MICHAEL B. SCHER

on doing "being reasonable"

Michael Scher is general counsel and compliance architect for the Chicago-based IT security firm Nexum. An attorney, anthropologist, and security technologist, he's been working where the policy tires meet the implementation pavement since 1993.

mscher@nexuminc.com

IT'S AN ADMIN'S WORST NIGHTMARE: Mission-critical servers are compromised, and you didn't know about it. Systems you can't patch except in tightly controlled downtime windows have nefarious changes being made to them by persons unknown; systems where uptime equals money and downtime equals loss; systems you probably could have patched sooner, but the politics were just too treacherous. Worst of all, you didn't even discover the intrusion—you found out from the legal department: Your company is being sued because those mission-critical, fiscally sensitive hosts are being used to attack a third party. That third party cried havoc and let slip the lawyers of tort.

Well, that's not the way it went down at IBM this summer [1], but a glimmer of that kind of scenario briefly made the news with IBM in the headlines. In short, a D.C.-area law firm sued Big Blue because, allegedly, a number of servers at IBM's Durham, N.C., facility were being used to attack the law firm, which had, allegedly, suffered harm as a result. IBM says the firm hasn't even demonstrated that either organization's systems had been compromised, let alone suffered harm, and has asked the court to throw the case out. We'll have to wait to see where this one goes, but even if it's a tempest in a teapot, it illustrates an emerging consciousness among the legal community that harm caused by way of an ill-protected computer can be worthy of a lawsuit.

Are you responsible for critical or Internet-facing systems at a large organization? Have you talked lately with corporate legal about the company's policies for systems security? Oh, sure, your group has probably discussed SarbOx, HIPAA, GLBA, the various state consumer information privacy acts (starting with California's SB1386), and maybe even 21 CFR 11 with them, inspired by auditors and under the shadow of possible penalties. Maybe your organization has a policy to cover and look for contributory copyright infringement, for uses that constitute harassment, or for communications that create a hostile workplace. But how about good old negligence? Now's a good time to have that talk.

Some of this paper will strike systems personnel as heavy on the legal material; it will strike attor-

neys as light on the legal side and full of too many technical details. My goal is to raise awareness about negligence law in systems groups and to help them start a dialog with their own legal departments or outside counsel. The content and positions contained in this article should not be taken as legal advice—the discussion is simply far too general to safely use that way. The purpose is to make you more conversant in the issues and able to discuss them with personnel responsible for corporate, fiscal, and legal risk.

The Hypothetical: Arnold's Widgets v. Burt's Technical Company

Let's take a look at the kind of lawsuit in question. We'll walk through a hypothetical set of facts, and see where and how a negligence suit could fly. Since the facts are ambiguous from the recent story in the news, we'll start fresh. Let's say a company, Arnold's Widgets, has had some of its Internet-facing hosts compromised and others hit with traffic-flood denial of service (DoS) attacks by persons unknown, who apparently used compromised servers at Burt's Technical Company (BTC) to do their dirty work.

Arnold's has suffered several days of DoS attacks that rendered its widget-ordering site unavailable. The company estimates a nonrecoupable loss of business (which went to the competition) amounting to $300,000. Arnold's has also spent some $50,000 on forensics and consultants to locate and clear compromised hosts in its DMZ. The forensics folks identified several IPs in the BTC netblock as the source of both the DoS traffic and the direct system compromises. Arnold's sues BTC for damages of $350,000, which Arnold's claims are the result of BTC's negligence.

