Navigating the Requirements of a Successful Information Security Program

There are a number of reasons why having an information security program is important, but one of the primary reasons is to comply with regulatory requirements. Your business is the holder of data – for your customers, for your employees, for your vendors, and for third parties you work with – all of which may or may not be covered by a regulatory framework. These frameworks were designed to standardize how data is protected. However, these same frameworks often leave the process by which organizations choose to take action open ended.

Depending on the type of data your business uses in its day-to-day operations, one or more of the numerous regulatory frameworks may stipulate how you store and protect your data. For organizations that work with protected health information (PHI), such as health insurance companies and agencies, the Health Insurance Portability and Accountability Act (HIPAA) stipulates that customer data must be handled and stored confidentially and securely. Companies that offer consumer financial products and services, a category that includes most insurance providers (insurers and agencies), fall under the jurisdiction of the Gramm-Leach-Bliley (GLB) Act, the Federal Trade Commission's (FTC) Safeguards Rule and New York Department of Financial Services' Regulation 173, which require the safeguarding of sensitive customer data, as well as transparency of information-sharing practices. While these, as well as other regulatory frameworks, require that information security protocols be in place and outline some baseline requirements for those programs, they both leave the choice of exactly how to implement an information security program up to each organization's discretion. The Department of Financial Services proposed Regulation 500, once implemented, will further define the requirements for security protocols.

To help shape your organization's information security program, there are several information security frameworks available. These include the US federal government's NIST 800 program, a catalog of security controls constructed by the National Institute of Standards and Technology (NIST) and utilized to secure federal information systems, the ISO/IEC 27000 series, a set of standards developed jointly by the International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC), and the Control Objectives for Information and Related Technologies (COBIT), a security framework developed by the Information Systems Audit and Control Association (ISACA). These programs outline many of the steps and best practices an organization must perform to successfully implement a proper security posture that meets regulatory standards. These frameworks cover a wide variety of information security requirements, including data accessibility protocols, network architecture, and user awareness training, among many others. They are often very comprehensive (the latest version of NIST 800-53 contains 462 pages of recommendations), but allow organizations to easily explain to outside organizations, such as auditors or other third parties, the basis of their security controls.

PROFESSIONAL
INSURANCE
AGENTS

NYIA®
New York Insurance Association, Inc.

iiabny
Independent Insurance
Agents & Brokers of New York, Inc.
Trusted Choice®

To make this process easier, there are additional programs that can assist in implementing an information security program that meets the standards established by these frameworks. One of these programs is the Center for Internet Security (CIS) Critical Security Controls, which are considered a subset of the NIST 800 program and map to many other information security programs. The Controls echo many of the requirements put forward in the security frameworks outlined previously, but provides both a ranking order of which tasks to tackle when and benchmarks that need to be met for each. As the Controls are threat-based and updated regularly to adapt to new developments in the threat landscape, they are highly regarded as a helpful and timely tool for organizations trying to cut through the "fog of more" around cyber security (more attacks, more data, more tools, no clear plan of action).

To aid in the implementation of these programs, there are specific guiding principles for the actual tools used to manage and protect the data, operating systems, servers, and other programs covered by your information security program. A few examples of these guiding documents are the CIS Security Benchmarks, a consensus-based list of best practices developed by cybersecurity experts, and the Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIGs), technical guidance protocols developed by the Department of Defense. Both of these guideline documents help organizations ensure that the software and hardware that maintain their data are as secure as possible, by providing detailed technical configurations (the settings and switches) developed specifically to make networks and systems less hackable and more secure. While these guidelines may not appropriately apply to every aspect of an organization, for those who are directed by regulatory frameworks to protect important data, they represent excellent roadmaps to execute those directives at a technical level.

Implementing an effective information security program that complies with all of the appropriate regulatory frameworks that govern our industry can be a daunting task. However, there are a multitude of resources that can assist your organization in developing a successful information security program that effectively secures your data. By choosing the right framework and tools to comply with the regulations that affect our industry, your business can ensure its security program protects the vital data entrusted to it by your customers, your employees, and your vendors.

This article was prepared to highlight Guiding Principle #4—Establishing Standards. Learn more at Guiding Principles to Advance Information Security in New York.

PROFESSIONAL INSURANCE AGENTS

NYIA
New York Insurance Association, Inc.

iiabny
Independent Insurance Agents & Brokers of New York, Inc.
Trusted Choice