What is Reasonable Security?

Version 1.1

October 11, 2020

info@assuredSPC.com

Assured SPC

Reasonable Security in the Law

The requirement to implement "reasonable security" practices and procedures or "reasonable safeguards" is embedded in US Federal, US State, and International laws. Examples include the Gramm-Leach-Bliley Act (GLBA), FTC administered law on unfair and deceptive trade practices, HIPAA, privacy laws including GDPR, the California Consumer Privacy Act (CCPA) and the NY SHIELD Act. The definition of reasonable security may feel elusive and ambiguous. I speak with many attorneys that focus on privacy and data security and whenever I meet a new one, I ask for their definition of "reasonable security". The most cogent legal definition comes from tort and criminal law and the definitions of a "reasonable person" and that person's "duty of care". The purpose of including the phrases "reasonable security" or "reasonable safeguards" in privacy and data security laws is that there is a concern about "negligence" or the "duty of care" to prevent harm. GLBA and the NY SHIELD Act are specific that security safeguards need to include administrative, technical and physical safeguards. In short, the question is "What administrative, technical and physical safeguards would a reasonable person take to prevent harm from a security event?"

So, to understand "reasonable security" we need to understand "reasonable person", "duty of care" and who could be harmed.

Definitions

Reasonable Person: If you do a Google search on "reasonable person" you will get about 130 million results. The definitions don't vary much. The reason there are so many results is that this is a very important concept in law and it is discussed a lot. Free-Dictionary.com defines reasonable person as "not an average person or a typical person but a composite of the community's judgment as to how the typical community member should behave in situations that might pose a threat of harm to the public." "The law takes into account a person's knowledge, experience, and perceptions in determining whether the individual has acted as a reasonable person would have acted in the same circumstances." The takeaway from this definition is that there is no perfect person and one does not need to act in a perfect way, but a business must consider what it knows, generally accepted experience and perceptions.

Duty of Care: Wikipedia defines duty of care as "In tort law, a duty of care is a legal obligation which is imposed on an individual requiring adherence to a standard of reasonable care while performing any acts that could foreseeably harm others." "Foreseeable harm" is part of the historical definition of duty of care and it explains why a security risk assessment is a very important administrative safeguard relating to reasonable security. **Completing a security risk assessment and tracking the implementation of the risk mitigation safeguards provides documentation that a business has evaluated and taken action on foreseeable risk.** In the US, most states have developed a multi-factor test to determine whether a reasonable person has breached his duty of care.

Who can be harmed: When cybersecurity events occur or personal information has been exposed, individuals and the businesses can be harmed. Individuals can be harmed by identity theft and fraud. Businesses can be harmed by loss of money, e.g. fraudulent money transfers, cost of identification and response to the security event, loss of intellectual property and loss of customer confidence. *In states where the duty of care is only defined by whether harm was foreseeable, there are additional harms to business.* They would come from the potentially infinite cost of damages and potentially infinite cost of safeguards. To prevent these two harms, courts in most US states use a multi-factor test to limit damages and cost of safeguards. **Another significant role of the security risk assessment and treatment**

plan is that it allows the business to show that it balanced the risk to its customers, to itself and to others in executing its duty of care.

Focusing only on Technical Controls

Many organizations think that cybersecurity risk is an IT function and reasonable safeguards are only about technical controls like firewalls, password strength and encryption of data. But to implement "reasonable security", businesses must implement a risk-based security program with documentation and effort that starts with a cybersecurity risk assessment. And the business needs to include administrative controls that would include security policies. Procedures like incident response plans need to be defined and tested. It is likely and sometimes legislated that businesses need to evaluate the risk that is created by its relationship with its product and business process supply chain, i.e. third party or vendor risk management. **Technical safeguards are not sufficient.**

Reasonable Security and Customer Requirements

It would be straight forward to implement cybersecurity that was reasonable for the business, its customers and others if the business only had to follow a risk-based approach that balanced its duty of care responsibilities across these stakeholders. But, just as every business needs to evaluate risks from its vendors and suppliers, it is often a vendor or supplier to its customers that have the same need. The challenge of responding to customer driven risk management is that customers can impose security safeguard requirements on a business that it does not view as 'reasonable". This reality can be a burden that ideally can be negotiated with significant customers.

Summary

Reasonable security is a very important concept but it is a legal concept first. The translation of the legal concept of reasonable security into administrative, technical and physical safeguards needs to be done through a risk-based security program. Risk-based security programs begin with an inventory of assets that need to be protected for the business, its customers and others in society. Then a threat-based risk assessment is done with a result that defines just the right amount of administrative, technical and physical safeguards needed to protect the assets and stakeholder interests. Many organizations focus only on technical controls like firewalls, passwords, and encryption when they implement a security program. This would not consistently be defensible as "reasonable" and could be more costly than using a risk-based approach to privacy and data security.

Barry Weber, ITIL, CISM is a vCISO and the Privacy Leader for Assured SPC. Barry has been a CIO, CTO and VP of IT for companies across many industries for 2 decades before focusing on cybersecurity and privacy in 2015.

Assured SPC helps organizations minimize compliance risk and achieve security and privacy requirements and goals. We assist organizations assess, design and implement operational compliance requirements.