Negligence

Negligence is at once a simple concept and a complex morass of subtle rules brought about through case law and statutes. Actions for negligence are part of "tort law"—non-criminal law handling harms caused by breaches of duty between two parties. At its core is the following principle: If you fail to live up to a duty, you're negligent. It gets a little complicated from there. There are a number of ways a person can be under a duty, but we'll just look at two:

- Duty to conform to regulatory or statutory requirements
- Duty to act reasonably

DUTY TO CONFORM TO REGULATORY OR STATUTORY REQUIREMENTS

This principle seems self-explanatory. If there's a law or a regulation, and you don't live up to it, you could be seen as negligent. Indeed, in some states, it's a special kind of negligence called *per se* negligence. In essence, that means that it's presumed to be negligent to fail to live up to it—the defendant has to show that *not* doing the duty was reasonable. Normally, the plaintiff (the person suing) would have to show it was an unreasonable act, but *per se* negligence turns that on its head. Sometimes, the regulation or statute specifies what the injured party can collect ("a remedy"); in some circumstances, that means the statutory or regulatory remedy is exclusive, and one cannot sue otherwise over the harm caused by negligence; one can just request whatever remedy is specified. Sometimes, the remedy is not meant to be exclusive—some provisions don't have a specified remedy at all, leaving "enforcement" mostly up to the public, who may sue for harms resulting from failures to obey the law. Politicos don't have to show much of a budget to enforce laws or regulations that will be

enforced by the public through lawsuits (though certainly it does cost the system money).

DUTY TO ACT REASONABLY

This duty can be more complicated and lies at the core of the more "interesting" lawsuits alleging negligence. As a member of society, or of some specific profession or subgroup, you have a duty to act like a reasonable person, taking reasonable care in your behavior to avoid reasonably foreseeable harm to a reasonably foreseeable swath of people. Doctors have to act like reasonable doctors when doing doctor stuff; systems administrators have to act like reasonable systems administrators when doing sysadmin stuff; and the person driving a car has to act like a reasonable car driver while driving. Sounds reasonable, right [2]?

DETERMINING WHAT'S REASONABLE

We already discussed how, usually, it's considered reasonable to follow the directives of law or government regulation, and how in some jurisdictions there's a presumption that failing to do so is presumed to be negligent. So where, for example, HIPAA lays down some rules, it would be wise to follow them, not just for HIPAA reasons but because not doing so may be construed as unreasonable behavior. But what about when there's no specific law or regulation? I mean, most of us think about lawsuits as the result of mistakes of some kind or clumsy error, so there's got to be some kind of reasonable standard, right? Right. Kind of.

Reasonableness is determined by the finder of fact—a jury quite often, and sometimes the judge—based on community standards of behavior. Usually, that means, in the absence of a law or regulation, you can look to common practice for a decent idea of reasonable behavior. But not always. "This is the way we've always done it" is usually disingenuous, and in any event, the excuse doesn't always hold water.

In a famous case from 1932, two barges sank in a storm while being guided by tugboats, and the tugboat operators were sued for losing the barges. Neither tug had a radio, so they failed to receive warning of the oncoming storm and taken shelter, as many other tugboats did that day. The industry was just starting to adopt radio receivers in boats and it could hardly be called the norm to have them at the time. The tug owners were found to be negligent for not having radios, and they had to pay for the barges, despite doing what many if not most tug companies were doing. In his decision affirming the judgment, Judge Learned Hand set down an important principle [3]:

> Indeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; *a whole calling may have unduly lagged in the adoption of new and available devices . . . there are precautions so imperative that even their universal disregard will not excuse their omission.* [emphasis added]

In IT, and all other fast-changing industries, that means in essence that one may want to look a little bit ahead—in short, at *best practice*—to help determine what's reasonable. If achieving best practice levels is *reasonably* cost-effective, it might not be reasonable to slouch along with the competition. Those lagging behind may be deemed negligent.

Another famous Learned Hand decision, again involving barges, came in 1947. Tugs and barges seem to have been on the technology and risk fron-

tier of the day, an industry trying to compete and cut costs by saying "this is the way we've always done it!" His decision will sound familiar to anyone familiar with risk analysis, in IT or in tugboatdom. This time, a barge broke loose in a storm, smacking into other vessels at dock, causing a lot of damage. No attendant was kept stationed at the barge because it would have been too expensive. Judge Hand wrote [4] that the level of reasonable care can be estimated from:

> (1) the probability that [the risky event will occur]; (2) the gravity of the resulting injury, if [it] does; (3) the burden of adequate precautions. Possibly it serves to bring this notion into relief to state it in algebraic terms: If the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P; i.e., whether B < PL.

