;login:
THE MAGAZINE OF USENIX & SAGE
December 2001 • Volume 26 • Number 8

inside:

SYSADMIN

Stepping on the Digital Scale
By Erin Kenneally

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

stepping on the digital scale

by Erin Kenneally

Erin Kenneally is a Forensic Analyst with the Pacific Institute for Computer Security (PICS), San Diego Supercomputer Center. She is a licensed Attorney who holds Juris Doctorate and Master of Forensic Sciences degrees.

erin@sdsc.edu

Duty and Liability for Negligent Internet Security

The Fine Line: Are You a Victim-Symptom or Liable-Cause?

Reality dictates that networked computers are vulnerable to undesired actors and events owing to computer security vulnerabilities. The important question becomes: should these insecure computers be tolerated given the nature of modern computing infrastructure? If the answer is "no," we must be prepared to define standards of care in securing network computers against damage by third parties and recognize the recovery of damages from those parties whose insecure computers were used to exact harm.

Much of the popular media has focused attention on the ever-growing incidence of insider malfeasance and external intrusions into computer systems, resulting in violations of privacy, network failures and disruptions, spread of viruses, fraudulent transactions, and corporate espionage and data tampering, among others. A comparable amount of publicity has been paid to identifying the cybervandals, kiddie hackers, angry customers, disgruntled employees, foreign moles, or unethical competitors. Indeed, the panoply of crimes and damaging activity carried out over computer networks (Internet included) has both emulated and broadened the miscreant feats of property-based society.

Similarly, it is not surprising that a litigious society confronted with these expanded criminal capabilities and opportunities for mischief will spawn a wide array of legal redress seekers. To be sure, the cyber-equivalents of the McDonald's coffee-scalding lawsuits and Twinkie defenses have emerged and will likely persist. When the digital perpetrator cannot be tracked or is insolvent, the wronged party will seek alternate entities to hold responsible for losses incurred. To this date, no court has squarely addressed the issue of liability for failure to adequately secure a computer system. But, insofar as computer security technology represents the means to thwart these harmful activities, the logical targets from which to seek redress are those parties that have failed to implement appropriate computer security practices.

Our legal system exists to provide a mechanism of protecting individuals' interests and resolving disputes in an effort to maintain an orderly society. It is guided by notions of reasonableness and judged by objective standards representing society's values. In this sense, laws – both legislative and judicially created – are formal embodiments of society's willingness to assign responsibility and redress grievances between parties. However, the nature of our computer-networked environment forces society to redefine what is reasonable and fosters responsibility shifting. The critical question entails assessing responsibilities, defining duties, and assigning liabilities amidst this novel playing field that cultivates both traditional and neoteric relationships, conduct, and consequences. It is against this backdrop that this article discusses potential liability for "computer insecurity" between software vendors (SWVs), service providers (ISPs/ASPs), Web businesses (WebCos), and individual users within our computer-networked society.

This article highlights the parties and common scenarios likely to spawn claims of negligence for failure to secure computer systems. Is there a duty to secure computers?

Where does that duty arise from? To whom does the duty apply? What is the scope of the duty? Should "insecure parties" be assigned different levels of duty regarding computer security? What does it mean to take reasonable precautions to prevent computer intrusions?

What does it mean to take reasonable precautions to prevent computer intrusions?

The Legal Playing Field – Enter Negligence Claims

Negligence is primarily a concept within civil law, which is intended to address grievances between people and encourage socially responsible behavior. This is in contrast to criminal law's purpose of enforcing the government's interest in deterring future crime by punishing perpetrators. When a user or business suffers loss from an invasion into their computer system or network, criminal law offers no compensation to the victim if the intruder cannot be identified and/or is judgment-proof. This is more of a rule rather than exception given the ability to act anonymously, difficulty tracing the origin of malfeasance, and perpetrator profile (i.e., juvenile miscreants) associated with the Internet.

Similarly, contract law redresses injuries that result from the failure of one party to live up to his part of a prior agreement. So, unless Acme has bargained with Widgets, Inc. to cover the damages that might result from an unknown intruder using Widgets' computers to launch an attack against Acme's systems, contract law would not provide relief. The rule in most cases is that the company used as a cut-out will have no prior relation with the damaged party, thus eliminating any hope for redress under contract law.

As a result, victims are likely to seek compensation for their losses by resorting to the civil arena, where the actual perpetrator need not be identified, the pool of entities with the ability to redress losses is much less discriminate (read: deep pockets), and prior promises need not exist. Specifically, negligence claims may be potent if the victim can show that the "insecure" party (1) owed a duty to use reasonable care in securing its computer systems; (2) breached that duty by failing to maintain adequate computer network security; and (3) was a reasonably recognizable cause of actual damages that resulted from his insecure computer network.

If we agree that there should be a standard of care to secure networked computers, thereby favoring a legal right to recover from the "insecure" party in negligence, we must ask:

What is the basis for imposing a duty to secure its computer system?

Who does that duty apply to in the Internet community – SWV, WebCo, ISP, and/or user? What is the scope/standard of care for each party?

Basis for Imposing a Duty to Secure Computers

Although foreseeability of harm is a primary determinant in deciding whether to assign duty, factors such as competing socioeconomic policies, assumption of responsibility by the allegedly negligent party, and the injured party's reliance have been instrumental.

FORESEEABILITY OF HARM

To say that WebCo had a duty to protect Jill User from harm as a result of a computer intrusion means that there is a standard of conduct (see Fig. 1) that WebCo must fol-

low for the protection of others on the network against unreasonable risks. Namely, WebCo must use reasonable care in adequately securing its computer systems.

