Global Knowledge®

Expert Reference Series of White Papers

"Reasonable Security" Best Practices: Learning From Noteable Data Breaches

info@globalknowledge.net

www.globalknowledge.net

“Reasonable Security” Best Practices: Learning From Notable Data Breaches

David Willson, CISSP

Introduction

Ask most IT or security executives whether their organization has been or will be breached this year, and most, if honest, will say yes. Ask the C-Suite the same question, and their answer will likely be no. Security and IT professionals rank security number one whereas the C-Suite ranks security number nine (The Economist, “The Cyber-Chasm”). The reality is that data breaches are increasing, but companies are still wholly unprepared. The lack of preparedness is causing huge recovery costs and loss of both business and customers (Ponemon, “2016 Cost of Data Breach study”).

If you suffer a breach, what are the ramifications: potential class-action lawsuit and/or an investigation and fines by a regulatory agency? At this point, most, if not all, companies should assume they cannot prevent a breach and, in fact, should assume a breach is inevitable. While speaking at the RSA conference in San Francisco in 2012, FBI Director Robert Mueller stated, “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.” Despite the inevitable breach, is it possible to avoid lawsuits by disgruntled customers or investigations by regulatory agencies? Maybe. Can you successfully defend against them? Most likely!

The common factor in most data breach class-action lawsuits and investigations by regulatory agencies is the allegation that the breached company failed to implement reasonable security or protections to prevent the breach. It logically follows that if you implement reasonable security and protections, you should be able to confidently defend your security practices and actions.

If you haven’t thought about what constitutes reasonable security lately, or possibly ever, the time to do so is right now. Most of us have become numb to the weekly news reports of another data breach and the report of a class-action suit being filed shortly thereafter. In fact, less than 24 hours after the Anthem breach was publicly acknowledged, a lawsuit was filed. 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. According to the Identity Theft Resource Center (ITRC) Data Breach Reports, 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. Many companies have also found themselves suddenly being investigated and possibly fined by regulatory agencies such as the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), Health and Human Services (HHS) or a State Attorney General. 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. Here is the spoiler alert: there is no clear definition for reasonable security or any standard one could point to that will prevent a breach or allow a breached company to completely avoid all lawsuits or regulatory investigations.

Class-Action Compliance Failures

I researched a sampling of companies such as Target, Home Depot, Anthem, Experian, Trump Hotels, and Wendy's. The companies in the 13 class-action suits had not implemented basic security or even some form of best practices. According to the allegations, here are some of the areas they failed in security:

- Use of encryption
- Destroy sensitive information
- Use good passwords
- Use a firewall or improperly configured the firewall
- Use or failed to properly update anti-virus
- Implement good vendor security
- Segment networks separating sensitive information from common or public networks
- Implement adequate intrusion detection systems
- Notify customers in a timely manner
- Outdated software/hardware
- Unsecure environment to accept, process, or store credit card information

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 patients or residents if their personal data that was breached was encrypted.

Allegation excerpt:

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." "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" (CIS Critical Security Controls). Many states recommend "best practices" as part of a good or reasonable security program and refer to the CIS Critical Security Controls for Effective Cyber Defense as an example of "best practices." 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."

Best Practice: Create an inventory all assets use to store or transmit data; restrict employee and vendor administrative access to data requiring a showing of a need to know; implement intrusion detection (IDS) and boundary defenses, e.g. firewalls, etc.

Destroy Sensitive Information

In five of the 13 complaints, the breached companies failed to destroy sensitive information once it was no longer needed.

Recommended Best Practice: Similar to the basic requirement of implementing regular backups, draft and implement a policy that identifies data to be destroyed and how often.

Good Passwords

There is some good news. The research indicates companies are getting better with regard to basic security issues the security industry has been preaching about for years. Only two of the 13 complaints stated 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. The other companies were apparently utilizing good passwords.

Best Practice: Require the implementation of good passwords that are neither words nor easily guessed. Whether passwords should be changed frequently is a pet peeve of mine. There are great arguments both for and against doing so, but this is a discussion for another time.

Outdated Software/Hardware

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.

Best Practice: Implement policies and procedures to ensure updates are accomplished. This is a huge task for many companies since software updates, in many cases, should be sandboxed and tested prior to implementation. However, ignoring it creates vulnerabilities.

Firewall Usage or Improper Configuration

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

Best Practice: Perimeter defenses are key. You have to be able to detect at least basic to intermediate attacks. No single approach, procedure, tool or configuration, nor individual can prevent all intrusions, but not implementing basic measures in an attempt to detect intrusions is tantamount to negligence.

Data Breach Victims Common Failures

Basic Security Practices

For the most part, it appears that the companies researched were not tricked into allowing hackers in and were not compromised because they failed to implement the latest and greatest security. They simply did not implement the basics. For instance, none of the 13 class-action complaints allege that any of the companies negligently clicked on an e-mail 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. This is not to say that an e-mail phishing attack was not the method the hackers used because in many cases it was. The allegations of negligence did not highlight employee error or mistakes as one of the failures.

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 it had not become publicly known.

Compliant to Guidelines and Standards

If by law or contract you are subject to a particular standard, e.g. GLBA, HIPAA, PCI, etc., or regulatory guidance, it is strongly recommended to at least strive to meet that guidance or standard and ensure your company is legally compliant. Legal compliance is defined as an organization's ability to maintain a defensible position in a court of law. (See "Enforceability vs. Accountability in Electronic Policies.") 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. (See "Legally 'Reasonable' Security Requirements: A 10-year FTC Retrospective.") This is not to say that legal compliance will ensure your company is secure and will not be breached. Rather, it is a standard imposed by law, and that's it.

