SoCal Privacy Consultants
Lean. Sustainable. Legally Defensible.

Legally Defensible – What is it and How to Approach it

In the information privacy and security context

March 29, 2017

Background

Michael Cox's first privacy client suffered three breaches within 18 months. In 2007, he testified before three FTC lawyers for two hours in their Washington, D.C. office on behalf of his client. Despite the client's external lawyers indicating this was usually a lawyer to lawyer discussion, he volunteered and in fact insisted. He thought having an independent consultant describe what took place and what he was doing to build a proper security program could make a difference in how the company was perceived. In 2008, the client entered into a 20-year consent order with the FTC. However, the client suffered no financial penalties and was required to have biennial third-party audits for only the first 10 years of the order, instead of the entire 20 years as is predominantly the case.

Cox's preparation paid off. However, the experience of sitting across from the FTC lawyers caused him to think deeply about how to convey to future clients the importance of pursuing a legally defensive posture.

Meaning of Legally Defensible

SoCal Privacy uses "legally defensible" posture to mean utilizing a comprehensive risk management and controls system of governance that provides assurance that reasonable measures are in place that can be defended as a legally compelling or persuasive argument to a regulator or plaintiff judge or jury. This system of governance should be implemented in a thoughtful manner and reasonable for each company's size, scale, and complexity. Legally Defensible does NOT mean breaches will never occur, all lawsuits will be defeated, or regulator fines never assessed. However, companies in a legally defensible posture are able to:

- mitigate the risk of a breach occurring (avoid the avoidable);
- mitigate the risk of the most egregious penalties when an investigation occurs; and
- facilitate a defensible position when facing lawsuits by consumers, employees, clients, and shareholders due to compromise of data, systems, technology, and/or IP/trade secrets ("compromise").

Just like there is no absolute privacy or security, there is no absolute legal defensibility. Legal defensibility is aspirational in nature, as the goal is constantly moving and thus can only be continually pursued to get as close as possible to achieving it. Legal defensibility is a mindset and approach: "What do I need to do to demonstrate in a court of law or to a regulator that our privacy and security program is comprehensive and reasonable in nature?"

The Need to Stay Current

The pursuit of legal defensibility requires understanding and staying current on:

- Published data breach reports and resources, such as the Verizon Data Breach Investigations Report[1]. Their 2017 report's dataset includes over 40,000 incidents, including 1935 confirmed data breaches, which is a rich dataset from which to draw conclusions about your threat environment and what effective controls should be implemented.
- Following your regulators' guidance and enforcement actions, which sometimes sets new precedent and expectations.
    - As an example, in February 2016 the California State Attorney General (AG) stated that "the 20 controls in the Center of Internet Security's Critical Security Controls (Top 20 CSCs) identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security"[2].
- What responsible companies in your industry are doing to strengthen their security posture.

1 You can download the report at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017

2 https://oag.ca.gov/breachreport2016

What Does Legally Defensible Look Like?

A Legally Defensible Privacy and Security Program has three components:

- Baseline compliance to appropriate regulations, guidance, industry standards, and enforcement action protocols. Compliance cannot be a check-the-box approach. It is the floor, but alone is not defendable because laws and regulations cannot keep up with emerging threats and technologies. For example, while the HIPAA Privacy and Breach Notification Rules were updated in January 2013, the HIPAA Security Rule is about 20 years old. Mobile devices and apps were not prevalent when the Security Rule was developed. The PCI-DSS standard is very straightforward, however the FTC stated in 2016 that that it would investigate how PCI-DSS operates, including probing nine QSA vendors. As noted above, the Top 20 CSCs should be adhered to based on the California State AG's guidance. Using the NIST Cybersecurity Framework, easily facilitates incorporation and harmonization of a variety of different standards. However again, compliance alone is not enough. Many "compliant" organizations have suffered breaches, regulatory penalties and enforcement actions, class action lawsuits, and huge reputation/brand risks.
- Systematically identifying foreseeable risks and applying reasonable standards of care both on a periodic basis, such as annually, and as a part of everyday risk-informed decision-making (Privacy/Security-by-Design – P/SbD) to mitigate risks to an acceptable level. The P/SbD process and owners must be well-defined. A future write-up will be dedicated to this subject.
- A system of governance including governance at the organizational level and of the data privacy lifecycle, P/SbD, third-party management, periodic evaluations, and policies and procedures. A risk management and control lifecycle management framework should govern the entire program. Documentary evidence of governance should be maintained and easily retrievable. Roles and responsibilities should be clearly defined and communicated. This will be further discussed in a future Governance write-up.

Summary

Organizations must do everything reasonable to prevent a breach. As there is no absolute privacy or security despite all reasonable efforts, organizations must assume that at some point they will be compromised. Statistics bear this out. And when an organization operates under the assumption that it will be breached, it must also assume it will be involved in a lawsuit and/or regulatory investigation.

Anticipating this eventuality and building a program that is prepared to defend its comprehensiveness and reasonability is what legal defensibility is all about.

Feel free to reach out to us if you have any questions. SoCal Privacy Consultants perform gap assessments and help organizations build lean, sustainable, and legally defensible privacy and security programs.

Michael Cox, CIPP/US | President and Founder
SoCal Privacy Consultants | www.socalprivacy.com
mcox@socalprivacy.com | m: 619.318.1263