Sounds reasonable, right? If the risk is caused by your operations, and the burden of protection is not so bad, and the potential harm is significant and not unlikely, then there's a duty as a reasonable person to avoid subjecting others to that risk.

Most states also have an inverse rule: The victim can be penalized if his or her *own* negligence added to or helped cause the harm. In many states, the ability to collect is completely cut off if the harmed party was more than 51% responsible, as determined by the fact finder. In a handful of states, the harmed party can't collect if they were even a little responsible, and in all the rest, some balancing act takes place to allocate the costs of fixing the damage among the parties based on comparative fault.

DO WHAT YOU SAY AND SAY WHAT YOU DO

Does your organization have any systems policies, designed to protect some group of people from some group of harms, which your organization isn't quite meeting? While probably not *per se* negligence, it's definitely good evidence that your organization knew what the right thing was, wrote it down, and then failed to do it. That is, it's evidence that your organization was negligent. That's a deep hole to explain your way out of when the harm the policy is supposed to have prevented comes to fruition.

Corporate legal should help the technical organizations craft policies that can actually be implemented on the ground in a realistic time frame. Don't set or accept pie-in-the-sky policies that can't be done. It's your job to talk with legal, and with corporate finance, to find that magic balance point of risk and the cost to avoid. If there's a need to reach some policy directive, but it will take time, make your policy actually set a time frame. If it looks as though you will miss the due date, ensure policy is changed to a later due date long before it's reached. It's better to try again honestly than to live with a policy level you're simply not meeting.

COLD HEARTS AND RISK ANALYSIS

There are of course circumstances where the harm is so significant that calculating it away as too costly to avoid will be frowned upon in the courts. Matters of life and death, or broad health disaster, or the performance of generally life-threatening acts, or allowance of obviously life-threatening problems under your control will probably not be considered reasonable and may be the subject of punitive damages [5]. Probably you won't see much of that in systems administration, but it would certainly be wise to ensure the controls to your medical therapeutic systems aren't available

from the Internet. In general, one should consider any precaution priced a lot lower than the potential harm.

At some level of inherent risk, the courts are likely to say that, if it's so expensive to fix, and so risky to do, it probably should not be done, unless one is willing up-front to take on the costs of harm. For example, there are practices that are so inherently dangerous that a standard called "strict liability" applies. That is, the practice is so dangerous that the risk of harm cannot be eliminated by any expense; therefore the organization so doing is simply liable for the consequences—costs to avoid and standards of care are irrelevant. Blasting and some aspects of defective product liability are, for example, held to strict liability standards [6].

HARM AND "ACTIONABILITY"

Here's a funny thing: if someone is completely negligent, but no one is harmed, then no one gets to sue for negligence. There has to be a harm. Tort law is there to make the harmed party whole—no harm, no tort. The harm also needs to be one that is reasonably foreseeable, the result of the failure to meet the duty, and of the general kind that the duty was there to prevent. It can be a surprising harm in its scale, so long as it's a direct result of the failure to meet the duty and a foreseeable kind of harm. That set of relations from an act makes that act the "actual and proximate cause"—that's a key (and sometimes quite complicated) concept in practice.

Another principle is that sometimes an intervening action by a third party can cut off your liability for failing to meet a duty. Their action must constitute a "superseding" cause: it has to occur after your negligence, and become one of the proximate causes of the harm. This principle holds mostly when the intervening act was itself not
a reasonably foreseeable circumstance, so that you could not reasonably be expected to take it into account in forming your behavior. So if you're a landlord in a bad neighborhood and the tenants complain that there is a dark spot at the entry that muggers can use to attack them, and you do nothing about it, the mugging is probably not going to be seen as an intervening act: It's the very act you were warned about and part of your duty as a landlord to mitigate. Mind, if you took every reasonable step and someone still committed such a criminal act, you would probably not be viewed as negligent and the act would be seen as intervening.

