COVER SHEET

PAPER

PRESENTED AT THE TWENTY THIRD ANNUAL NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE

Title: The Curse of Service: Civil Liability for Computer Security Professionals

Author: Arthur J. Wylene
Law Student - Juris Doctor Candidate, 2002
New College of California
School of Law
50 Fell St.
San Francisco, Ca 94102
Voice: (916) 925-5948
Email: awylene@hotmail.com

Point of Contact: Arthur J. Wylene
2229 River Plaza Dr. No. 146
Sacramento, Ca 95833

Abstract: This article provides an overview of the potential exposure to civil liability faced by any individual, company, or government agency for their use, or lack, of information systems security. Included is an analysis of liability arising from claims of failure to adequately protect sensitive information in one's care, failure to prevent a system under one's control from being used to facilitate tortuous or criminal conduct, and liability arising from the provision of security products and services to others. This article is intended only as an examination of liability resulting from unauthorized access to an information system. Potential liability resulting from the use of a system by an authorized user, acting within their authorization, is beyond the scope of this article. The article organized by potential source of liability, each of which is prefaced by an illustrative, hypothetical fact pattern.

Keywords: liability, negligence, law, lawsuit, legal, civil, criminal, products liability, warranty, malpractice

The Curse of Service: Civil Liability for Computer Security Professionals

I. ABSTRACT:

This article provides an overview of the potential exposure to civil liability faced by any individual, company, or government agency for their use, or lack, of information systems security. Included is an analysis of liability arising from claims of failure to adequately protect sensitive information in one's care, failure to prevent a system under one's control from being used to facilitate tortuous or criminal conduct, and liability arising from the provision of security products and services to others. This article is intended only as an examination of liability resulting from unauthorized access to an information system. Potential liability resulting from the use of a system by an authorized user, acting within their authorization, is beyond the scope of this article. The article organized by potential source of liability, each of which is prefaced by an illustrative, hypothetical fact pattern.

II. INTRODUCTION:

One who gains unauthorized access to an information system (the archetypal "hacker"), or uses a system in excess of authorization they possess, is subject to criminal prosecution under a variety of state and federal laws. The wrongdoer is likewise responsible for compensating those injured by their acts. However, in practical terms, this is of little reassurance to the injured parties. Those responsible for security breaches are often impossible to identify, and if identified are rarely capable of paying for the damage they have caused.

Any information system relied upon by a business or government entity is vicariously relied upon by all of those who depend on the entity. Thus literally anyone who interacts with the entity is potentially harmed if the system is damaged or compromised. If one's failure to provide adequate security harms another, it hardly requires a great leap of imagination to predict that the other will look to him for compensation. While there have been very few suits of this kind as yet, the increasing dependence upon information systems, and the tendency of any injured party to seek the deepest pockets available, suggest that they may become common in the near future.

While this may suggest nearly infinite liability, such liability is limited, both by specific laws enacted to protect certain kinds of information, and by the contours of the traditional legal doctrines which make one party responsible for another's injury.

III. FAILURE TO PROTECT SENSITIVE INFORMATION IN ONE'S CARE:

Scenario: A major online retailer's customer database is compromised. Several hundred credit card numbers are stolen. The thieves make numerous purchases with the stolen cards, and vanish. The cards' issuing banks, who bear the brunt of the loss, now contend that the retailer's failure to adequately secure their information system is the cause of the loss, and have filed suit.

Many companies and government agencies are custodians of information the disclosure or modification of which could cause injury to others. Unless legislation has been enacted specifically requiring the protection of the type information in question, the custodian's

liability will be measured under the traditional legal concepts of tort and contract.

In the past, most disputes over faulty computer systems have arisen between parties who have had prior dealings with one another, typically the provider of the faulty system and it's buyer. As a result, the allocation of responsibility for the resulting loss has been controlled by the express or implied contract between the parties. However, as the above hypothetical scenario suggests, the growing dominance of the information system as a way of doing business increasingly allows a system failure to injure those who have had no direct contact with the system’s operator. No legal fiction will create a contract between the banks and the retailer.