STANDARD OF CONDUCT

Reasonable Care – what reasonable measures can be taken to secure your system?

Foreseeability – if those measures were not taken, who would be harmed?

Reasonably Perceived Risk of Harm – was the harmed party created by not reasonably securing your system?

Figure 1

What is "reasonable care"? It is the attention, knowledge, intelligence, and judgment defined by society for its protection. These objective qualities have traditionally been measured by the foreseeability of injury to the aggrieved party.[1] In other words, there is no duty of care owed to an injured party who is not within the foreseeable risk of harm created by the defendant.

SOCIOECONOMIC POLICIES

The costs associated with insecure computers on the Internet weigh heavily in favor of assigning a duty to secure systems. Direct monetary damage due to denial of service (DoS) attacks and unauthorized compromises can, have been, and will continue to be substantial. This can take the form of business downtime which is often measured in terms of revenue losses, compensatory payments, employee downtime, inventory costs, depreciation of capital, and actual damage to a company's own computer systems. For example, distributed network sites can lose $20,000–$80,000/hour in centralized network downtime.[2]

Other indirect monetary costs take the form of security infrastructure upgrades, loss of customer base, damage to business reputation and public image, destruction of potential partnerships, delays to market, and capitalization losses. For instance, the infamous February 2000 DDoS was estimated to have caused about $1 billion in capitalization losses and $100 million in lost sales and advertising.[3]

Duty creates an incentive to use higher care. If parties are not held accountable by liability for failure to secure, there is an economic incentive to use the lowest care. For example, if there were no law against theft, would people think twice about taking without paying? Would spammers continue to disseminate digital junk mail if they faced stiff fines?

The need to secure information will persist and magnify. For instance, in the corporate world where intellectual property is often the only thing separating competitors, it is cheaper and easier to steal information than to develop it.[4] The motivation driving acts of theft, destruction, and misfeasance combined with increasing expertise, sophistication, and effectiveness of attacks on networked computers ensures the importance of information security.[5]

Security will become more difficult and important as evolving networks grow increasingly complex. This complexity means that security bugs in software will proliferate, vulnerabilities will multiply with the increased modularity of software, extensive testing will be demanded, and security analysis will become more difficult.[6]

This also means that the danger of false victimization claims grows more prevalent in complex digital environments. For instance, the added functionality that is in the fore-

front of system design comes with a vulnerability cost. The appliances and other devices being made with programmable computer chips and Internet access are a case in point. Technology will advance regardless, but without assigning due care, there should be little expectation of security. But by assigning reasonable security measures, the wildfires due to insecurity can be downgraded to a controlled burn.

Finally, assigning vendors, service providers, WebCos, and users a duty to secure distributes the risk of loss among the people who employ the technology. This policy recognizes that no single entity is responsible for the security of the entire Internet, but each should be responsible for his/her identifiable part.

. . .no single entity is responsible for the security of the entire Internet, but each should be responsible for his/her identifiable part.

REASONABLE EXPECTATION OF SECURITY

Reliance by Injured Party

In general, reliance on the performance of another party can factor into the imposition of duty. If A depends on the protection of B, and B has knowledge (actual or imputed) of that dependence and the ability to protect, A is relying on the security capabilities of B. If you give your credit card number to a WebCo over the Internet, you depend on WebCo to protect this fiduciary data, WebCo is aware that this number is not for public distribution, and it has the ability to safeguard this data. In this way, you have a reasonable expectation that this information will be kept secure and rely on WebCo to implement appropriate safeguards. However, WebCo may not be using reasonable care if your credit card number is stolen from its database because it was stored unencrypted on the Web server.

Reasonable expectations of security are created in various ways and help determine who is entitled to protection. Industry customs are one way to measure the objective reasonableness of a victim's expectations of care. Widely disseminated bulletins (SANS, CERT/CC, BugTraq, etc.) and company policies and procedures that address computer security put users on notice that there are generally agreed upon methods to assess security and protect systems. This notifies people that data and transactions, for example, can be secured, and their subsequent actions are made with that in mind. In this way, duty may arise from information security best practices that shape the expectations of people outside.

Reasonable expectations of security are also shaped by the discrepancy in authority between the injured party and the allegedly "insecure" party. Because of the authority and control exerted by landlords over common-use areas (walkways, stairways, elevators, lobbies, front doors), they may have a duty to secure and can be held liable when defective security exists. Likewise, there are entities that have the ability and authority to manage the risks of network insecurity. When this is manifest, that party creates a reasonable expectation that security exists and will be maintained.

For example, an ISP which exists to provide users with Internet connectivity, could reasonably be relied on to forestall or mitigate the damages from a DDoS. The reciprocal knowledge that ISPs can monitor and control network traffic affecting users may create a reasonable expectation that the ISP configures routers to block directed broadcast traffic during a DDoS, for example. The ISP is aware that users are cognizant of this attack yet are incapable of implementing the same level of protection. As such, the ISP's knowledge of users' reliance on its authority to implement security may provide a basis for imposing duty.

Each party who affects computer network security . . . may owe a duty to exercise reasonable care in maintaining adequate computer security.

Assumption of Duty by "Insecure" Party

Another basis for imposing a duty to secure may arise when one party assumes the responsibility and places the injured party in a worse position. This is similar to duty based on reliance, but involves more explicit assurances by the "insecure" party. Here, reasonable expectations of security may arise when one party makes representations as to current/future security assurances or voluntarily assumes control of security, and leaves another party in a worse position by failing to use reasonable care.