Whew!

Summing It Up for Our Theoretical Arnold's v. BTC Case

Arnold's has alleged the following:

- BTC has a duty to keep its servers reasonably secure against unauthorized access; alternatively, if an employee failed to perform his or her duty securing the hosts, BTC nevertheless has a duty to supervise its employees.
- BTC failed to act reasonably as is evidenced by someone using its servers to attack the Arnold's network.
- BTC is responsible even if the attacker was an unauthorized attacker who illegally gained access to the BTC servers.
- Arnold's has suffered actual fiscal damage as a proximate result of these attacks.

BTC replies:

- BTC takes reasonable steps to secure its hosts, based on industry-normal practices and recommendations from its auditors. It looks to its industry for guidance.
- The break-in occurred despite reasonable practices.
- The intervention of a criminal act cuts off the proximate causation of BTC's alleged failure to meet a duty and places the fault strictly on the criminal.
- The compromised servers at Arnold's were compromised only because they themselves were not well secured, unreasonably so, to no less a level than BTC's alleged negligence, and so Arnold's is contributorally negligent.

Let's go through it by the numbers.

1. Did BTC have a duty to keep its hosts secured to some level? Does such a duty exist? Well, we all know a compromised host can be used to attack others and cause harm. Compromised hosts also help shield the identity of an attacker using them to go after third parties. That in turn hurts the third party's ability to sue the real attacker. Is it reasonable, knowing all that, to set up a situation where attackers are *likely* to be able to use your servers to attack others? Probably not. It seems likely that such a duty could be found to exist, a duty to keep the hosts secured to a reasonable level. If BTC had a policy saying it had to keep its hosts patched up to snuff, and failed to meet its own policy, that's some more evidence that BTC didn't live up to a reasonable standard of behavior—one it had set for itself, no less. BTC could claim its own policy was unreasonable, but let's face it—that isn't going to sound good in court.
2. Were BTC's practices reasonable? Did BTC fulfill its duty to act reasonably? Most companies do make the effort to firewall, watch, and patch their hosts, especially the Internet-facing ones. If nevertheless many get broken into on a recurring basis, common practice may not be enough to be reasonable. "Reasonable" behavior may be to move toward protection levels that more or less cut off what we all understand to be *one of the most likely* (and therefore foreseeable) outcomes of a host compromise. So if BTC's actual practices were below what (many expensive) experts say is "common practice" for the industry, it could well be found negligent. If it acted at "common practice" levels but below "best practice" levels, it could still be found negligent, a rather damning message to the industry in question. The question would be in essence: What does the company need to have done to constitute "reasonable" steps to cut off such a likely harm?
3. Did the criminal actions of the attacker cut off BTC's responsibility? Consider that, but for the actual criminal actions of the attacker, there would have been no harm to anyone, let alone to Arnold's. Yet, an exposed system, we are all aware, would probably be probed by automated attack processes several times a week, if not more frequently. Studies show that they are subsequently compromised on an ever-more-frequent basis [7]. Was it inevitable or at least reasonably foreseeable that a host with a vulnerability would be compromised (criminal act) and used for nefarious purposes (another criminal act)? I think we can all agree that, yes, it is likely. Is the action, therefore, more like a mugger in a dark spot that is plainly useful to muggers and about which the landlord has been warned than like a burglar using top-of-the-line tools to break into an ordinary apartment? I think we can agree that a key point of border security and patching is to prevent

exactly this kind of criminal act, so it would be likely that the act would not cut off liability. It's the very series of events the duty would be there to prevent.

