SHUMAKER
Shumaker, Loop & Kendrick, LLP

Data Privacy Protection and Cybersecurity: A Business and Legal Primer

Business Information for Clients and Friends of Shumaker, Loop & Kendrick, LLP

July 1, 2016


Silverman


Spaulding


Cherry

Peter Silverman | psilverman@slk-law.com | 419.321.1307
Matt Spaulding | mspaulding@slk-law.com | 419.321.1455
Doug Cherry | dcherry@slk-law.com | 941.364.2738

The news regularly reports on data breaches and cybersecurity. While we read about the biggest breaches – Home Depot, Target, Anthem, JP Morgan, Wyndham – probably every business has been hacked and will be hacked again. According to a 2015 IBM study, the average cost of the 350 major data breaches it studied in 2014 was $3.8 million.[1] This is an issue that demands everyone's attention.

This article is a business and legal primer to advise on how to protect against, and respond to, cybertheft. It's neither legal advice nor a detailed how-to manual. Rather, it's a guide for developing a data privacy protection and cybersecurity plan appropriate to any business.

The simple message is this:

- Develop a team comprised of your specialists in computer and information technology (IT), insurance, risk management, law, and public relations. (In a small business, the owner may wear most of these hats.)
- Develop a written plan to:
  - protect your company and the private information of your customers, and employees;
  - respond to a breach; and
  - restore your system.
- Implement the plan company-wide -- real implementation, not lip service.

At Shumaker, we have experts in this area, and we're glad to help you develop and implement a policy appropriate to your business, and to do so with the maximum protection of confidentiality under the attorney-client privilege.

In our discussion below, we've italicized some words commonly used in discussing cybersecurity issues to help familiarize you with them. And we've added footnotes for further reading on standards and legislation we discuss.

1. Who does this apply to?

Government data privacy protection laws apply to any business that has employees or customers. The regulations relate to protecting your employees' private data, primarily health and financial (known as *personally identifiable information or "PII"*), and remediating any harm to the employees or customers stemming from a breach of the system.

Another policy applies if your business is part of the nation's *critical infrastructure* (for example, energy, transportation, chemicals, manufacturing, and defense). As a matter of national security, the federal government wants to make sure that these businesses continue to function and are protected from attack and data piracy.[2]

Beyond these legal requirements, your business needs to protect its operations and goodwill against malicious hacking or ransomware that aims to crash your system, steal your proprietary data, and destroy your goodwill.

[1] - 2015 Ponemon Institute/IBM Data Breach Study, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEW03053WWEN.

[2] - EO 13636, February 12, 2013, Improving Critical Infrastructure Cybersecurity, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

2. Assemble a team

Putting together a plan requires a team. The team is basically the same if you're a small or large business, just scaled appropriately. Even if you're a small business, you should have a plan that addresses any private data you have on customers and employees. That's a legal requirement. For the small company, the team may simply be the owner consulting with his or her insurance agent, computer service, and lawyer. The larger the company, the more sophisticated the team needed.

Here are the elements of the team, and how they contribute to the elements of the plan:

First, you need your managers and especially those who manage IT and risk.

Second, you need a cybersecurity expert to help you (i) *identify* the data you need to protect; (ii) *protect* the data and use *penetration testing* to probe your protection; (iii) *detect* intrusions; (iv) *respond* to intrusions and mitigate the harm; and (v) *recover* from any damage.

Third, you should obtain *cybersecurity insurance*. (Your CGL policy may provide coverage, but don't count on it.) Your insurance agent and the carrier should help review your procedures and may provide discounted rates for having a good policy and implementing it well.

Fourth, you should have counsel with expertise in this area. There are certain benchmarks to hit to manage your risks appropriately, and counsel will help you meet these standards. Counsel also will help create the response and remediation part of your plan, and review the sufficiency of your insurance coverage. Response and remedies are complex areas involving many considerations, including state and federal statutes, overlapping law enforcement agencies, and whether (and when) to contact law enforcement and potentially harmed individuals. Further, you need to deal proactively with potential business risks like civil lawsuits or government investigations or lawsuits. Finally, counsel can help you prepare the plan with the maximum protection of confidentiality under the attorney-client privilege.