A party who voluntarily assumes the performance of a duty is required to do what an ordinary, prudent person would do in accomplishing the task. If a landlord installs an alarm system leading his tenants to forego deadlocks, and an intruder causes injury because of careless installation, the landlord may be in dereliction of duty. Likewise, a software vendor may create a false sense of security in its product by misrepresenting protections or implementing them carelessly, thereby causing an end user to eschew other safeguards. In this way, the vendor has assumed the duty to disseminate a reasonably secure product and has left the user in a more vulnerable position, thus providing a basis to impose a duty to secure.

Who Owes a Duty to Secure Computer Systems?

Each party who affects computer network security – software vendors (SWVs); services providers (ISPs/ASPs); WebCos and their respective IT managers, directors, and system administrators (sysadmins); individual users – may owe a duty to exercise reasonable care in maintaining adequate computer security. The standard of care / scope of the duty will depend on the quality and quantity of the measures needed to secure relative to the actor's ability to control, assumption of responsibility, and/or socioeconomic concerns.

Software Vendor/Manufacturer Duty

Should a vendor be liable for failure to secure when its software provides the means for an intruder to damage an end user (ISP, WebCo, or consumer)?

Foreseeability: Knowledge and Ability to Control

The harm to users of software with known vulnerabilities is foreseeable, and prevention is well understood. For example, developers of Web-server applications invariably focus on business and technical concerns (functionality and time-to-market) at the expense of security, thus allowing attackers to deviate from the script's intended application. It is no secret that programmers have had the knowledge and ability to deal with buffer overflow vulnerability for decades. Since the coding and hardware solutions slowed down the program, buffer checks were eliminated.[7] This appears to be the rule, as newer versions of products continue to harbor the same vulnerabilities that plagued earlier versions. Repeatedly condoning demonstrably flawed designs proven to be problematic is remarkable because it indicates a conscious choice to disregard security measures in the face of knowledge of their importance.

Also, the mere existence of security vulnerability alerts, posting of patches, and prerelease warnings by both the vendors/manufacturers independently and in response to security watchdog bulletins[8] show tacit knowledge that these products are routinely targeted by intruders as a means to break into systems. Notwithstanding these indicators, foreseeability of harm to victims would be imputed to vendors by virtue of the widely disseminated news of Web companies, users, and ISPs' incurring disruption in business or theft of information because of the exploitation of product vulnerabilities.

Although knowledge alone would be insufficient to impose a duty, the SWV has the ability to control the extent of many security exploits. Just as gun safety would be more easily enforced if safety locks were required of manufacturers rather than solely relying upon user adherence to a wide array of handling and storage procedures, SWVs are in a position to design-away the Achilles' heel of computer security.

. . . an operator's safe configuration of software is only as good as the underlying code.

Party in the Best Position: Burden of Security

Another factor used to determine whether SWVs owe a duty to help secure networks looks to the party in the best position to secure networks. This may be judged by the relative burden of implementing security along with any negative social consequences. The technical burden involved with security evaluations of complex systems weighs in favor of SWVs bearing the brunt of implementing security in product design. In addition to technical imbalance, quantitatively it is more reasonable to assign software security to a single body of producers versus shouldering it on the product's 100 million users, for example.[9]

There is a drastic imbalance between the knowledge and skill needed by ordinary users to install and operate programs versus the technical proficiency and resources needed to configure and run them securely. This holds true for system administrators, albeit to a lesser extent, insofar as the skill and resources needed to secure systems are far more demanding compared to the ease with which harm can be wrought in this automated attack environment.[10]

Further, the technical proficiency expectations of IT professionals are irrelevant if the vendor produces a digital land mine. Just as a contractor can follow a blueprint copiously yet construct a house that crumbles during inclement weather, an operator's safe configuration of software is only as good as the underlying code. Thus, reasonable preventative measures imposed on SWVs – programming against known/knowable security vulnerabilities, and shipping software with safer default settings – would stopgap the source of a majority of network insecurities and further society's interest in maintaining a secure computing infrastructure.

Opponents to assigning duty on SWVs argue that doing so would unduly hamper market competitiveness by elevating operational costs, inhibiting functional improvements in software, and impeding product releases, the costs of which will ultimately be borne by the end user. However, ascribing a duty to exercise reasonable care does not entail wholesale abolition of every software vulnerability. Rather, it balances the responsibility in proportion to the level of authority. The alternative to not extending this duty to SWVs is to foster an unreasonable expectation that persons ill-equipped to configure for security will eliminate vulnerabilities. Furthermore, the functional effects of unusable software caused by insecure design are far more ruinous than making due with an application that does not auto-complete words, for example. Indeed, the expenses associated with cleaning up after an intrusion that could have been prevented by more secure software are much more prohibitive than heightened product costs at the front end.[11]

Reasonable Expectations of Security

Software end users have a reasonable expectation that the product will not be an open invitation for malicious intrusions. That is, a user who relies on the SWV to disseminate a product that functions adequately and does not place him in a worse position for having purchased it, is not acting unreasonably. For example, if a SWV makes a word processing program that bars a user from composing a simple letter, or exposes

. . . it is unreasonable to expect users to appraise the security of off-the-shelf software . . .

the user's entire system to any number of invasions, that SWV has created a plight for the user. What if a homeowner bought an air-conditioning unit that arbitrarily opened doors and windows at any time of the day or night to enhance cooling features?

