Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

System Security and Your Responsibilities: Minimizing Your Liability

With security incidents increasing almost exponentially every year, we need to protect our customer's information and ourselves more diligently. The increase in incidents will bring a rise to an increase of lawsuits claiming that we did not do our part to protect and secure the data we need to do business. Will a good security policy and sound security procedures stop a hacker from trying to gain access to your systems and networks? No, but it will greatly reduce his chances of success. Will a secure system and network...

Copyright SANS Institute

Author Retains Full Rights

AD

Streamline IT security environments and compliance processes.

Transforming IT Management.

System Security and Your responsibilities. Minimizing your Liability.

Introduction

We talk about the need for system security. With security incidents on the rise, many of us are doing our best to stay ahead of the hackers to protect our systems for numerous reasons. One of which is to protect the data on our system from falling into the wrong hands. There are many consequences if this should happen. First and foremost is that your systems most likely contain vital information that is the lifeblood of your companies business. If this information is lost or falls into competitors' hands it could be devastating to the future of your company through loss of revenue, company secrets and customers. Above and beyond all of this, what if this information falls into criminal hands and is used and or abused to the detriment of the people and or organizations who's information is stored on your systems? What are your responsibilities to them with regard to the protection of this information? Are you and or your company liable for any damages the result from the misuse of this data?

The Law

Recently there have been a number of laws that have been written regarding just this topic. The first governs the health industry that now has to follow HIPAA. HIPAA is the Health Insurance Portability and Accountability Act. President Clinton signed HIPAA into law in 1996. The main goals of HIPAA are:

1. Guarantee health insurance coverage of workers during job transitions.
2. Protect privacy of patient records.
3. Promote national, uniform security standards for the secure electronic transmission of health information.

Large and medium sized organizations must be compliant with HIPAA security requirements 24 months after the Final Rule is published. Smaller companies have 36 months to become compliant. Penalties for known misuse of individually identifiable health information and failure to comply with HIPAA security requirements can result in fines up to $250,000.00 and/or up to 10 years imprisonment.

If you are a financial Institution you are subject to the Gramm-Leach-Bliley Act of 1999. On November 12, 1999, President Clinton signed the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 106th Cong., 1st Sess. (GLBA). The GLBA applies to all national banks and federal branches of foreign bank that are subject to the supervision of the Federal Trade Commission (FTC), Security and Exchange Commission (FTC), Federal Reserve System (FRS), Office of Thrift Supervision (OTS), Office of the Comptroller of the Currency (OCC) or Federal Deposit Insurance Corporation (FDIC). The purpose of the Act is to the protection of customer information. This act requires banks to develop privacy notices and give their customers the option to prohibit the banks from sharing their customer information with non-affiliated third parties. GLBA also requires financial institutions to install risk controls for "foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alternation or destruction of customer information or customer information systems." Controls include

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

authentication, access control and encryption systems. The law isn't specific as to what protections should be implemented, thus leaving it up to individual organizations to determine how to best mitigate their risk. Organizations are also encouraged to implement systems for detecting and recording attempted intrusions and attacks. It also requires financial institutions to have a comprehensive written information security program in place.

Not only should you be concerned about healthcare and financial information, certain other kinds of information is protected from disclosure by law whether the information has been released on purpose or through negligence. During the Robert Bork Supreme Court confirmation hearings in the mid-'80s, Bork's opponents dug up his video rental records in the hopes of finding something subversive? So why didn't Clarence Thomas's video rental records find their way into the Thomas confirmation hearings a few years later? Anita Hill claimed that Thomas had made repeated references to specific pornographic movies, those records might have been pretty revealing. The reason is that, in the meantime between Bork's and Thomas's hearings, Congress passed the Video Privacy Protection Act of 1988, which makes it a crime to release individualized data about the videos any individual may rent or buy. Why so? The reason was that the Bork hearings called attention to the necessity for such a law.

