Published on *The National Law Review* https://natlawreview.com

The Importance of Information Security Plans

Article By:

Dena M. Castricone

In the first installation of our weekly series during National Cybersecurity Awareness Month, we examine information security plans (ISP) as part of an overall cybersecurity strategy. Regardless of the size or function of an organization, having an ISP is a critical planning and risk management tool and, depending on the business, it may be required by law. An ISP details the categories of data collected, the ways that data is processed or used, and the measures in place to protect it. An ISP should address different categories of data maintained by the organization, including employee data and customer data as well as sensitive business information like trade secrets.

Having an ISP is beneficial for many reasons but there are two primary benefits. First, once an organization identifies the data it owns and processes, it can more effectively assess risks and protect the data. Second, in the event of a cyber attack or breach, an organization's thorough understanding of the types of data it holds and the location of that data will expedite response efforts and reduce financial and reputational damage.

While it is a tedious task to determine the data that an organization collects and create a data inventory from that information, it is well worth the effort. Once an organization assembles a data inventory, it can assess whether it needs all the data it collects before it invests time, effort and money into protecting it. From a risk management perspective, it is always best to collect the least amount of information necessary to carry out business functions. By eliminating unnecessary data, there is less information to protect and, therefore, less information at risk in the event of a cyber attack or breach.

Some state, federal and international laws require an ISP (or something like it). For example, in Massachusetts, all businesses (regardless of location) that collect personal information of Massachusetts residents, which includes an organization's own employees, "shall develop, implement, and maintain a comprehensive information security program that is written . . . and contains administrative, technical, and physical safeguards" based on the size, operations and sophistication of the organization. The MA Office of Consumer Affairs and Business Regulation created a guide for small businesses to assist with compliance.

In Connecticut, while there is no requirement for an ISP, unless you contract with the state or are a health insurer, the state data breach law pertaining to electronically stored information offers a presumption of compliance when there is a breach if the organization timely notifies and reports under the statute and follows its own ISP. Practically speaking, this means that the state Attorney

General's office is far less likely to launch an investigation into the breach.

On the federal level, by way of example, the Gramm Leach Bliley Act (GLBA) requires financial institutions to have an ISP and the Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to perform a risk analysis, which includes an assessment of the types of data collected and how that data is maintained and protected. Internationally, the EU General Data Privacy Regulation (GDPR), which took effect on May 25, 2018 and applies to many US-based organizations, requires a "record of processing activities." While this requirement is more extensive than the ISP requirements noted above, the concept is similar.

Here is a strategy for creating an ISP for your organization:

1. Identify the departments that collect, store or process data.

2. Ask each department to identify: (a) the categories of data they collect (e.g., business data and personal data such as name, email address, date of birth, social security number, credit card or financial account number, government ID number, etc.); (b) how and why they collect it; (c) how they use the data; (d) where it is stored; (e) format of the data (paper or electronic); and (f) who has access to it.

3. Examine the above information and determine whether it needs to continue to be collected or maintained.

4. Perform a security assessment, including physical and technological safeguards that are in place to protect the data.

5. Devise additional measures, as necessary, to protect the information identified. Such measures may include limiting electronic access to certain employees, file encryption, IT security solutions to protect the information from outside intruders or locked file cabinets for paper documents. Training should always be an identified measure for protecting information and we will explore that topic thoroughly later this month.

National Law Review, Volume VIII, Number 278