“Cyber War & the Boardroom: Defining of ‘Reasonable Security’”

By David Willson*

Can your company be breached by hackers? Could you have prevented that breach? If you suffer a breach what are the ramifications: Potential class-action lawsuit or an investigation and fines by a regulatory agency? Assuming you can’t prevent the breach,[1] can you avoid lawsuits by disgruntled customers or investigations by a State Attorney General (AG), the FTC, SEC, HHS, PCI (Purchase Card Industry), etc.? Prevent, probably not, but successfully defend; most likely!

The common factor in most of data breach class-action lawsuits as well as investigations by regulatory agencies is the allegation that the breached company failed to implement “**reasonable security or protections**” to prevent the breach. Logically then, if you implement “reasonable security and protections” you should be able to confidently defend your security practices and actions.

Reasonable Security

If you haven’t thought about what constitutes “reasonable security” lately or ever maybe the time to do so is right now! Most of us have become numb to the weekly news reports of another data breach, and shortly thereafter the report of a class-action suit being filed.[2] Sadly these reports are only a small percentage of the actual number of breaches. Realistically the number is closer to two or more a day.[3] Once a company is outed as having been breached, the potential for damage to the company’s reputation and the threat of a lawsuit hangs in the air. These are not the only threats plaguing breached companies though. Many companies have also found themselves suddenly being investigated and possibly fined by regulatory agencies such as the FTC, SEC, HHS or a State AG.

Since most of the data breach class-action suits and regulatory investigations claim breached companies did not implement “reasonable security or protections,” it is logical to assume that “reasonable security” is the antidote to getting sued or fined. This article will look at some of the claims and allegations made in the lawsuits and agency findings as well as the requirements or guidance provided by regulatory agencies and States in order to develop a clear definition and standard for “reasonable security.” As we will see, most of the allegations against breached companies include a failure to implement or properly utilize software, hardware and techniques which are very basic. Bottom-line, most companies are not even implementing the basics.

---

[1] “I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.” See, Federal Bureau of Investigation Speeches, RSA Cyber Security Conference San Francisco, CA (March 2012).

[2] Less than 24 hours after the Anthem breach was publicly acknowledged a lawsuit was filed. *See,* Schenker, Lisa, “Anthem in legal crosshairs as three class-action lawsuits filed over breach.” Modern Healthcare (Feb. 2015).

[3] Identity Theft Resource Center (ITRC) Data Breach Reports, (Dec. 2015), http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf.

Class-Action Complaints

A sample of the allegations in the 13 class-action lawsuit complaints I researched include: the breached companies did not use encryption, failed to use good passwords, didn't use a firewall or improperly configured the firewall, did not use or failed to properly update anti-virus, failed to implement good vendor security, failed to segment networks separating sensitive information from common or public networks, failed to implement adequate intrusion detection systems, failed to notify customers in a timely manner, continued to utilize outdated software/hardware and, or failed to properly implement a legally or contractually required standard like PCI.[4] These companies include Target, Home Depot, Anthem, Experian, Trump Hotels, Wendy's, Wyndham, just to name a few.

- Of the 13 class-action lawsuits which I reviewed, 10 of the breached companies were alleged to have failed to use or improperly used encryption. Security practitioners for years have been encouraging companies to use encryption, and many data privacy laws such as HIPAA and some enacted by various States have stated that there would be no requirement to notify if the data that was breached was encrypted.

- The complaints also alleged, in some cases specifically and others more broadly, that the breached companies failed to implement various industry standards and "best practices."[5] "Best practices" is a term frequently used in the security industry. One of the most popular set of so-called "best practices" is "The CIS Critical Security Controls for Effective Cyber Defense," aka "SANS Top 20." [6] Many States recommend "best practices" as part of a good or reasonable security program and refer to the "SANS Top 20" as an example of "best practices." As stated, many of the 13 companies researched did not even implement basic security standards or did not do so competently. Therefore, it would appear that the recommended best practices really equate to "basic practices." Practices such as inventorying what assets your company has, restricting administrative access, setting up intrusion detection and boundary defenses would appear to be commonsense basics that all should implement.

- In five of the 13 complaints, the breached companies failed to destroy sensitive information once it was no longer needed. This is easily addressed via a policy that identifies what should be destroyed, and when, on a continuing basis, similar to implementing regular backups.