In such a case, the injured party may bring a civil lawsuit alleging negligence. While the law of negligence varies somewhat from state to state, the fundamental concepts are fairly uniform. The defendant in such a lawsuit is only responsible for the other’s injury if he or she was legally required to use reasonable care to avoid the harm that occurred, and failed to exercise such care, causing the injury.

This legal requirement is known as a duty, and the critical question in a lawsuit alleging inadequate computer security will be whether the court will impose a duty upon an information custodian to prevent the unauthorized disclosure or modification of information in his or her care. The court will typically not impose a duty if the harm that occurred was not a foreseeable result of the defendant’s acts. However, in the hypothetical given, harm to the issuing banks is a highly foreseeable result of the retailer’s failure to provide reliable computer security.

Once it has been established that the injury was foreseeable, the decision to impose a duty becomes a policy choice. Who, in the court's opinion, should be held responsible for the injury? The court generally grounds this decision on it's view of how best to prevent future injury, and the consequences to the greater community of imposing a potentially onerous duty to prevent this kind of injury.

These policy factors seem to weigh in favor of imposing a duty of reasonable care upon the information custodian. Only the custodian is in a position to prevent this harm from recurring, and requiring the custodian to provide reliable security is not unduly onerous, in view of the existence of means of protecting against all but the most determined attacks.

One factor which may weigh against the imposition of a duty is the so-called "economic loss rule". Under this rule the defendant is not liable for purely economic damage (as opposed to personal injury or property damage) caused to another by his negligent acts. In other words, he does not have a duty to avoid causing such a loss. This rule was an attempt by early, more conservative courts to limit potential liability that was perceived as discouraging business growth. The rule, as a categorical denial of liability, is the subject of increasing academic and judicial criticism, and is giving way, in many jurisdictions, to a more balanced policy decision, which weighs the many social concerns. However, it is still the law in some states.

The "economic loss rule" presents other complications in terms of information security. The line between economic loss and property damage is at best vague. Whether to characterize damage to the value of

information, caused by it's modification or disclosure as property damage, or merely economic harm, presents a complicated question on which the courts have differed.

While no identified court case has addressed the issue, it appears likely that a court doing so today would impose a duty upon the custodian. Once a duty has been imposed, it would require the custodian to use reasonable care to prevent the unauthorized disclosure or modification of the sensitive information under his control. Whether he has done so will in a particular case be a question of fact, decided by a jury in most states and the federal courts.

The traditional measure of reasonable care balances the likelihood and gravity of the potential injury, with the burden on the defendant to prevent the injury. Obviously the more high profile the custodian, and the more sensitive the information, the greater the measures that will be required. Custom in the industry is always evidence of reasonable care, but is never conclusive. Additionally, the importance of responding to security breaches when they happen, and plugging holes as they are located can not be overstated. A failure to respond to a prior similar security breach practically begs a jury to find the defendant liable.

If the custodian is a government agency, different rules may apply. Under the Federal Tort Claims Act, agencies of the federal government are generally liable to the same extent as a private person in similar circumstances. State government agencies may or may not be liable for their negligence, depending on the rules of that particular state. In many cases, however, specific statutes, rather than the general doctrine of negligence, will set forth the scope of a governmental custodian's responsibility.

Under the Privacy Act, each federal agency must "establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality" of records containing personal information regarding any individual. The act allows any individual injured by an agency's "intentional or willful" failure to comply. While this standard prevents an agency from being liable for mere negligence, it is possible that an agency exhibiting a complete disregard for technical safeguards will be held liable for a resulting disclosure or modification.

Other types of information in government custody are given greater protection. The Internal Revenue Code provides that tax return information shall not be disclosed except in certain limited circumstances. The code provides for a civil action against the United States for an intentional or negligent disclosure to an unauthorized person. While the vast majority of suits under this provision concern voluntary, but unauthorized disclosure, there is no theoretical or practical reason that it can not apply to negligent failure to protect the tax return information.