One need not search far for examples of software that was bought with an expectation that it would perform as advertised, yet placed the user in a detrimental position. The MS Office Assistant feature illustrates how a vendor created reliance on the part of its customers and then left them in a worse position. Little did users know that when the jovial Paperclip prophetically appeared at the behest of a comatose user, the scripting technology that fueled his trojaned white horse enabled yet another back door into the application and system at large. When a Web page or HTML-enabled email was clicked, the script could add or delete files. The distinction with this security hole is that it was not a result of poor programming but was an intended "feature" built in to the program to allow the vendor to run macros through a back door. Even an exceptionally knowledgeable and scrupulous user who may have attempted to verify the risks of using this type of scripting would have found it to be labeled "safe."[12]

What is more damning is when a SWV makes explicit security pledges that are false. Users' reasonable reliance on the security of software is betrayed when prophylactic statements are made, the vendor is aware of the confidences created, and the admonitions are false. Simply put, this is Misrepresentation, and to not hold the vendor responsible for resulting damages is to invite deception. It is akin to a landlord making assurances about apartment-complex security, yet placing a master key ring in the lobby without informing the tenants about the very existence of the keys, let alone their open accessibility.

For example, labeling a control "safe for scripting" exemplifies how a relationship between parties with unequal knowledge and capability fosters a reliance that can place the "weaker" party in a worse position. Controls, such as Active X, are used extensively throughout Windows platforms, especially in Web-based applications. Safety assertions in this context can reasonably be interpreted to mean that the control cannot be used by an intruder to damage or compromise one's system. Yet, auditing or examining control properties are arduous and invoke the use of a specialized tool within the Windows registry. Coupled with the fact that controls are ubiquitous, it is unreasonable for users to discount the patent safety assurances of a product licensed by a dominant software manufacturer, and have the ability and wherewithal to search and verify the veracity of such avowals. Thus, a high degree of trust must be placed in the vendor-author that when viewing a Web page, newsgroup posting, or email message containing the safety-branded control, an intruder will be prevented from disabling Office macro warnings and executing arbitrary code.

If it is unreasonable to expect users to appraise the security of off-the-shelf software, then absurdity transudes new meaning if vendors are permitted to issue programs that lead users to believe that an application is secure yet wreaks havoc on a system, leaving users with neither warning nor recourse. If that is the case, society should tolerate clothes irons that may discharge electrical sparks and issue warning alarms after homes are incinerated.

Socioeconomics: The Emperor Has No Clothes

Consumers are quick to demand cars free of any type of defect, yet continually accept software products that are "recalled" for being unsafe. If Ford released a car into the marketplace that was continuously being recalled for potentially injurious defects or,

rather than undertaking safety R&D, used its consumers as a crash test base for design flaws, history has shown that this would not be tolerated.

Socioeconomic considerations support the imposition of a duty to secure on SWVs. Accepting the argument that bugs in computer systems and software are inevitable, it would be unreasonable to expect that SWVs should test for and eradicate every insecurity. Nevertheless, if the current lack of accountability persists, end users will continue to bear the risk and cost associated with applying the vendors' bandaids to the broken bones that hackers can readily x-ray.

Furthermore, imposing a duty creates an economic incentive to render higher-quality products. Without liability for insecurity, there is an economic incentive to create lowest quality.[13] Therefore, unless SWVs are held accountable for designing insecure software, speed, features, and options will dominate the SWV agenda. Currently, users face an uphill battle in attempting to prove that a vendor was negligent in not using reasonable care to design with security in mind. In a dispute between a user and vendor, it is assumed that SWVs are not negligent. Since the burden of proof is on the user, the SWV is in the clear unless the user can prove the elements of negligence. Statutes such as UCITA, shrink-wrap licenses, and general disclaimers work against any attempt to prove that a SWV did not use reasonable care, not to mention the cost involved in proving this on a case-by-case basis acts as a disincentive to take on Goliath. Therefore, if duty is not defined and imposed at some point, it may be infeasible for a user damaged from an insecure software product to seek redress. Furthermore, society will grow increasingly desensitized to the real damages being wrought, and ramifications of insecure software will become an accepted cost and defining attribute of networked society.

Without liability for insecurity, there is an economic incentive to create lowest quality.

SERVICE PROVIDER (ISP/ASP) DUTY

Should an ISP be held liable for failing to implement reasonable security measures that would have prevented or mitigated damages to its customers by malicious intruders? The nature of a service provider's authority (knowledge and ability to control security vulnerabilities) and its assumption of responsibility create a reasonable expectation that it implement security measures.

Foreseeability – Knowledge of Harm

ISPs arguably possess the same awareness of intrusion methods and targeted victims as product vendors/manufacturers. Just as software vulnerabilities are a common target, so, too, are poorly configured network servers. These servers are well-known in the hacker lore and finite in number. That is not to say that ISPs ought to be Reserve White Hats, but they should have imputed knowledge of the reasonably perceived risk that an intruder will try to use their network to harm their customer(s). The reasonably perceived risk of not implementing security measures at the service-provider level is that its customers will be targeted, invaded, and ultimately damaged by online miscreants. The injured customer(s) is owed a duty since she falls within the risk of harm controllable by the ISP.

This imputed foreseeability might also extend to downstream victims of an attack launched from ISP clients. In this way, the ISP resembles a public contractor that undertakes to work in a public way such as on a highway, street, or sidewalk. Here, the ISP contracts through a service level agreement (SLA) to work in the Internet, a public way. The elevator contractor or auto repairperson is deemed to automatically foresee that negligent performance (misfeasance) will likely cause injury. A contractor's failure

Service providers are increasing their exposure to negligence liability by implicitly and explicitly assuming the duty to secure their networked customers.

to perform may lead to liability if it is foreseeable that nonperformance will likely cause injury. Likewise, an ISP's failure to implement some security within its network does not limit exposure to potential harm to its customers, alone. Other entities share and utilize the digital accessways such that even though they are not in privity of contract with the particular ISP, they are foreseeable victims of its nonfeasance.