[4] *See* "Reasonable Security Breached Companies Spreadsheet" at: http://www.psatec.com/downloads/, or at: https://cyberwarandtheboardroom.wordpress.com/about/, wherein I reveal my research on class-action lawsuit complaints.
[5] The standards referred to here are not legally required or such as HIPAA or GLBA, or contractually required such as PCI, but are industry recommended standards.
[6] SANS, at: https://www.sans.org/critical-security-controls/.

- In one regard the research indicates companies are getting better. Only two of the 13 complaints claimed that the breached company did not utilize good passwords. The complaints against Wendy's and Target allege they did not assign strong passwords to their security solution in order to prevent application modification.

- In five of the complaints, the companies failed to employ regular updates to software or replace outdated hardware or software. Security is a process and cannot be treated as a "set and forget" concept.

- Three of the complaints alleged that the companies either did not have a firewall or the firewall was improperly configured.

The above are just some of the allegations. See the "Reasonable Security Breached Companies Spreadsheet" for all of the research.[7]

The allegations are not that companies were tricked or did not implement the latest and greatest security, but did not do the basics. For instance, none of the 13 class-action complaints alleges that any of the companies negligently clicked on an email attachment or link that introduced malware to the network causing the breach. It is unlikely a company would be accused of being negligent any time soon for a mistake or an incident wherein an employee was tricked by a hacker. Mistakes happen, but companies must still show due diligence in their efforts to protect data.

One thing is clear in all of the complaints: All breached companies were on notice about the pervasiveness of hackers and the overwhelming potential for such companies to be the next victim. In fact four of the 13 companies had previously suffered a breach that was publicly known. Realistically, most of the companies likely suffered a breach previously but the breach did not become publicly known.

If by law or contract you are subject to a particular standard, e.g. GLBA, HIPAA, PCI, etc., or regulatory guidance, it likely behooves you to at least strive to meet that guidance or standard and ensure legal compliance.[8] If some of the requirements don't make sense for your company, you may be able to make a sound business argument as to why that requirement in the guidance or standard was not applicable to your company and circumstances and may actually cause greater security issues.[9]

States Guidance

We can also find some guidance as to what might be considered "reasonable security" by reviewing guidance provided by States in their privacy and data breach

---

[7] *Id.* at note 4.

[8] "Legal compliance is defined as an organization's ability to maintain 'a defensible position in a court of law.'" T.D. Breaux, A.I. Antón, C.-M. Karat, J. Karat, "Enforceability vs. accountability in electronic policies", IEEE 7th International Workshop on Policies for Distributed Systems and Networks (POLICY'06), London, Ontario, pp. 227-230, Jun. 2006.

[9] For a more thorough review of FTC regulatory enforcement actions surrounding "reasonable security," *see*, Breaux, Travis D. and Baumer David L., "Legally 'Reasonable' Security Requirements: A 10-year FTC Retrospective," at: cs.cmu.edu/~./breaux/publications/tdbreaux-cose10.pdf.

laws. The following States, and to some degree most states, all advocate or require any business that collects personal information to implement "reasonable security" protections or practices. This is not an exhaustive list but a sampling.

- California: "Requires businesses to use '**reasonable security** procedures and practices…to protect personal information from unauthorized, access, destruction, use, modification, or disclosure.'"[10]

- Oregon: Businesses "shall develop, implement and maintain **reasonable safeguards** to protect the security, confidentiality and integrity of the personal information, ..."[11]

- Rhode Island: Businesses "shall implement and maintain a risk-based information security program that contains **reasonable security** procedures and practices appropriate to the size and scope of the organization; . . . ."[12]

At this point you may be noticing that "reasonable" is a very subjective standard. In some instances though, like California, the guidance includes a recommendation to review and seek to implement the SANS Top 20.

Regulatory Guidance and Standards

When it comes to federal regulatory guidance and rules, the FTC, via the "Standards for Safeguarding Customer Information (Safeguards Rule)," appears to be the most active in investigating and pursuing breaches. The Safeguards Rule states in part: "This part [§314.1], which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act (GLBA), sets forth standards for developing, implementing, and maintaining **reasonable** administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[13] Companies must show due diligence in protecting customer information, due diligence being defined as, "the care that a reasonable person exercises to avoid harm to other persons or their property."[14]

A review of an FTC action against a breached company should shed some light on what "reasonable security" may look like. For instance, in the Petco case, the FTC claimed that Petco:

- Created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business need to keep the information, in violation of bank rules;
- Did not use readily available security measures to limit access to its computer networks through wireless access points on the networks;

[10] California Civil Code §§ 1798.29, 1798.80 et seq.
[11] Oregon § 646A.600 to .628, 2015 S.B. 601, Chap. 357.
[12] Rhode Island Gen. Laws § 11-49.2-1 et seq.
[13] 16 CFR Part 314.
[14] Meriam-Webster, "Definition of Due Diligence," at: http://www.merriam-webster.com/dictionary/due%20diligence.