Federal law requires any educational institution receiving federal funds, either directly or through student loans, to refrain from any "policy or practice" of releasing student information, except as permitted by statute. While the penalty for violation is usually the loss of federal funds, courts have held that the unauthorized release of information is, in some cases, actionable by the injured student as a civil rights violation. While perhaps unlikely to succeed, a plaintiff might claim that failure to use adequate measures to protect such information creates a practice of releasing student records in violation

of federal law, which in turn violates his civil rights. This may become a genuine issue, as school computers of various sorts are virtual magnets for outside attackers.

Private entities are also specifically required to protect certain kinds of information in their care from unauthorized modification or disclosure. Under the Fair Credit Reporting Act, "credit reporting agencies" are required to maintain accurate consumer credit information, and are prohibited from disclosing that information, except for specified purposes. The act provides for a civil lawsuit by any consumer injured by an agency's willful or negligent failure to ensure the accuracy and confidentiality of information regarding them.

State law typically regulates the disclosure of medical information regarding any person. While the extent and nature of the protection this information is given varies, and not every state allows a civil suit by the injured patient, the majority of states permit one whose medical history or status is wrongly disclosed to sue the party responsible. This liability extends to negligent, as well as intentional disclosures. *Estate of Behringer v. The Medical Center at Princeton*, an instructive New Jersey case (concerning administrative, rather then technical safeguards), notes that "it is the easy accessibility to the [information] and the lack of any meaningful medical center policy or procedure to limit access that causes the breach to occur...it is incumbent on the medical center, as the custodian of the charts to take such reasonable measures as are necessary to insure that confidentiality. Failure to take such steps is negligence". Such reasoning will easily extend to issues of technical computer security.

Several other kinds of information (insurance claims, video rentals, etc.) are accorded varying levels of protection under federal and state laws. Even if a civil cause of action is not explicitly granted, the injured party may still have remedy in a claim of negligence. The existence of a law specifically protecting the information will, in many cases, operate to establish a legal duty, and set the standard of care.

IV. FAILURE TO PREVENT A SYSTEM UNDER ONE'S CONTROL FROM BEING USED TO FACILITATE HARMFUL CONDUCT:

Scenario: An ex-employee of a mid-size wholesaler discovers that his old user ID and password have not been deleted. Impersonating an authorized user of the wholesaler's system, he gains access to the system of one of the wholesaler's customers, and proceeds to cause extensive damage. He is arrested and convicted, but is unable to compensate the customer. The customer sues the wholesaler, claiming that their negligence has resulted in a substantial loss.

Computers are not merely tools for information storage, they are also an important means of communication. Business partners often allows their systems to interact at a high level of trust. A breach of one party's system puts the other's system at risk. Additionally, in a number of situations, individuals are directly dependent upon computer systems run by others. Computers operate heavy machinery and are increasingly involved in medical care. A security breach could be literally life threatening.

In a case such as the hypothetical, a contract between the parties may expressly provide for the allocation of responsibility. If the

agreement does not expressly address the issue, the injured part may still sue for breach of contract, under the theory that the other's failure to take reasonable steps to prevent this from happening is a breach of the obligation to act in good faith, which implied by law in every contract.

Even if the attackers do not cause damage to any system, they may still create liability to third parties, by incurring costs which the system operator must pay. The United States District Courts and the Federal Communications Commission have held the operators of telephone systems responsible for the payment of charges for unauthorized long distance made by "hackers".

Even if there is no relationship of trust, liability may still exist for damage caused. Corporate and government information systems often have resources beyond those of any individual wrongdoer. A breach of one entity's system may give the "hacker" an enhanced ability to commit further bad acts ranging from defamation to denial of service attacks on other systems. The legal remedy of the injured party, if any, will be dependent on the type of injury suffered.

In a situation where one entity's system is used, illicitly, to directly cause property damage or economic loss to another, as in a denial of service attack, the potential remedy will be in a suit for negligence. Whether the court will impose a legal duty will depend greatly upon the facts of the case, but generally seems unlikely. Not only will the injury have to be foreseeable, but the court might decide, as a matter of policy, not to create liability to everybody potentially harmed by the unauthorized use of a system's resources. Obviously creating such a broad class of potential plaintiffs poses a serious impediment to business growth. There will also be issues of contributory negligence. If the injured party's own security was inadequate, and contributed to their injury, this will serve to offset or eliminate the damages that the defendant is responsible for.

