:	December 2003
Brief Description:	The Controlling the Assault of Non-Solicited Pornography and Marketing Act is one of a number of regulatory attempts to control the proliferation of SPAM. The law creates requirements for labeling of unsolicited email, establishes guidelines for proper

	electronic marketing, and establishes stiff penalties for violations. It also enables the FTC to establish a "do not email" registry. Similar acts are either being passed or considered in many other countries. Although widely considered as ineffective in stopping SPAM by the security community, it does establish a precedent for enacting a law specifically to address one cyber-security issue. Are you read for "The Do-Not-Phish Act of 2004?"
Industry Effected:	All industries engaged in email marketing
Country:	United States
Related Regulations:	EU E-Privacy Directive, The SPAM Act of 2003 (Australia), Marketing Practices Act (Sweden, 1995), Marketing Control Act (Norway, 2001),

Lessons for security professionals

If we study the history and current trends in regulatory compliance we discover a couple of key ideas. First, that many regulations are simply re-iterating the same security and privacy requirements with different words and different regulatory bodies. Second, to comply with most security-related regulations, we must simply follow the same standards of good security practice that have been taught for years. If we select a security framework such as ISO 17799, and manage our security program toward that framework, we will be in compliance with most security-related regulations.

In the end, regulations do not introduce new security concepts, but reinforce what we already know. It's the "Mom and Apple Pie" of information security: Have security policies for protecting people and systems. Establish security baselines and monitor them. Have incident response procedures. Train and educate users on security and privacy principals. Perhaps now, however, we have a legitimate reason to implement the security practices that have proven out over time but rarely get funded. Just make sure you say "Sarbanes-Oxley" when you are asking for budget approval.

About Information Shield - Information Shield is a global provider of security policy solutions that enable organizations to effectively comply with international regulations. Information Shield products are used by over 7000 customers in 59 countries worldwide. Find out more at our Regulatory Resource Center at www.informationshield.com or contact the author at dave@informationshield.com