This year Congress has introduced no less than 36 privacy bills to protect consumers from online fraud, theft, impersonation and junk e-mail. Lawmakers want better protection of personal information exchanged over the Internet. Some of the other laws you should be aware of are:

- The Fair Credit Reporting Act of 1970
- The Privacy Act of 1974
- The Cable Communications Policy Act of 1984
- The Electronic Communications Privacy Act of 1986
- The Telephone Consumer Protection Act of 1991
- The Drivers Privacy Protection Act of 1994
- The Children's Online Privacy Protection Act of 1998

Make sure you know what laws apply to the information you (or your client) are handling, so you know if you need to take special actions about protecting that information. And try to keep up to date, while it may seem like we're being inundated with new rules for digital content, it's nothing compared to what's to come. For instance, the European Union has already approved a directive that protects a wide range of personal information and, while it doesn't yet apply in the United States, any companies that wish to do business in Europe will have to act in accordance with it. Companies not in compliance will face severe restrictions on their business operations and stiff penalties for violations.

Civil Liability

Beside specific laws, companies and individuals can seek damages for any losses that they may incur. This falls under US laws regarding tort. A "tort" is some damage, injury or wrongful act done willfully or negligently for which a civil suit can be brought. In order for a plaintiff to successfully win a tort case, four basic elements must be established.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

1. Duty – the defendant must have a legal duty of care toward the plaintiff.
2. Breach of Duty – the defendant must have violated a legal duty of care toward the plaintiff. Usually this violation us the result of "negligence" on the part of the defendant.
3. Damage – the plaintiff must have suffered harm.
4. "Proximate cause" – the defendant's breach of a legal duty must be related to the plaintiff's injury closely enough to be considered the cause or at least one of the primary causes of the harm.

Merriam-Webster's Dictionary of Law defines Duty as "an obligation assumed (as by contract) or imposed by law to conduct oneself in conformance with a certain standard or to act in a particular way." If a customer provides information as part of doing normal business with your company this information is covered by your company's privacy policy. Your company's privacy policy can create a duty and can require that you act in ways more stringent than the law requires. Even though there is no direct contract or agreement between the customer and the company, your company has an implied duty to the customer to take reasonable steps to protect his information from disclosure to unauthorized parties.

Negligence

If a hacker breaks in to your system, you may ask yourself, "Wasn't it the hacker that did something wrong?" The answer to that question is yes but… You may have been negligent. Negligence is defined as "failure to exercise the degree of care expected of a person of ordinary prudence in like circumstances in protecting others from a foreseeable and unreasonable risk of harm in a particular situation." Under tort law, even though the hacker would be liable in a trespass against the company, the company would be liable, under negligence, for any injuries the hacker caused a third party. For example, if the hacker was able to delete a customer's order from a supplier's computer file, the customer could hold the supplier liable for any damages it sustained by not receiving its order. The negligence theory is based on the fact that the supplier should have installed the necessary equipment (hardware and software) and took reasonable actions to prevent the hackers from invading its computer system. Also, because the supplier did not have the necessary protection on its computer system, it should have known that such an act was likely to occur, and, therefore, guarded against it. The same goes for information that was disclosed in violation of a company's privacy policy. A court would determine whether or not that company complied with it's own policy and whether the company took the necessary actions to protect the information.

For example, lets assume a hacker gains access to your systems using a well-known exploit. He then obtains the names, addresses, birth dates and social security numbers of your top 1000 clients. He then uses their social security numbers and other personal information to obtain credit cards. He publishes these credit card numbers on the Internet. Suppose one of these clients decides to sue your company for negligence. Even though the hacker committed the theft of your client's identity, the plaintiff could claim that you failed to properly protect his personal information and that this was the proximate cause of his financial and emotional harm. A judge or jury would then decide whether, given the information store on your systems, your company

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

took reasonable actions to protect your client's data on your systems. In their decision they would probably ask the following questions:

1. Did your company have a duty to protect this client's information?

2. Did your company fail to uphold that duty?
   - What steps did your company take to protect the information stored on your system? Would a "reasonable person" have done things differently?
   - Was the vulnerability publicly known? Would any "reasonable person" have known about the vulnerability?
   - Was the vulnerability fixable and if so how long had a fix existed? Would a "reasonable person" have installed the fix prior to the time the hack had occurred?
   - Was that type information stored in a location that any "reasonable person" would have thought to be acceptable?

3. Was there any damage to your client? Does the client have proof of actual damages financial or emotional?

4. Was the failure to uphold your duty to your client the proximate cause for the damages incurred?

Obviously this situation would not look good for your company but the idea behind this area of the law is to make people behave in a way that protects all parties involved.

