;login:

THE MAGAZINE OF USENIX & SAGE
April 2001 • volume 26 • number 2

inside:

THE WORKPLACE
You've Been Cracked . . .
and Now You're Sued!

USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

you've been cracked . . . and now you're sued

by John Nicholson

John Nicholson is an attorney in the Technology Group of the firm of Shaw Pittman in Washington, D.C. He focuses on technology outsourcing, application development and system implementation, and other technology issues.

<John.Nicholson@ShawPittman.com>

The scene opens on a very serious man in a dark suit sitting on the edge of a desk in front of a wall of identical books. He says, "Has your privacy been invaded because a company exposed your personal information to unnecessary risk? Has a hacker stolen your identity or has your credit rating been damaged because a company should have done more to protect your credit card number? Did you lose your job or have you suffered embarrassment and humiliation because your private medical information was disclosed? You may have a claim. Call the lawyers of Able, Baker and Charlie. Your first consultation is free and, remember, there's no fee unless we recover for you. Able, Baker and Charlie – we're fighting for your privacy."

So far, that commercial hasn't been made. But given the increasing public interest (and paranoia) about information and data privacy, how long will it be before someone sues a company for damages because the company "allowed" that person's credit card number or other personal information to be stolen? It may not be long before ads like that are just as common as the other ads for lawyers that you see on late night TV. The purpose of this article is to help you understand the basics of this area of the law, with particular emphasis on the concept of negligence, so that you can work with your company's lawyers to develop a policy that minimizes the risk to your company of a lawsuit.[1]

Despite the apparent surge in seemingly silly lawsuits in the US, under US law every "tort"[2] claim must satisfy a four-part test in order for a plaintiff to succeed. Every tort claim must prove four basic elements:

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 is 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.

Unless all of these are found to be true, the plaintiff in a lawsuit will not succeed.

When a Duty Can Exist

A duty can exist when there is a relationship between two or more parties. For example, a homeowner has a duty to protect guests from risks known to the homeowner but not to the guest. If a homeowner knew that a particular step on a staircase could not support weight, the homeowner would be liable if a guest were not aware of the risk and were injured by stepping on the broken step. According to the four-part test above, (1) the homeowner had a duty to the guest, (2) the homeowner failed to warn the guest about the step and breached the duty, (3) the guest was injured, and (4) the broken step was the "proximate cause" of the injury.

In a more technology-oriented situation, if a customer is providing information to your company as part of a transaction, usually such information is covered by your company's privacy policy. That privacy policy can create a duty and can bind your company

Even if there is no specific contract between your company and a person whose information gets disclosed because of something your company did or did not do, a court may still find that your company had a duty to take reasonable steps to protect that person's information.

to a level of behavior more stringent than that required by law. Even if there is no specific contract between your company and a person whose information gets disclosed because of something your company did or did not do, a court may still find that your company had a duty to take reasonable steps to protect that person's information.

What Exactly Is "Negligence"?

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."[3] In the homeowner example, above, the homeowner may have been negligent in not warning the guest about the broken step. In the case of a person who claims that a company disclosed information in violation of that company's privacy policy, a court would determine whether or not that company complied with its own policy. In the case of breach of data security, a court would determine whether a company had been negligent by evaluating whether the company protected its information in a reasonable way given the cost of the protection, the sensitivity of the data, and what the company knew about the vulnerability that resulted in the information being disclosed.

Example Scenario

In the summer of 2000, a cracker used a password sniffer to compromise over 5,000 detailed medical records in an internal network at the University of Washington Medical Center (UWMC). The compromised information included the names, addresses, birth dates, social security numbers, and medical histories of over 4,000 cardiology patients, and additional information related to every discharged or transferred patient during a five-month period.[4]

Suppose, hypothetically, the cracker used that compromised information to steal the identity of one of those cardiology patients, and that patient decided to sue the UWMC for the damages, both financial and emotional, involved in repairing the patient's credit record. Despite the fact that someone else committed the identity theft, the plaintiff would be arguing that UWMC's failure to properly protect his medical records was the proximate cause of the financial and emotional harm suffered. In that situation, a judge or jury would look at whether, given the type of information being stored by UWMC, the UWMC was reasonable in the way it protected such information.

Going through the four-part analysis from above:

1. Did UWMC have a duty of care toward the plaintiff to protect the information provided by the plaintiff? Probably.
2. Did UWMC breach that duty?

In its analysis of breach of duty, a court would probably ask the following questions:

- What steps had UWMC taken to protect its information, and would a "reasonable person" have done things differently? According to *Information Security*, all information was taken over the Net and there were no firewalls in place.[5]
- What vulnerability was exploited to get privileges on the system?
- Had the vulnerability been made public and, if so, would a "reasonable person" have known about the vulnerability?
- Did a fix to the vulnerability exist and, if so, for how long prior to the breach was the fix available? Would a "reasonable person" have implemented the fix prior to the breach? For example, "More than 80 percent of successful attacks against NT-based Web servers exploited a vulnerability in RDS . . . [which] is installed by default on

NT-based IIS Web servers and is not commonly used by most Web sites. The RDS vulnerability is more than two years old and has had good patches available since July 1999."[6] If the UWMC vulnerability was something like this, that might weigh heavily against UWMC.