Control

As a gatekeeping authority, ISPs are in control of their respective networks to the extent that they are the only actors capable of directly implementing security mechanisms that affect the whole of their customer base. For example, they can turn off Web connections that do not follow up with valid HTTP requests, employ tools to scan systemwide for the installation of any host or broadcaster software, and help customers prevent spammers from spoofing their addresses. The same identifying features (i.e., defined signatures) that allow ISPs to block spam are present in email viruses and empower ISPs to stop them at the email server. Nevertheless, some ISPs are reluctant to effectuate their ability to secure their networks. Similar to the SWVs' failure to code against known bugs out of concern for market deadlines, ISPs may forego filtering or scanning out of concern for degradation of network performance and additional costs.

This network control and ability to enact security therein is a unilateral capability, as service subscribers lack both the technical know-how and/or operational capabilities to implement these same large-scale security measures. For example, some viruses can only be detected and halted using server and proxy-based antivirus and filtering tools. A user's desktop antivirus product would be ineffectual. Because of this authority, ISPs should bear a duty to secure since they are capable of providing reasonable security to protect another party whose ability to provide for its own safety is restricted.

Assumption of Duty

Service providers are increasing their exposure to negligence liability by implicitly and explicitly assuming the duty to secure their networked customers. As ISPs evolve and take on more functional authority they may be ultimately self-imposing a duty to establish and maintain security. By assuming the duty to secure they may be creating a reasonable reliance that users will be protected from intrusions.

For example, some providers offer free spam blocking in response to customer complaints. This same capability and authority that enables email and Web-surfing monitoring can and is marshaled by some ISPs to prevent viruses or stopgap DoS attacks against customers on their network. This drive to satisfy customers may unwittingly raise the expectations of customers that they will be protected from common threats. Even though most ISPs are not explicitly contracting security into their service level agreements, the generic disclosure statements highlighting the company's commitment to security could bear on expectations. Take the case where a business is shut down as a result of its ISP's failure to use spoof filters, even though most other ISPs, including its competitors, successfully averted the attack. The damaged company might argue that its ISP's actions fell below the standard of care referenced in the disclosure statement and manifest by the actions of the majority of other ISPs.

Thus, providers may be opening themselves to negligence claims if customers are aware of these measures, providers realize the users' reliance upon these security measures, they miscarry these self-protection strategies, and an intruder wreaks damage.

Socioeconomics

Reliability of Web hosting services is key to e-commerce proliferation. Reliability presumes security insofar as a network service or applications with widespread and exploitable vulnerabilities cannot be counted on to deliver consistent and repeatable performance. In this way, e-commerce depends upon the assurance of secure networks. To exemplify, an insecure Web server that is vulnerable to malicious acts opens WebCos to a deluge of operational damages, not to mention the costs of reimbursing their own customers who relied upon service. This has an overall negative effect on the propagation of business and transactions in the digital realm.

A related concern raised by imposing duty on service providers is the effect it will have on business enterprise technology and the need for government regulation. As software continues to migrate from ownership of applications that are run at the user level to leasing of software maintained at a centralized network, the acceptance of these enterprises will depend on the reliability of the computing, which boils down to the security of the application.[14]

WebCo Duty: Security Obligation to Downstream Victims

Should a WebCo be liable when its insecure computer(s) was used by an intruder to damage a third party? Is it reasonable to expect companies hosting Web sites to anticipate misconduct directed at their systems? As with vendors and ISPs, WebCos should owe a duty to exercise reasonable care in maintaining adequate computer security based on the legal rationale underlying negligence. Namely, to the extent that a WebCo has knowledge and the ability to control the harm to a third party from an intruder, the situation is no different than in the physical world and the same standards of conduct should apply.

Should a WebCo be liable when its insecure computer(s) was used by an intruder to damage a third party?

To date, no US case has squarely addressed liability for failure to secure, though a presage to this novel claim arose in late 1999. Pacific Bell was the target of a class action lawsuit alleging, among other things, negligence for inadequately protecting its customers against unauthorized Internet intrusions and failure to inform them that the Digital Subscriber Line (DSL) connections were not secure.[15] Regardless of the outcome, this claim illustrates the evolution of users' expectation of care regarding ISPs' duty to secure the network. Furthermore, the decision to pursue litigation for breach of this alleged duty has lowered the threshold beyond which a multitude of similarly situated parties had not previously sought redress.

Interestingly, a case embracing this issue has been levied in the UK against a prominent American company for lax security in "allowing itself to be hacked."[16] In June 2000, a UK-based ISP sought damages from Nike.com for negligent security when its domain was hijacked. The argument alleged that by selecting the lowest form of security (called "mail-from") when it registered its site, a criminal was able to spoof email, alter Nike's registry data, and re-direct Nike.com's traffic through the UK Web server. Damages were sought for the time and money associated with administering the overloaded servers.[17] Others argued that responsibility belongs with the domain registrar, Network Solutions, for allowing the spoofed email from the Nike authorized contact without the password required to change the Nike domain status. Despite the disparate damages allegedly caused by the insecure parties – Pac Bell, Nike, or Network Solutions — the underlying thread is a demand to recognize and account for exposures created by insecure network security.