Limiting Your Liability

So now that you are sufficiently scared what should you do to minimize your liability? You need to go about securing you systems in a way that any court would say that you took reasonable steps to protect yourself by locking down your systems and networks and maintaining that security.

1. Establish a budget and staff with time that is dedicated to system security.

2. If don't already have one in place create a written security policy. Review RFC 2196 to get you started. http://www.cis.ohio-state.edu/Services/rfc/rfc-text/rfc2196.txt

3. As part of your security policy, develop and implement a procedure that tracks security risks and as they are identified, evaluates their potential risk to your business, identifies the appropriate fix, and schedules a date for implementation of that fix. Include follow-ups to ensure that the fix has been completed.

4. Check with your systems/OS vendor and find and implement all suggested lock down procedures for your OS and Hardware.

5. Install a good firewall. Roughly eighty percent of all attacks happen from within the firewall but you still need to protect against the other twenty percent.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

6. Employ some form of Intrusion Detection and monitor it regularly.

7. Keep yourself and your staff educated on the latest in security and vulnerabilities. Review security resources such as Bugtraq, SANS, Securityfocus, virus reports and other security publications, books and web sites as well as vendors websites on a regular basis.

8. Perform regular security audits on your systems and networks. These can be done internally but should also be done on a regular basis by an independent auditing firm that specializes in security auditing. Read the results of your audits carefully and act on any holes found in your security, procedures and policy.

9. Make sure your company has a security awareness program for all employees. Whether through social engineering or leaving sensitive information displayed on an unattended computer screen, a good security policy does no good if your employees are unwittingly releasing information to a hacker.

10. Properly destroy all unusable media and printouts. Use a professional information destruction company or at a minimum run all unusable tape and printouts through a shredder. When a hard disk drive is upgraded or replaced, the old drive must be sanitized and or destroyed.

11. If you are a health organization educate your self on HIPAA and make sure you lock down your systems and networks according to HIPAA regulations.

12. If you are a financial organization educate your self on GLBA and make sure you lock down your systems and networks according to GLBA Guidelines.

13. Even if you do not fall under the rules of HIPAA and GLBA. Review them. They may help in setting up your own security guidelines and policy.

14. Make sure you understand and abide by any other laws that may cover the types of information and data being handled on your systems and networks.

15. Use Data Encryption in the transmission and storage of sensitive data.

16. Do everything you can to maximize security but get insurance. Review your insurance policies and if your insurance does not cover your business for situations regarding hacking losses and/or online liabilities, get covered.

17. After you feel you have all your bases covered review your strategy and situation with an attorney who specializes technology law. Make sure that he feels comfortable that all your bases have been covered.

Conclusion

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

With security incidents increasing almost exponentially every year, we need to protect our customer's information and ourselves more diligently. The increase in incidents will bring a rise to an increase of lawsuits claiming that we did not do our part to protect and secure the data we need to do business. Will a good security policy and sound security procedures stop a hacker from trying to gain access to your systems and networks? No, but it will greatly reduce his chances of success. Will a secure system and network stop someone from filing a lawsuit against your company? No, but it will increase the likelihood of you winning a case against you. If you understand and comply with the law and follow the suggestions mentioned you will considerably limit your liability.

DISCLAIMER

I am not a lawyer and I don't even play one on TV. This article is for informational purposes and does not constitute legal advice. It should not be used or taken as legal advice relating to any specific situation. Before making any kind of decision that might affect your liability, make sure you consult an attorney.

Branco, Marcia "Overview of HIPAA's Security Concepts" 13 April 2000
URL:http://www.sans.org/infosecFAQ/legal/HIPAA.htm (7 Aug 2001)

Forcier Anderson, Michelle "The Buck Stops Here" Information Security
June 2001. 18-19
URL:http://www.infosecuritymag.com/articles/june01/departments_news.shtml

Saul, Joseph M "E-COMMERCE LAW Balancing Acts" Information Security
October 1999
URL:http://www.infosecuritymag.com/articles/1999/octcover.shtml

Nicholson, John "You've Been Cracked…And Now Your Sued" :Login;
Vol 26. No 2. April 2001

Merriam-Webster's Dictionary of Law. Merriam-Webster, Incorporated 1996
URL:http://dictionary.lp.findlaw.com (7 Aug 2001)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**