4. Was the negligence the proximate cause of the harm? If (given all the above) the attacker's act is held to be just part of the stream of reasonably foreseeable events, then BTC's negligence is a proximate cause of the harm. Arnold's wins! Well, maybe not. BTC alleges that Arnold's was at least partly responsible for the harm by *not securing its own machines*—the very same duty BTC failed to perform. Here it looks like BTC finally has some traction: those servers that were compromised were certainly not up to snuff, and an expert could argue that they would have been broken into eventually. Depending on the state law, Arnold's could be in a position to collect nothing for its damages in finding and fixing the compromised hosts. Applying comparative negligence to a DoS attack, however, is harder. It's not currently even best practice to be truly DoS proof, lots of products claiming to help at low cost notwithstanding. It costs a lot to defend against a traffic flood on your own, and having the resources to do so is a business decision mostly brought about by frequently being in the sights of DoS-based attackers. Then again, good contracts with upstream providers, good upstream providers, and emerging services that significantly reduce the effects of a traffic flood DoS will shift reasonable DoS protection from the rare and extreme to the best practice realm probably within a few years. Only companies requiring instant defense (rather than within an hour from a service provider) might require a higher standard. Which way the jury might go on this last score will be the result of the expert testimony. Nowadays, not noticing that your servers are flooding someone else's network could tend to be seen as negligent. Conversely, I'd guess most businesses don't need extreme DoS defenses to be "reasonable" but someday, not too far away, they well might.

Hypothetical Case Summary

BTC is probably going to have to pay out something to Arnold's for the harm caused by the DoS flood. Yet, the entire experience was probably stunningly expensive for both companies. Obviously, they might well settle long before reaching the trial stage. Nevertheless, one doesn't want to be in BTC's position. And one never wants to be on the receiving end of a landmark case.

You're probably not negligent if you act with reasonable, due care, even if harm somehow happens. You're probably not liable (though you would be negligent) if your failure to act reasonably results in no harm, or harm of an utterly different kind than that which the duty to act reasonably is there to prevent. It's not an excuse much of the time that the harm depended on a criminal third party if the third-party action is reasonably foreseeable and the harm is the kind you'd expect.

Compliance Is a Two-Way Street

Systems and security/risk teams need to talk to corporate legal and business risk personnel. Instead of just implementing controls that react to compliance regimes, systems and network security needs to work hand in hand with legal in the crafting of security policies. The issues aren't just that the company will itself be directly harmed (risks that a good risk man-

agement group can estimate) but that the company's security posture decisions could result in harm to foreseeable third parties.

And hey—let's be reasonable out there.

REFERENCES

[1] "D.C. Law Firm Claims IBM Worker Hacked Its Computers": http://www.informationweek.com/security/showArticle.jhtml?articleID=190400233.

[2] We'll just pretend we didn't all just think "and what about the reasonable attorney," for now. OK? Good.

[3] The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932).

[4] U.S. v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

[5] Although the famous Ford Pinto cases from the 1970s are often discussed as exemplifying this principle, they are actually not very good examples. See "The Myth of the Ford Pinto Case," by Gary T. Schwartz, 43 Rutgers L. Rev. 1013 (1991), available at http://www.pointoflaw.com/articles/The_Myth_of_the_Ford_Pinto_Case.pdf.

[6] *Inc.* magazine had a 1999 article with a number of strict liability examples. It's online at http://www.inc.com/articles/1999/11/15396.html.

[7] See, for example, the SANS ISC study: http://isc.sans.org/survivalhistory.php.

OTHER RESOURCES

Carter Schoenberg of ISS has written an excellent primer on the relationship of regulatory processes and patching to negligence: http://www.infosecwriters.com/text_resources/pdf/InformationSecurityCClass.pdf.

A discussion of the differences among contributory, comparative, and modified negligence, and a listing of which states follow which principle, can be found at http://www.mwl-law.com/PracticeAreas/Contributory-Neglegence.asp.