Would imposing a duty to secure its computer systems and subsequently holding a WebCo liable for failure to safeguard be an unreasonable burden?

Defining Reasonable Care in the Environet

Traditionally, downstream liability determinations hinged on proof of causation: how far down a chain of connected events leading to the injury would society be willing to ascribe responsibility? The environet (Internet environment) challenges the very meaning of "downstream" since everyone online is but one click away, placing all connected users within a reasonably perceived risk.

In other words, the pool of foreseeable plaintiffs in the physical world is limited by time, location, and predictable relationships. On the Internet, when those measuring sticks are removed, the liability chain transforms into a cloud encompassing a torrent of probable plaintiffs. For instance, in the property-based world, courts would have no trouble finding a chink in the chain of causation when One-Armed Jack sues Acme for leaving its warehouse unattended and unlocked, with the keys in the ignition of its delivery trucks. Acme's nonfeasance enabled Snidely Whiplash to abscond with the vehicle. In the midst of this transgression, he displaced Jack's limb as he was exiting his car. The same scenario played out in the Environet entails "r00t Whiplash" routing his activity through 15 different hosts in five countries and storing his exploit on an insecure host at Acme. This program directs a malicious payload at some business one week later, but Victim.com happens to suffer a denial of service (DoS) and business disruption in the course of routing the scripted traffic.

In the first instance, society is not willing to impose a duty on vehicle owners (Acme) to protect persons on the highway from thieves. In other words, since it is not reasonable for Acme to foresee that a thief would be an incompetent driver, Acme could not be a cause of the injury.[18] Applying this rationale to the second scenario, the same decision may be trivially apparent given that the harm occurred well after the insecure incident, in a location far away. However, the critical question is whether the conduct of r00t Whiplash was foreseeable. A strong argument can be made that Acme had substantial reason to foresee that maintaining an insecure site increased the risk of a compromise to its own system, and correspondingly, that a criminal would maximize the vulnerability to exact harm on others connected to the Internet. Thus, Acme would have a duty to persons on the digital highway to use reasonable care to keep its system from being controlled by a digital vandal. Under this reasoning, the chain of causation may indeed link Acme's failure to secure with the damage to Victim.com.

Socioeconomics

Would imposing a duty to secure its computer systems and subsequently holding a WebCo liable for failure to safeguard be an unreasonable burden?

When the cost of accidents is less than the cost of prevention, a rational, profit-maximizing enterprise will pay civil judgments to accident victims rather than bear the larger cost of avoiding liability.[19] Following this rationale, WebCos may choose to risk paying judgments to downstream victims injured by its lack of security or insure against the risk. This would likely mean that the insurance costs would be factored into its pricing or business costs in some way, which could ultimately translate into computer intrusion costs being borne by the parties entitled to protection.

At the opposite end of the duty spectrum, where downstream victims of insecure computers are not extended protection under negligence law, the situation resembles a digital caveat emptor. Only, in this case, it would be "let the Netizens beware," and in the absence of some contract-based theory of liability or yet-to-be-established regulation, entities connected to the Internet would assume the risk that a miscreant could attack,

intrude, and wreak damage upon them. However, history has proven that whenever a major technology or industry has proliferated to effect society at large, some measure of social control will follow. If judicial imposition of duty and liability is not one such mechanism, regulations, legislation, and insurance will unquestionably rule. One needs only to refer to the automobile industry as an illustration of how its socioeconomic impact was dealt with on all three fronts.

Foreseeability of Harm

It is reasonable to expect that companies hosting Web sites should anticipate misconduct in the form of attempted intrusions. WebCos' indifference toward the security of their machines can contribute to a disastrous loss for many other Internetizens and dot-coms. The ability to capitalize on security vulnerabilities and thereby commit crimes anonymously and more easily is what fuels the criminal element in a network society. A significant underlying theme is that regardless of the measures not taken to protect its own proprietary data or information assets, a WebCo's lack of computer security plays an identifiable part in the probability and reality of another Internet entity being intruded on and damaged. Thus, both the victim (other Netizens/WebCos) and harm (theft of information; denial of service; theft of service; damage to computer systems, etc.) are not so inconceivable as to remove them from the realm of foreseeability.

It is reasonable to expect that companies hosting Web sites should anticipate misconduct in the form of attempted intrusions.

For example, the Oregon State University computer used by the hacker claiming to steal 300,000 credit cards from CD Universe was only partially secured because it was not thought to harbor anything of value.[20] This rationale undoubtedly accounted for the slapdash security on many servers nationwide that helped make possible the infamous February 2000 DDoS attack on Yahoo, ZDNet, eBay, CNN, Amazon, and eTrade. The popular media is satiated with instances where businesses are compromised. These reports focus on the victimized businesses and efforts to trace the miscreants. What is rarely reported, however, is the trail of insecure hosts along the way that facilitated the intrusion.

In the non-digital world, a grocery store owes a duty of care to secure against vandals preying on would-be patrons. If the store owner fails to attend to security concerns – hiring a security guard, putting lighting in the parking lot, installing cameras – and someone is victimized by Hamburglar as a result, a lawsuit would be filed before the purse handle was cut. However, if Trinkets-R-Us sets up a Web server out of the box, without configuring for security, the inferential leap to hold it accountable for ensuing damages is not being made. In this case, Magic8.com may suffer loss of business for hours or days as a result the DDoS servant launched from Trinkets' compromised server.