States Guidance

Some guidance as to what might be considered reasonable security does exist in state privacy and data breach laws. The following states 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'" (California Civil Code §§ 1798.29, 1798.80 et seq.).
- Oregon: Businesses "shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information. …" (Oregon § 646A.600 to .628, 2015 S.B. 601, Chap. 357).
- 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. …" (Rhode Island Gen. Laws § 11-49.2-1 et seq.).

At this point, you may have noticed that "reasonable" is a subjective standard. In some instances though, like California, the guidance includes a recommendation to review and seek to implement the CIS Critical Security Controls for Effective Cyber Defense.

Federal Regulatory Guidance and Standards

We can also find some guidance for reasonable security in federal regulatory guidance and rules. For instance, 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" (16 CFR Part 314). Companies must show due diligence in protecting customer information. *Due diligence* is defined as, "the care that a reasonable person exercises to avoid harm to other persons or their property" (Merriam-Webster).

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, which is 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;
- Failed to employ sufficient measures to detect unauthorized access or conduct security investigations;

- Failed to encrypt personal information;
- Stored customer information in files that could be accessed anonymously by using a commonly known default user ID and password (Joel B. Hanson, "Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements").

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.

FTC Guidance

The guidance by the FTC states that a sound data security plan is built on five 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 (Federal Trade Commission, "Protecting Personal Information, A Guide for Business").

Each of these principles include 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 used, the organization then points to practice criteria like the "CIS Critical Security Controls for Effective Cyber Defense" 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. A plan that will make it difficult for an attorney in a class-action suit, 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, which are what have been discussed thus far.

Prepare for the Inevitable Breach

Many companies I have spoken to claim they take cybersecurity seriously and invest a lot of money in it. However, in reality, much of it is invested in the latest and greatest technology or lip service paid to the effort by executives who don't really understand the risks and just want to throw money at the perceived problem. Very few seem to be willing to put in the hard work and effort to prevent a breach. If you found out tomorrow your company was breached, what would you do and who would you call? If the building caught on fire, you probably know the answer to these questions. Why do you not have similar answers for cybersecurity concerns?

What can you do in advance of a breach to prepare and either ward off or effectively defend a lawsuit and bad publicity? Despite efforts to prevent a breach, most companies today are in a reactive mode and are completely unprepared. The first action item is for the C-suite, not the IT department: conduct a risk assessment. The IT department, as well as all other departments, can and should be included, but the assessment must be sponsored, organized and conducted by the company leadership, which includes the CEO and other executives.

Identify and Assess Risks

Assess the risks to the organization and the information that is important to your company. This includes loss or theft of data as well as known vulnerabilities in your software and the processes and procedures you use. This does not refer to a technical vulnerability scan such as vulnerability assessment or penetration test, which should be accomplished at least annually. Instead, begin with generalized risks to all companies including the threat of hackers, malware, and viruses. Then review risks to companies in your particular industry such as financial, manufacturing, and retail. Finally, review any risks that may be specific to your company including insider threats, competitors, disgruntled employees, and customers. Once all risks are identified, develop a plan to address these risks.

Continue the assessment by developing a list of what information the company collects, processes and stores; examine how the information enters the organization, where it is stored, and where it leaves, who has access to it, whether inside or outside the organization, and what vendors have access or hold the data such as cloud providers, your accounting firm, payroll firm, IT support company, law firm, etc. In short: understand data flow. Furthermore, how is data at rest and in transit secured? Next, ask the IT department to provide an inventory of all assets that store or process data: smart phones, routers, firewalls, servers, desktops, etc. Ask the IT department if they are using "best practices" or some sort of standard (NIST, ISO, etc.) and exactly what practices and procedures they use, especially to control access inside and outside the organization, whether these are captured in writing and in logs of all activity.

Next, what policies related to cyber and information security exist in the company and are they captured in writing? If yes, who has read them, and does the organization have proof that they have been read and how often? Then, capture on paper the unwritten policies, draft those that don't exist, and update those that are older than a year. Policies should be reviewed and read by all at least annually. Once all policies have been updated and/or drafted, conduct cyber security awareness training. During this training, review all policies and ask for feedback. Frequently, policies are written in a vacuum and don't take into account how they may affect all functions of the company. Asking for feedback will allow you to adjust policies so they are not making life difficult for employees.

One of the primary policies/plans your company must have is a security policy/plan. Ensure your specific security plan/policy includes measures for identifying a data breach and the steps to follow once this identification is made. Such steps include how to identify a breach, who to call and when, sample statements to release to the public, which vendors to call for support, conducting forensics, how and when to notify customers and shareholders, etc.

Additionally, there is a growing trend wherein companies employ a law firm to oversee and manage their incident response. Using a law firm to hire and manage vendors, such as a forensic examiner, security company, public affairs company, etc., will ensure that any communication between you, the vendors and the law firm are, for the most part, protected under attorney-client privilege.

Conclusion

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 improve it. Security is also not a set-and-forget concept. It must be monitored and managed. Since 100% prevention is unrealistic, the goal is to deter and prepare for that ever-looming breach, lower risk, reduce or eliminate liability, and minimize or eliminate the threat of a lawsuit or fines, all by implementing a reasonable security program you can confidently defend.

Learn More

Let us help you create a cybersecurity solution that is right for your reasonable security and risk assessment. Visit www.globalknowledge.com or call 1-800-COURSES (1-800-268-7737) to speak with a Global Knowledge training advisor.

About the Author

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 concerns among other issues. He can be reached at david@titaninfosecuritygroup.com.