If the claim is defamation or invasion of privacy, as where an unauthorized person uses a company website to make public untrue or embarrassing information about another, the plaintiff is out of luck. The federal Communications Decency Act of 1996 provides in part that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". This law serves to shield the operator of any computer system with multiple users from liability for the speech of any other party, authorized or unauthorized, using it's system.

Claims of copyright infringement, as might arise if an unauthorized person were to use a system to store or distribute another's intellectual property, are also barred. The federal Digital Millennium Copyright Act, enacted in late-1998, protects a "service provider" from liability for the infringing activities of any user, whether or not authorized, unless the operator had actual knowledge that the activity was occurring. This is similar to the protections given by the courts before the act went into effect. Note that in order for the "service provider" to take advantage of the protections offered by the Act, he or she must publicly identify a point of contact for claims of infringement.

The Act is primarily concerned with the activities of legitimate users of companies whose business is the provision of Internet services. Whether it will apply in the context of an unwilling "service provider" is an open question. Even if it does not, the system operator is

unlikely to be liable, under the reasoning of the pre-Act federal court decisions. As the United States District Court noted in *Religious Technology Center v. Netcom On-Line Communication Services, Inc.,* "although copyright is a strict liability statute, there should still be some element of volition...which is lacking where a defendant's system is merely used to create a copy by a third party". Obviously this is all the more true where the infringing user is unauthorized. It should be noted that failure to promptly stop the activity once discovered may lead to liability, regardless of whether the Act applies.

V. WARRANTY AND PRODUCTS LIABILITY:

Scenario: An Internet Service Provider purchases a new, off-the-shelf, server software package. Some time after installation, the server is compromised by "hackers", who vandalize the websites of several of the provider's clients. The clients thereafter cease to do business with the provider. The provider sues the seller and manufacturer of the package, claiming that its security features were defective, causing a substantial loss of revenue.

Concerns over Y2k have made liability for software failures a hot button issue. While there have been few court cases as yet, the subject has received extensive academic treatment. However, few commentators have addressed the specific issue of liability for defective computer security products.

This issue is exclusively one of state law, and will vary. However, as this is an emerging area of law within the relatively standardized field of commercial transactions, a fairly uniform body of law is likely to develop.

The standard by which liability will be determined will initially depend whether the software is characterized as a product or as a service. While nearly all courts consider software purchased as a part of a transaction involving a tangible item, such as software pre-loaded onto a personal computer, as a product, the treatment of software purchased independently has varied widely. The emerging majority view considers package software as a product, while viewing custom software as the services of the designer. Liability in cases where the software is considered a service will be considered in part VI.

The nature of the liability will also depend on the sort of damage done by the defective software product. If the security breach causes personal injury or property damage, the remedy may be in a suit for Products Liability or negligence. However, in the ordinary commercial setting, where the damage is merely "economic harm", such as lost profits, the remedy will be controlled by the express and implied warranties accompanying the software.

Products Liability is a legal doctrine which holds the manufacturer or seller of a product which is defective in design or manufacture responsible for the damage caused by the product without regard to negligence. If the product is actually defective, they are liable regardless of their level of care. A product is considered defective if it departs from its intended design in any way, has an unreasonably dangerous design, or fails to warn of the risks associated with the product. Any product may be the target of a failure to warn claim, and a departure from intended design is possible in the context of information security, as where a programmer leaves himself a "backdoor" during development and then fails to remove it either

accidentally or intentionally. However, most claims in the area of computer security are likely to concern allegations of defectively poor design.

A product's design is defectively poor if it fails to minimize foreseeable risks, rendering the product unreasonably dangerous. This determination bears a resemblance to the basic negligence inquiry. The likelihood and seriousness of the potential harm is weighed against the burden to prevent the harm by adopting an alternative design or warning of the danger. Practice in the industry weighs very heavily in determining whether a particular alternative design was reasonable. Likewise, the expectations of the consumers of the product is a major factor in determining reasonableness of design.

