;login:

THE MAGAZINE OF USENIX & SAGE

August 2001 • Volume 26 • Number 5

Special Focus Issue:Clustering

Guest Editor: Joseph L. Kaiser

inside:

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

letters to the editor

Question on Liability

From Fernando Montenegro
fsmontenegro@hotmail.com

To John Nicholson

I was recently going through your article about liability in the April issue of *;login:* and I have a question:

If I understood correctly (I am not a lawyer), every tort claim in the US has to have four elements:

- Duty – the defendant has to have a relationship where he had to "care" for the plaintiff.
- Breach of duty – there has been "negligence" by the defendant on providing that care.
- Damage – there must have been some harm to the plaintiff.
- "Proximity cause" – I understand this to be the assertion that the breach of duty above had to be "close enough" to whatever caused the damages.

I understand how the first three elements can be quickly established in an information security setting. However, I am having trouble with the fourth ("proximity").

The example you listed in the article, with the store owner, deals with a physical entity (bullets). However, using the identity theft example, how does one establish the "proximity" when the goods are just information? Worse, information that could *potentially* come from all sorts of different places (magazine subscriptions, banks, credit reports, club memberships, etc.). Do the same rigorous standards for burden of proof that we see in criminal cases apply to civil suits? Would it be reasonable to expect an individual to prove the "proximity" of the negligent act in a Web site attack?

Thanks for a great article! I thoroughly enjoy reading about "real-life" issues relating to information security.

From: John Nicholson
John.Nicholson@shawpittman.com

Your understanding of the four elements of a tort claim is correct. And you are also correct in thinking that proximate cause is frequently the most difficult part of any tort claim. Ultimately, it is the finder of fact (the judge or jury) who decides whether a specific action satisfies each of the four elements. In the US, the standard of proof for civil claims is what's called a "preponderance of the evidence" standard, and it is basically a "more likely than not" standard (i.e., more than 50% likely). Therefore, what a plaintiff must do is convince a judge or jury that information released from a poorly secured server was the "proximate cause" of some harm, and the defense must convince the judge or jury that, among other things, (1) the information was not the cause, or (2) even if the information was the cause, the server was reasonably secured.

Identity theft may not be as easy an example as release of medical data. If you had some medical condition that you did not wish to be disclosed, and, as a result of unreasonably poor security, that information became public knowledge, you could have grounds for a tort claim if you suffer some damage – whether actual, direct damage or what is called "emotional distress."

There could also be significant direct impacts from an identity theft. The thief could incur debts for which you end up being held responsible. Also, since your credit rating may be damaged, it might be difficult for you to get loans, and you might have to spend lots of time and effort trying to correct the situation, which could also be quite stressful. So, there could be actual, direct damages, and there could be "emotional distress" related to an identity theft case.

In addition to damages suffered by the victim, the US system allows for what are called "punitive damages," which are intended to penalize the party at fault so that the party takes steps to prevent the problem from happening in the future.

The point of my article was to raise awareness of the potential impact that the absence of a clear security policy could have. From a corporate point of view, the reasonable potential for a lawsuit should be enough to at least cause people to think about establishing a reasonable security policy. In addition to the prospect of being taken to court, there is the potential for a very bad public relations situation (the public knowing not only that you had been hacked but that people were filing lawsuits claiming your security procedures were insufficient), which might be very bad for business.

Charity

From Greg Black
gjb@gbch.net

To Andrew Hume

I am one of the small number of non-American members of USENIX. I believe very strongly that USENIX should continue to provide a (small) proportion of its funds to charitable ends such as those discussed in your article in the June 2001 *;login:*.

I'd also like to see more reporting on the destinations of these charitable contributions; and on the outcomes from them.

We do try to publish news about recipients of USENIX grants, and also publish some of the results: see page 92 about USACO.
The Editors