Similarly, a company that sets up shop in the Internet is presumed to invite/entice visitors. This undertaking should be accompanied by a corresponding degree of care measured in terms of some modicum of security against third-party malfeasance. Surely, the presence of a physical threat in the grocery instance would justify a heightened expectation to secure on the part of the store. However, does the economic/physical harm distinction justify tolerating a WebCo that ignores security? This is answered by recognizing the liability realities of companies failing to protect financial data needed to consummate online purchases. If online companies take no measures to protect their customer credit card databases, thereby putting the economic health of their customer in jeopardy, courts would have no trouble holding them responsible, and the MasterCards of the world would not be so quick to write off this type of fraud.

The traditional notion that there is no duty to protect others is challenged by the ubiquitous, distributed, and tightly knit nature of network computing.

User Duty

Does an individual user owe a duty to reasonably safeguard their systems against unauthorized access for the protection of downstream victims? The answer depends in part on users' ability to implement safeguards and overcome common network vulnerabilities; users' knowledge of the risk of failing to secure; and society's willingness to expand the scope of foreseeable plaintiffs.

Control

As there is advancement in solving the issue of uniformly and reliably informing and enabling average users how to fix their vulnerable systems, control will factor into assessing a user's duty. To the extent that users have the ability to secure – through reasonable instructions accompanying a product, disseminated by a service provider, or via widely publicized bulletin(s) – their failure to install available patches or enable antivirus software may no longer suffice as an excuse.

Foreseeable Risks and Victims

As discussed previously, the computing community of vendors, service providers, and Web companies has knowledge that miscreants seek unauthorized entry. To the extent that the general user can be imputed with awareness of this penchant, he should be on notice of the potential harm in failing to secure. As network computing has become part of the daily lives of society on the whole, security issues are no longer confined to the computer-related workforce. Rather, first-hand exposure and media attention paid to security exploits has raised the public awareness and contributed to a more informed user populace. To be sure, virus propagation and malicious exploits occurred prior to the Love Bug and Trinoo, but consistent coverage in major news media headlines was unprecedented. In this way, there is a stronger argument for imputing knowledge of the foreseeable risks to end users today than even a few years ago.

In addition to the foreseeability of the danger, the conceivable parties within the purview of that danger must factor into a duty analysis for users. To a certain extent, the same popular media mechanisms (CNN Headline News, *New York Times*, etc.) that raise awareness of insecurity risks impart knowledge of the person(s) likely to be harmed. Furthermore, the ignorance card may carry less weight in situations where a user had been intruded on or infected in the past and was put on notice. Indeed, other parties connected to the network are foreseeable victims of a user's failure to safeguard his system. A user's indifference toward the security of his system can contribute to a disastrous loss for many other Netizens and dot-coms.

Socioeconomics

The degree to which courts are willing to extend the pool of foreseeable victims to encompass other networked users will hinge on socioeconomic policies. The traditional notion that there is no duty to protect others is challenged by the ubiquitous, distributed, and tightly knit nature of network computing. Based on the principle that an orderly society demands authority be accompanied by responsibility, the fact that nearly every host connected to the Internet exacts some control over the others should imbue networked users with comparable responsibility. Unlike point-to-point telephony, Internet communications are three-dimensional, thus rendering every connected host a potential portal to any and all others. This interconnectedness makes security an embedded dynamic such that there is no clear boundary separating entities on the Internet. In the property-based world, security is based on drawing lines that separate you from outsiders. If you fail to protect yourself by not locking your door, for exam-

ple, then your property is the casualty. Responsibility for the invasion does not shift to your neighbor four doors down. Correspondingly, you have no duty to secure your premises for the protection of your neighbor. Short of disconnecting from the network, self-protection in networked society is a misnomer since each host's security is linked to each other's.

Insofar as electronic commerce is driving the influx of users onto the network, placing a duty on those that choose to engage in this activity recognizes that security is an embedded risk that should be distributed accordingly. Where suppliers offer the means to prevent viruses, dissuade port scanners, or detect unauthorized access attempts, for instance, users should be held to a reasonable standard in preventing the ill-effects of these activities. For example, a user employing one or more of these prophylactics may prevent a hacker from being employed in a distributed denial of service attack against a commercial Web site.

CONCLUSION

Whether you are a victim-symptom or a liable-cause, reality dictates that networked computers are vulnerable to undesired actions and resulting harm owing to computer security vulnerabilities. The nature of this environment both forces society to redefine what is reasonable and facilitates the shifting of responsibility. To this end, the critical question to be addressed is: should insecure computers be tolerated given the nature of modern computing infrastructure? Legal claims based in negligence prove to be a viable answer, insofar as they attempt to assess responsibilities, define duties, and assign liabilities amidst this new interconnected environment, where both traditional and unprecedented relationships, conduct, and consequences intertwine.

The potential onslaught of claims arising from insecure computer systems is not a veiled threat but, more aptly, a ripening promise. This article has highlighted the parties and common scenarios likely to spawn litigation for failure to secure computer systems, between vendors, service providers, Web businesses and individual end users within networked society. Indeed, there is support for the imposition of duty to safeguard networked computers. This duty arises from traditional factors used to judge negligence: the foreseeability of harm for failure to secure; reliance on the party in the best position to implement and maintain security; the assumption of responsibility to secure; and, various socioeconomic considerations. The scope of this duty can be defined in light of these factors, recognizing the various levels of knowledge, control, and identifiable effect that each respective party has on securing networked computers against injurious damages.

References

1. *Palsgraf v. Long Isl RR Co.*, 162 N.E. 99 (N.Y. 1928).