- Given the sensitivity of medical data and that the cracker used a password sniffer, would a "reasonable person" require users to use some kind of token in combination with a password? What were UWMC's requirements for password length and composition? How frequently were passwords required to be changed?
- Would a "reasonable person" have kept that type of data in that location? Was the database sitting on a Web server or was it somewhere else in the network? Given the power of a social security number for committing identity theft, was it reasonable for UWMC to track patients by social security number?

3. Was there damage? The plaintiff would have to show actual damages (which could include emotional damage).
4. If UWMC had a duty to the plaintiff and that duty was breached, and if the plaintiff suffered damage, was the breach by UWMC the proximate cause of the damage?

You might feel that the cracker in this hypothetical situation was the one who actually committed both crimes – first, cracking UWMC's network and stealing the information and, second, stealing the patient's identity, and that the only reason someone would sue UWMC would be to get money. However, the goal of this area of the law is to make people behave in a way that increases the relative safety of everyone. For example, if a store owner fails to properly lock his gun store, and a thief manages to break in and steal bullets which the thief then uses to shoot someone, then the store owner could be held liable. The reason for this is to encourage the store owner to recognize that his bullets create a hazard, and he should take appropriate care to prevent others from being harmed by that hazard. Tort litigation exists so that there is a cost-benefit analysis for people and companies to perform: the cost of preventive measures vs. the cost of the lawsuit.

Tort litigation exists so that there is a cost-benefit analysis for people and companies to perform: the cost of preventive measures vs. the cost of the lawsuit.

So What Do I Do?

Your first step should be to develop and implement, as part of your overall security policy, a procedure that tracks security risks (both external and internal) as they are identified, evaluates their potential risk to your business, identifies the appropriate fix, schedules a date for the implementation of the fix, and includes a follow-up procedure to ensure that the fix was properly implemented. For example, your policy should include:

1. Regular reviews of the relevant security vulnerability sources (i.e., Bugtraq, NTBugtraq, security reports published by software vendors, virus reports, security researchers, the various cracker Web sites, etc.) and, if appropriate, a procedure to ensure that such reviews are performed

In a diverse environment, your company may have multiple people responsible for various platforms and/or software packages, or your company may have various administrators with responsibility divided by geography. It's important to make it clear who will have the ultimate responsibility for monitoring security issues related to each platform or software package.

2. A determination of how the identified vulnerability applies to some aspect of your business

NOTES

1. This article provides general information and represents the author's views. It does not constitute legal advice and should not be used or taken as legal advice relating to any specific situation.

2. A "tort" is some damage, injury, or wrongful act done willfully or negligently for which a civil suit can be brought.

3. Merriam-Webster's *Dictionary of Law*, 1996, as published on <*http://www.findlaw.com*> as of Feb. 6, 2001.

4. *Information Security*, vol. 4, no. 1, January 2001, p. 24.

5. Ibid.

6. Peter Tippett, "Sweat the Easy Stuff," *Information Security*, vol. 4, no. 1, January 2001, pp. 30–31.

For example, a security hole that lets a script kiddie put graffiti all over your Web page can be embarrassing to your company or might result in your taking down your page until you can plug the hole. If your Web page is just information about your company, this might not be a big problem. If your Web page is the means by which your customers order, that's a different matter. It's important to understand how the vulnerability could impact your business if it were exploited.

3. A rating of the risk represented by the security issue (i.e., critical, high, medium, or low) based on the potential impact of the security issue to the business (in terms of lost business, public perception, potential cost, etc.)

4. A schedule for the implementation of the relevant fix for the risk (i.e., all critical fixes will be implemented within one day, all highs within one week, etc.)

5. A follow-up procedure that checks whether fixes were actually installed and, depending on the importance of the security issue, verifies whether the fix actually solves the problem.

A follow-up procedure could vary depending on the rating of the issue. For example, you might want to ensure that all fixes for critical issues are implemented, and use statistical sampling for the rest. Alternatively, you might want to ensure that all fixes for a mission critical system are performed, regardless of rating.

Once you've completed your procedures and made them part of your routine, do an audit of how your system stacks up against the known threats. This might involve having a "white hat" security attempt to penetrate your network. Use this as an opportunity to test your priority ratings as well. If a problem someone rated as "low" allows the penetration team to take control of your system, then you might need to reevaluate that rating.

Conclusion

It may not be long before people begin suing companies for information disclosures that result from a company's network being cracked. Companies need to develop the policies and procedures that will protect both the information (which is the primary goal) and the company in case the company is ever sued in relation to such a disclosure. Will having a security policy like this in place keep you from getting sued? No, although it might make it less likely. A security policy that includes the procedures described above won't prevent you from being attacked, and it won't prevent you from being sued because of an information disclosure. It will enable you to prioritize and understand the known risks to your system, and it will put your company in a better position if you ever are sued, including potentially protecting your company from punitive damages.