Compliance and Security Are Not the Same

A rapidly and ever-increasing number of international, multinational, federal, regional, state, and local laws and regulations mandate numerous cybersecurity and data protection requirements for businesses and organizations worldwide. Various industry directives, such as the Payment Card Industry Data Security Standard (PCI DSS), also establish their own cybersecurity standards and best practices for businesses and organizations operating under their purview.

This complex regulatory environment is further complicated by the fact that many laws and regulations are obsolete, ambiguous, not uniformly supported by international communities, and/or inconsistent (with other applicable laws and regulations), thus requiring legal interpretation to determine relevance, intent, and/or precedence. As a result, businesses and organizations in every industry struggle to achieve and maintain compliance.

You should understand that compliance and security are not the same thing. An organization can be fully compliant with the various cybersecurity laws and regulations that are applicable for that organization, yet still not be secure. Conversely, an organization can be secure yet not be fully compliant. As if to underscore this point, the compliance and security functions in many organizations are separate.

Pertinent examples (neither comprehensive nor exhaustive) of current cybersecurity laws and regulations include:

Australian Privacy Principles. The Privacy Act 1988 establishes standards for collecting and handling personal information, referred to as the Australian Privacy Principles (APP).

California Consumer Privacy Act (CCPA). A privacy rights and consumer protection statute for residents of California that was enacted in 2018 and became effective on January 1, 2020.

Canada Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA defines individual rights with respect to the privacy of their personal information and governs how private sector organizations collect, use, and disclose personal information in the course of business.

European Union (EU) General Data Protection Regulation (GDPR). The GDPR applies to any organization that does business with EU residents. It strengthens data protection for EU residents and addresses the export of personal data outside the EU.

EU Network and Information Security (NIS) Directive: An EU directive that imposes network and information security requirements for banks, energy companies, healthcare providers, and digital service providers, among others.

North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP). NERC CIP defines cybersecurity standards to protect the physical and cyber assets necessary to operate the bulk electric system (BES) – the power grid – in the United States and Canada. The standards are mandatory for all BES-generating facilities with different criteria based on a tiered classification system (high, medium, or low impact).

Payment Card Industry Data Security Standard (PCI DSS). PCI DSS applies to any organization that transmits, processes, or stores payment card (such as debit and credit cards) information. PCI DSS is mandated and administered by the PCI Security Standards Council (SSC) comprising Visa, MasterCard, American Express, Discover, and JCB.

U.S. Cybersecurity Enhancement Act of 2014. This act provides an ongoing, voluntary public-private partnership to improve cybersecurity and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness.

U.S. Cybersecurity Information Sharing Act (CISA). This act enhances information sharing about cybersecurity threats by allowing internet traffic information to be shared between the U.S. government and technology and manufacturing companies.

U.S. Federal Exchange Data Breach Notification Act of 2015. This act further strengthens HIPAA by requiring health insurance exchanges to notify individuals whose personal information has been compromised as the result of a data breach as soon as possible but no later than 60 days after breach discovery.

U.S. Federal Information Security Modernization Act (FISMA). Known as the Federal Information Security Management Act prior to 2014, FISMA implements a comprehensive framework to protect information systems used in federal government agencies.

U.S. Gramm-Leach-Bliley Act (GLBA). Also known as the Financial Services Modernization Act of 1999, relevant provisions of GLBA include the Financial Privacy Rule and the Safeguards Rule, which require financial institutions to implement privacy and information security policies to safeguard the non-public personal information of clients and consumers.

U.S. Health Insurance Portability and Accountability Act (HIPAA). The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information. It requires appropriate safeguards for *protected health information* (PHI) and applies to *covered entities* and their business associates.

U.S. National Cybersecurity Protection Advancement Act of 2015. This act amends the Homeland Security Act of 2002 to enhance multidirectional sharing of information related to cybersecurity risks and strengthens privacy and civil liberties protections.

U.S. Sarbanes-Oxley (SOX) Act. This act was enacted to restore public confidence following several high-profile corporate accounting scandals, most notably Enron and Worldcom. SOX increases financial governance and accountability in publicly traded companies. Section 404 of SOX specifically addresses internal controls, including requirements to safeguard the confidentiality, integrity, and availability of IT systems.

Key Terms

Protected health information (PHI) is defined by HIPAA as information about an individual's health status, provision of healthcare, or payment for healthcare that includes identifiers such as names, geographic identifiers (smaller than a state), dates, phone and fax numbers, email addresses, Social Security numbers, medical record numbers, and photographs.

A *covered entity* is defined by HIPAA as a healthcare provider that electronically transmits PHI (such as doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies), a health plan (such as a health insurance company, health maintenance organization, company health plan, or government program, including Medicare, Medicaid, military and veterans' healthcare), or a healthcare clearinghouse.