BCLP. Client Intelligent

Insights

DO COMPANIES NEED A WRITTEN INFORMATION SECURITY PLAN ?

Jan 07, 2020

As of January 1, 2020, California became the first state to permit residents whose personal information is exposed in a data breach to seek statutory damages between $100-$750 per incident, even in the absence of any actual harm, with the passage of the California Consumer Privacy Act ("CCPA"). The class actions that follow are not likely to be limited to California residents, but will also include non-California residents pursuing claims under common law theories. A successful defense will depend on the ability of the breached business to establish that it implemented and maintained reasonable security procedures and practices appropriate to the nature of the personal information held. The more prepared a business is to respond to a breach, the better prepared it will be to defend a breach lawsuit. To help our clients prepare for the CCPA, Bryan Cave Leighton Paisner is issuing a series of data security articles to empower organizations to focus on breach readiness.

Do Companies Need a Written Information Security Plan ?

After a security breach occurs, customers, the media, regulators, and other interested parties routinely ask what measures the organization took to prevent the breach in the first place. In-house counsel should consider, therefore, whether their organization would be able to produce documents that demonstrate that it was attempting to secure the information. Many outside observers will expect that this includes, at a minimum, a written information security plan or "WISP." Indeed, states like Massachusetts require companies to implement and maintain WISPs if they own or license personally identifiable information ("PII") about a state resident. In the event of a data breach impacting Massachusetts residents, an organization must inform regulators and impacted residents whether the organization maintains a WISP and whether it has or intends to update the WISP.[1]

While the most stringent, Massachusetts is not alone in enacting legislation mandating the implementation of safeguards to protect PII. California, Oregon, Texas, Rhode Island and Illinois all have enacted laws requiring certain levels of security for PII. The CCPA will provide for statutory damages where an individual's sensitive information is breached if the plaintiff can establish that the organization failed to implement and maintain reasonable and appropriate security measures.

In February 2016, California published the California Data Breach Report, in which it specifically identified the 20 controls set forth in the Center for Internet Security's Critical Security Controls ("CIS") as the "minimum level of security" an organization should meet.[2] Indeed, the report states that the "failure to implement all of the Controls that apply to an organization's environment constitutes a lack of reasonable security." Thus, it will be imperative for an organization to show, at a minimum, that it has a WISP addressing the CIS controls.

Financial institutions and health care entities also will need to comply with the WISP requirements of the Gramm-Leach- Bliley Act Safeguards Rule ("Safeguards Rule") and the Health Insurance Portability and Accountability Act ("HIPAA"), respectively. Companies will want to carefully review the requirements of those laws when creating a WISP.

The format and contents of a WISP can greatly vary depending on an organization's operations. Nonetheless, there are areas of commonality. Although in-house counsel should be aware of any regulations and standards that apply to the specific organization's industry, at a minimum, the organization's WISP should include a description of the following:

- The administrative safeguards that exist to keep sensitive personal information secure;
- The technical safeguards that exist to keep sensitive personal information secure;
- The physical safeguards that exist to keep sensitive personal information secure;
- The process used by the organization to identify, on a periodic basis, internal and external risks to the information that it maintains;
- The specific employee who is ultimately responsible for maintaining and implementing security policies;
- The sensitive information maintained by the organization;
- Where and how sensitive information will be stored within the organization;
- How sensitive information can be transported away from the organization;
- Procedures that discuss the following:
  - Username assignment
  - Password assignment
  - Encryption format
  - Provisioning of user credentials
  - De-provisioning of user credentials (e.g., for terminated employees)

- Employee training on security topics
- Destroying data
- Retaining service providers that will have access to data

Some organizations choose to draft their WISP based on standards or formats created by third parties. Although there are many frameworks that can be looked to, some of the most popular frameworks are those published by the International Standards Organization ("ISO") or the National Institute for Standards and Technology ("NIST"). Other organizations retain third parties to certify that their WISP complies with these frameworks.

Tip: Your organization's WISP should, at a minimum, incorporate both the WISP requirements set forth under Massachusetts's law and in CIS.

For additional information, BCLP's Data Security Breach Handbook provides a comprehensive guide on how to respond when a breach happens and how to prepare your organization before one occurs. BCLP is working with clients to assess – and mitigate – risks by putting in place the policies, procedures, and protocols needed to address data security breach issues.

---

1. Mass. Ann. Laws ch. 93H, § 3 (2018)

2. Available at http://src.bna.com/cFY

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Linda C. Hsu

Los Angeles

linda.hsu@bclplaw.com
+1 310 576 2192