2. The Gartner Group estimates the average cost of downtime in brokerage operations at $6.5 million/hour; eBay paid $3.9 million in credits to customers for a 22-hour service outage in June 1999. See "Towards a Dependable Self-Healing Internet," Testimony to the Senate's Subcommittee on Communications, March 8, 2000 (prepared statement of Raj Reddy, co-chair, President's Information Technology Advisory Committee; Herbert A. Simon, professor of computer science and robotics, Carnegie Mellon University). See generally "E-Business Survival during Denial of Service Tornadoes" (viewed August 12, 2000) *http://gartner6.gartnerWeb.com/public/static/store/networking.html.*

. . .should insecure computers be tolerated given the nature of modern computing infrastructure?

3. Matthew Kovar, "$1.2 Billion Impact Seen as a Result of Recent Attacks Launched by Internet Hackers," Yankee Group, February 14, 2000, *http://www.yankeegroup.com/Webfolder/yg21a.nsf/pusharea/$1.2+Billion+Impact+Seen+as+a+Result+of+Recent+Attacks+Launched+by+Internet+Hackers*. See generally Cahners In-Stat Group (viewed July 16, 2000) *www.instat.com/abstracts/ia/1999/is9906spabs.htm*.

4. See generally "Annual Computer Crime and Security Survey," Computer Security Institute and Federal Bureau of Investigation (1999) (e.g., there was a $50,000 "bounty" placed on notebooks belonging to any executive of an energy company involved in bidding on international projects). See Susan Breidenbach, "How Secure Are You?" *Information Week*, August 21, 2000, p. 74.

5. See generally "CERT/CC Overview Incident and Vulnerability Trends" (viewed August 20, 2000) *http://www.cert.org/present/cert-overview-trends/tsld001.htm*.

6. Bruce Schneier, *Crypto-Gram*, March 15, 2000, *http://www.counterpane.com/crypto-gram-0003.html*. Complex systems must be broken into manageable pieces; security often fails where two modules interact; complex systems demand increased testing of specifications, design, and implementation.

7. Matt Bishop, "UNIX Security: Security in Programming," SANS '96, Washington, DC, May 1996. "A small number of flaws in software programs are responsible for the vast majority of successful Internet attacks because attackers don't like to do extra work. They exploit the best known flaws with the most effective and widely available attack tools. And they count on organizations not fixing the problems. System administrators report that they have not corrected these flaws because they don't know which of over 500 potential problems are the ones that are most dangerous, and they are too busy to correct them all." Quoting Alan Paller, "The Ten Most Critical Internet Security Threats," SANS Security Alert, May 2000, pp. 1, 2.

8. See generally CERT/CC – Computer Emergency Response Team / Coordination Center, *http://www.cert.org*; Security Alert for Enterprise Resources, h*ttp://www.safermag.com*; Security Focus, *http://www.securityfocus.com*; BugTraq, *http://www.bugtraq.securepoint.com*; SANS Security Digest Services, *http://www.sans.org/newlook/digests/SAC.htm*; Attrition, *http://www.attrition.org*; Microsoft Technical Updates, Microsoft Security Bulletins, *http://www.microsoft.com/technet/security*.

9. For example, the Apache Web Server constitutes nearly two-thirds of installed Web servers, yet every copy is shipped with CGI vulnerabilities that can lead to root access to the server. Breidenbach, *How Secure Are You?* p. 74. There are about 100 million MS Office customers. Security Wire Digest, *ICSA Information Security Magazine*, July 24, 2000 *http://www.infosecuritymag.com/securitywire/index.html*.

10. For example, many attacks are batch mode processes that discover vulnerabilities, compromise these weaknesses, install daemons, and cover their tracks.

11. See generally "1999 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues & Trends*, Winter 1999. This survey tallied $266 million in total losses due to computer security threats.

12. See, CERT Advisory CA-2000-07, "Microsoft Office 2000 UA ActiveX Control Incorrectly Marked 'Safe for Scripting,'" May 24, 2000, *http://www.cert.org/advisories/CA-2000-07.html*.

13. Bruce Schneier, *Crypto-Gram,* April 2000, *http://www.counterpane.com/crypto-gram-0004.html.*

14. "Application Service Providers: Are They Sitting Ducks?"; SQL *Server Magazine*, April 7, 2000, *http://packetstorm.securify.com/mag/winsd/winsd.040500.txt*.

15. Todd Spangler, "Home Is Where the Hack Is," ZDNet News, April 10, 2000, *http://www.zdnet.com/zdnn/stories/news/0,4586,2524160,00.html* (Nathan Hoffman initiated this suit after learning that his DSL-connected computer was wide-open to potential attacks, and discovering that he was being port-scanned many times a day from worldwide locations).

16. David Raikow, *New Legal Storm on Net Horizon*, ZDNet News, July 4, 2000, *http://www.zdnet.com/zdnn/stories/comment/0,5859,2597881,00.html.*

17. Craig Bicknell, "Whom To Sue For Nike.com Hack," Wired News, June 29, 2000, *http://www.wirednews.com/news/politics/0,1283,37286,00.html.*

18. See *Avis Rent A Car System, Inc. v. Superior Court*, 12 Cal. App. 4th 221 (1993).

19. *See* Richard A. Posner, "A Theory of Negligence," 1 *J. LEGAL STUD.* 29 (1972) (citing *US v Carroll Towing Co.*, 159 F.2d 169 (1947)).

20. Ted Bridis, "Hacker Victims or Unwitting Accomplices," Associated Press, February 10, 2000, *http://www.canoe.ca/TechNews0002/11_hackers.html.*