- Failed to employ sufficient measures to detect unauthorized access or conduct security investigations;
- Failed to encrypt personal information; and,
- Stored customer information in files that could be accessed anonymously by using a commonly known default user ID and password.[15]

As stated by Joel Hanson in his 2008 article,

> If a business is attacked by hackers or other kinds of thieves stealing sensitive consumer information, the FTC may not take action against the business if it finds that the business has employed **reasonable** and appropriate measures to secure the personal information of its customers. Such measures include adequate security software, protections against well-known hacking methods, limiting the time personal information is stored, limiting access to networks, and having a method of detecting and investigating unauthorized access. Further, businesses should take precautions against the threat of insider theft of consumer information.[16]

The guidance by the FTC states,

A sound data security plan is built on 5 key principles:

1. Take stock. Know what personal information you have in your files and on your computers.
2. Scale down. Keep only what you need for your business.
3. Lock it. Protect the information that you keep.
4. Pitch it. Properly dispose of what you no longer need.
5. Plan ahead. Create a plan to respond to security incidents.[17]

Each of these principles includes further details for implementing "reasonable security."

Again, the term **reasonable** is used, but with very little specific guidance and criteria. In most guidance wherein the term reasonable is use, the organization then points practice criteria like the SANS Top 20 or various standards like NIST and ISO. Meeting a "reasonable security" standard requires implementing and deploying a plan that you, the leadership of the company, can confidently defend. One that will make it difficult for an attorney in a class-action suit, or an agency like the FTC or State Attorney General to claim you were negligent in your effort to protect data. Certainly you should assume that "reasonable security" would include meeting "basic security" standards.

Getting Started

[15] Joel B. Hanson, Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements, 4 Shidler J. L. Com. & Tech. 11 (5/23/2008), at http://www.lctjournal.washington.edu/Vol4/a11Hanson.html.
[16] *Id.*
[17] "Protecting Personal Information, A Guide for Business," Federal Trade Commission (2011) at: business.ftc.gov/privacy-and-security.

To begin, start with an assessment of the risks to your organization and the vulnerabilities in your processes and procedures.[18] Develop a plan, and implement the basics that make sense by choosing from guidance or standards like the SANS Top 20, and work from there. Capture how you will accomplish your new security in a written plan that is very detailed and train all employees so the plan and procedures are understood and implemented by the entire company. Finally, ensure the plan includes measures to identify a breach and then the steps to pursue once this identification is made. Such steps include, sample statements to release to the public, what vendors to call for support, conducting forensics, how to notify customers and shareholders and when, etc.

One last piece. There is a growing trend wherein companies employ a law firm to oversee and manage their incident response. If the vendors that you use to investigate the breach are hired by the law firm supporting you, then any communication between you, the vendors and the law firm are, for the most part, attorney-client protected communications.

Despite what many believe, security is not rocket science. It is commonsense and hard work. Do what's right and stand by your decisions. Burying your head in the sand won't make it go away or make it better. The goal is not to prevent a breach. The goal is to prepare for that ever looming breach, lower risk and reduce or eliminate liability to minimize or eliminate the threat of a lawsuit or fines, by implementing a "reasonable security" program you can confidently defend.

* David Willson is a licensed attorney, CISSP and owner of Titan Info Security Group. He focuses on helping companies with risk management, cyber security, risk assessments, policy review and development, incident response investigation management, messaging, reputation management, cyber awareness training, and cyber and data protection legal issues, among other issues. He can be reached at david@titaninfosecuritygroup.com.

[18] This does not refer to a technical vulnerability scan, e.g. vulnerability assessment or penetration test, which should be accomplished at least annually, but this refers to seeking to understand the vulnerabilities in your processes and procedures and how you physically control access to and the flow of sensitive data.