In the hypothetical given, the court would likely hear expert testimony concerning the design of the product, the nature of the security breach, and any possible design choices that could have prevented the breach. Whether the product was defective will generally be a question for the jury. Whether or not the buyer was himself negligent, as by faulty installation of the software, or in some way assumed the risk of the product's failure, as by modifying the software, will also be a question of fact. If either of these is found to be the case, his recover will be reduced or eliminated accordingly.

Whether or not a court will allow products liability as a remedy for a information security software failure is an open question. As noted above, Products Liability is generally limited to circumstances involving non-economic loss. As discussed above, this "economic loss rule" is not without it's detractors. However, in the context of Products Liability, unlike negligence, the rule is still widely accepted.

The difference in treatment is related to the differing reasons for the rule’s adoption. The rule was originally applied to negligence claims as a matter of policy, to avoid potentially "excessive" liability. By contrast, the rule was applied to Products Liability claims not as a matter of social policy, but as a matter of legal theory, to allow effect to be given to the product's warranties.

In *East River S.S. Corp. v. Transamerica Delavel*, a Supreme Court decision followed in many states, the court reasoned that if the defective product damages only itself, or causes merely "economic damage", then the buyer has only been deprived of the benefit he expected to receive from his purchase. This sort of loss is traditionally dealt with as a breach of the parties’ contract or warranty. However if the product causes harm to a person or to other property, the loss is not of the sort typically contemplated when purchasing products, and can thus be given an independent remedy such as Products Liability.

The “economic loss rule” raises several issues when applied to computer security products. Separating property damage from economic loss may be difficult. While some losses, such as the lost profits in the hypothetical, are clearly categorized as economic, others, such as damage to other software and data, or the damage to a company's reputation that can result from a breach, are not so easily pigeonholed.

Even if the loss is characterized as property damage, the recovery may still be limited to the warranty. While there have been no court cases regarding computer security products, several courts addressing physical security devices, such as alarms, have refused to allow a suit

for Products Liability when the device failed. The courts reason that in the case of security devices, damage to other property is exactly what the parties had in mind when the product was purchased, and thus the buyer has only lost the benefit that he expected to receive from his purchase, which is best dealt with by reference to the device's warranty.

A suit for negligence in the hypothetical case runs into the same problems. The existence of a contract or warranty contemplating the sort of loss that occurred would effect a claim of negligence in much the same way as a Products Liability claim.

From the above, it appears that a court facing the hypothetical case would only permit the injured customer to sue for a breach of warranty, rather Products Liability or negligence. As will become apparent, the difference is often more academic that practical. The major real difference is the greater willingness of the courts to enforce a disclaimer of warranty. Disclaimers of negligence and Products Liability claims, dealing as they do with personal injury and property damage, are often not enforced, on grounds of public policy.

The nature and effect of the warranties for a computer security product will probably be governed by the Uniform Commercial Code (UCC). While the courts have differed over whether the UCC, which is primarily concerned with the sale of goods, is applicable in the context of package software, where the buyer is actually obtaining a limited license to intellectual property, the majority view finds the UCC applicable, either directly or by analogy.

Courts have also differed over who may be sued for a breach of warranty. A warranty is a contract, and like any contract it is only binding upon the parties to it. In the case of package software, the buyer and the designer have often had no dealings. While most modern courts allow a suit against the manufacturer directly, regardless, some courts require the buyer to sue the retailer from who he purchased the product, the retailer to sue the wholesaler, and so on. From the designer's point of view however, the question is academic. Liability is going to catch up with them one way or another.

Under the UCC, there are two kinds of warranties, express and implied. An express warranty is created by the seller’s actual communications with the buyer. If the seller or designer claims that the product provides security against a particular sort of attack, this is an express warranty. In such a case a successful attack of this kind would be a breach of warranty. It should be noted that an allegation that the seller has breached an express warranty is often accompanied by an accusation of fraud. If credited, this accusation serves to avoid any disclaimers of warranty, and increases the damages the buyer may receive.