Fifth, you should have a public relations expert. These problems hit fast and hard and can become public quickly. You want to preserve your company's goodwill, and to assure potentially affected customers and employees that you're addressing the problem aggressively with steps to protect them from harm.

3. Create the plan

You need a written cybersecurity plan, sometimes called a *Written Information Security Program ("WISP")*, which should include an *Incident Response Plan ("IRP")*. Don't simply pull one off the internet. The plan should be tailored to your company's specific needs.

If you're a $100,000 company, the plan can be short, but should address the points discussed above. Legally, the government recognizes that companies should adopt policies appropriate to their size and the risks they face.

Larger companies face more challenges. Special statutes and regulations apply if you're in the health[3] or financial field,[4] or if you're part of the nation's critical infrastructure.[5] Those standards can also be looked to for general application by companies not in those fields. The Federal Trade Commission, which regulates data privacy and breach, has issued two sets of guidelines on setting up policies.[6] There are also International Organization for Standardization ("ISO") standards, especially important for international companies, which have requirements for adopting and implementing an *Information Security Management System ("ISMS")*.[7] Counsel specializing in this area should help you navigate these issues.

Make sure the plan addresses your dealings with companies that share or store your data. You should have data security contract clauses in your contracts that require vendors to have a plan that meets certain standards and to carry cyber-insurance.

[3] - Health Information Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. §300gg, 29 U.S.C. §1181, *et. seq.*, 42 U.S.C. 1320d, *et seq.*, 45 CFR 144, 146, 160, 162, and 164. *See also* The Health Information Technology for Economic and Clinical Health Act (HITECH), and the Genetic Information Nondiscrimination Act (GINA).

[4] - The Gramm-Leach-Bliley Act (GLB), 15 U.S.C. §6801 *et. seq.*, 16 CFR § 313.1 *et. seq.*, 314.1, *et. seq. See also* Fair Credit Reporting Act (FCRA), Fair and Accurate Credit Transactions Act of 2003 (FACTA), and Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.

[5] - *Cybersecurity Framework*, National Institute of Standards and Technology (NIST), http://www.nist.gov/cyberframework/.

[6] - *Personal Information Guide* (2011): https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business; and *Start With Security* (2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[7] - ISO 27001 – 27005.

4. Implement the plan

Don't simply develop and publicize your plan, and then put it in the files. You'll have no actual and no legal protection. You need to implement it and test it.

The National Institute for Standards and Technology ("NIST") has produced a *cybersecurity framework* for critical infrastructure industries to follow. Part of the framework describes what it calls *implementation tiers*, which provide a helpful lens for developing implementation goals.

Each tier looks at the business' cybersecurity plans, implementation, and integration with third parties. Companies should try to ascend the tiers, as appropriate to the size and data-sensitivity of the business, in each of these areas. Here are the four tiers:

- *Tier 1 (Partial)*: initially addressing each of these issues;
- *Tier 2 (Risk Informed)*: approving and having general company-wide awareness of policies and external participation;
- *Tier 3 (Repeatable)*: Regularly updating and fully implementing policies and external participation; and
- *Tier 4 (Adaptive)*: Implementing a comprehensive continuous improvement[8] cybersecurity culture for policies, implementation and external participation.

The whole team should be involved in implementation, and the whole company should consider the plan and implementation part of its culture. The best companies in the world are vigilantly sharing information and updating their plans.[9]

Conclusion

You don't need to technically master all the information in this article to develop and implement a smart plan, though it would be good to become familiar with the concepts and the terminology. All you really need to know is that you should assemble the right team, develop an appropriate plan, and implement it. If you already have a plan that you're implementing, you should be reviewing and adapting it.

Shumaker has a team of lawyers with expertise in cybersecurity, and we'd be delighted to help you develop and implement your plan.

[8]- Often referred to as *Plan-Do-Check-Act ("PDCA")*. *See, e.g.* ISO 9001:2015, §0.3.2.

[9] - *See, for example*, The Information Technology-Information Sharing and Analysis Center (IT-ISAC), http://www.it-isac.org/.