An implied warranty is automatically created by law whenever a product is sold. The implied warranty relevant here is the warranty of merchantability, which guarantees that the product is "fit" for use to which such products are normally put. If the product is unfit, by reason of design or manufacture, then the warranty is breached, and the seller is liable for all foreseeable damage sustained by the buyer.

A product is unfit if it does not conform to the buyer's reasonable expectations. If the product is similar in quality to the other products on the market it will normally not be found unfit. While this standard and the standard for "defectiveness" under Products

Liability are not identical, the same result is reached in most cases. A product with a "defect" is likely to be "unfit", and vice versa. In the context of information security products, no buyer can reasonably expect perfect security. However, a buyer can reasonably expect the product to be free of obvious errors, loophole, and back doors.

Additionally, if the seller has reason to know that the buyer intends the product for a specific use, and is relying on his expertise to select the appropriate product (as where a novice buyer asks the retailer to help him select a security product), the software selected must be fit for that particular purpose.

Express and implied warranties may be limited or disclaimed if done in large print or other conspicuous manner. The legal doctrine of unconscionability places limits on the extent to which liability may be disclaimed. If the parties did not actually bargain for the disclaimer (such as a disclaimer in located in a “shrink-wrap” software license), and the disclaimer is unreasonably favorable to the seller, it will probably not be enforced. Note that the courts have had no problem enforcing a common limitation of warranty, which limits the injured party’s recovery to the purchase price of the product.

VI. INFORMATION SYSTEMS PROFESSIONAL MALPRACTICE

Scenario: A large investment brokerage hires a reputable computer security consultant to improve the security of its system, specifically voicing concerns over denial of service attacks. Shortly after the consultant has completed the job, the system is subjected to a denial of service attack, leaving it inoperable for 72 hours. The brokerage is unable to trade effectively during this period, losing a substantial amount of money, and several clients. They have sued the consultant under several legal theories.

Y2k concerns have also prompted a flood of academic speculation concerning the liability of a software designer when his work is characterized as the provision of a service. Again, little of the commentary focuses specifically on computer security.

As noted above, designers of custom software are generally held to be providing a service, as the "predominant thrust" of the transaction is not the provision of a finished good, but of their professional services. If the software fails to function effectively, the buyer's best potential remedies will be in a suit for professional malpractice, ordinary negligence, or breach of contract.

From the injured party's prospective, the professional malpractice theory is the most attractive. The defendant will be held to a higher standard of care, and will be liable for all damages, even if they are purely economic losses.

Members of certain skilled professions are held to a higher standard of care, in professional matters, than the “reasonable person” standard of ordinary negligence. While the “reasonable person” in a negligence case is required to use all of the skills possessed by the average person, he is not required to possess any special skills. A professional, on the other hand, is required to possess all of the skills and knowledge of a reputable member of that profession practicing in the same locality. He must also use reasonable diligence and his best professional judgement in applying those skills.

The few courts addressing the issue are divided over whether computer professionals should be held to this heightened standard of care. In *Diversified Graphics, Ltd. v. Groves*, a federal appeals court concluded that Ernst & Whinney (now Ernst & Young), an accounting firm, had an obligation to use professional care when it assisted a small business in its purchase of computer system. The court reasoned that the client's reliance upon Ernst & Whinney's superior knowledge of information systems was implicit in the consulting agreement between the parties, sufficing to hold them to the higher professional standard.

This conclusion is contrary to the vast majority of court decisions both prior and since. These decisions have refused to recognize information services providers as "professionals" in this context. The courts have noted that the professionals upon whom the higher standard is imposed (doctors, attorneys, accountants, etc.) are typically subject to minimum requirements of training and professional ethics, enforced by a system of licensure and discipline. Information systems professionals are not subject to any such requirements at this time.

The *Diversified* case is regarded as wrongly decided because the court in that case simply found that the client had relied on Ernst & Whinney, and that a professional duty was thus created. The *Diversified* court never questioned the reasonableness of the client’s reliance. Other courts addressing the issue have concluded that absent universally applicable professional standards and licensure, such reliance is not reasonable, and the technician should not be held to a professional level of care.

Consequently, information systems professionals are unlikely to be subject to professional malpractice actions anytime in the near future. Computer security professionals are even less likely to be held to the professional standard of care. As noted above, this heightened standard is justified by the reasonable reliance placed by clients on the professional's superior skills and ethics. While the majority of computer security professionals are well trained, competent, and ethical, the field, perhaps more so than computer consulting in general, has it's share of "ex-hackers", private investigators, and others offering consulting services who may or may not live up to professional standards. It does not appear likely that any court addressing the issue would find that the profession was suitable, at present, for the imposition of the professional standard of care.

The fact that the court will not impose a high standard of care does not mean that no care is required. Those courts refusing hold information systems professionals to the higher standard of care have been quick to point out that a failure to use the “reasonable care” exercised by an ordinary person still qualifies as negligence, and is actionable. If the action is for ordinary negligence, one must contend with the economic loss rule. As there is a typically a contract between the parties, courts generally limit negligence actions to situations not contemplated when the parties made their contract, i.e. personal injury and property damage, just as they do in actions alleging Products Liability.

The most common remedy available to the injured client will be a suit for breach of contract. As a general rule, failure to exercise reasonable care in performing one’s contractual obligations constitutes a breach of the contract, and of the implied promise to act in good faith. This will entitle the injured client to compensation for his disappointed expectations, and for all reasonably foreseeable harm he

suffers as a consequence. The contract may, however, modify these general principles and limit the consultant’s liability. The nature Of the client's recovery will thus depend a great deal on the terms of the parties’ contract.

VII. FUTURE OUTLOOK

The legal field surrounding liability for "cybertorts" in general, and computer security failures in particular, is poised on the brink of a massive explosion. Computer crime will become more lucrative as more value is entrusted to information systems. Significant segments of emerging economies may turn to various forms of "hacking" to compensate for industrial and technological deficiencies. As the Internet brings more individual consumers into contact with large information systems, the sheer number of potentially injured parties increases. A company or agency whose security is breached could be faced with any number of lawsuits, or worse, a large class action suit. Even if no damage is done outside of the company itself, the shareholders may still attempt hold the officers liable if their carelessness contributed to the loss. This potential for massive liability has not gone unnoticed. At least three major insurance companies now offer "hacker insurance" policies, covering losses sustained by the insured company both directly, and as the result of third party liability.

The major legal change on the horizon comes in the form of the Uniform Computer Information Transactions Act (UCITA). Proposed by The National Conference of Commissioners on Uniform State Laws, an advisory group, UCITA will have to be approved by a state's legislature before becoming law in that state. While some of the group’s previous efforts, such as the UCC, have been widely accepted, many have received a less favorable response. As the final draft of UCITA has yet to be submitted to any state, it remains to be seen whether UCITA will become the law anywhere.

If adopted, UCITA would bridge the gap between product and service. UCITA generally considers "computer information", whether package or custom, as a product, subject to the general warranties, remedies, and limitations currently applicable to goods under the UCC. However, if the developer is paid for his time, rather than for the finished product, it will be presumed that he guarantees only that he used reasonable care in his work, and does not guarantee the software’s fitness. The Act makes no provision for a heightened standard of care. Products Liability remains available to compensate for personal injury and property damage, although UCITA provides no guidance as to what constitutes property. Additionally, while UCITA makes "shrink-wrap" licenses generally enforceable, a disclaimer of warranty or limitation of remedy made in such a manner is as unlikely to be enforced under UCITA as under current law.

VIII. CONCLUSION

While no conduct is a guaranteed shield against liability, an entity which maintains a meaningful security policy, consistently implemented and enforced, responds quickly to identified problems, and keeps accurate and complete records, should be able successfully defend its actions. The standard which pervades tort law, and this article, is one of reasonable care. This is not an unattainable ideal or a complex standard. It is, for the most part, simple and straightforward. It does not take a lawyer to define reasonable care. The reader of this paper is likely better qualified than the author to describe what is reasonable

in the computer security field. When in doubt, think long-term, and envision justifying an action or policy in a courtroom.