M E M O R A N D U M

TO: Members Of Computer
Security Response Center

FROM: Geoffrey S. Stewart
David Sylvester

DATE: December __, 1989

SUBJECT: Potential Liabilities Of Computer Search Response Centers Arising From Notification To Publishers And Users Of Security Deficiencies In Software

I. Introduction

The main computer network used by the United States research community is a loosely organized web of over 500 autonomous unclassified national, regional and local interconnected networks. This computer network is called the Internet and over the past 20 years has come to play an integral role in the research community, providing a means to send electronic mail, transfer files and access data bases and super computers. The Internet now connects over 60,000 computers nationwide and overseas and plans exist to have an enhanced and upgraded version of the Internet serve as a "super highway" that would run faster, reach further and be more accessible than any other computer network system in the world.

In recent years this "super highway" has been used to spread computer viruses to many of its host computers. Two recent incidents clearly illustrate the potential damage: The "Christmas Tree Virus" of 1987 and the "Internet Virus" of 1989. The "Christmas Tree Virus" attacked IBM mainframes through an international network. It used electronic mail services to send copies of itself to network users. It displayed the holiday message on the receivers screen and then mailed itself to others. The virus spread like an electronic chain letter through many kinds of communication links, including satellite and ocean cables, reportedly affecting computers in over 130 countries. This virus caused both the denial of services and system shutdowns.

The "Internet Virus" produced in 1988, was the first to use several security weaknesses to promulgate autonomously over a network period. It was designed to attack Sun-3 and VAX computer systems that use systems software based on Berkeley Software Distribution UNIX. It incorporated four primary attack methods to access thousands of computers connected by network communications lines. Two attack methods relied on implementation errors in network utility programs, a third method gained system access by guessing passwords, and the last method exploited local network security assumptions to propagate within the local networks. Because of the independent and flexible nature of the attack strategy, the "Internet Virus" was able to affect many systems within a short period.

With the importance of the Internet and possible successors, the introduction of these viruses, and the apparent ease of their introductions, have increased concern for the security of the host computers on the Internet and the potential damage to those computers that could result from security holes. The rapid growth of Internet, and particularly its international expansion, has increased the vulnerability of host computers to penetration and the damages that could result from software holes. In view of these concerns, some Internet users are developing computer security response centers ("CSRC") to establish emergency and preventative measures. Given the decentralized management of the Internet, the CSRCs are viewed by many users of the Internet as the best vehicle for addressing their security concerns.

Although software publishers generally include security features in their programs, gaps or holes in these security features are often found. A CSRC is to assist in the protection of the computers on the Internet by operating as clearinghouse to receive reports of these software weaknesses and to report those weaknesses to software publishers and, if necessary, to software users to have them corrected.

The implementation of a CSRC raises a number of legal issues, including the following:

1. What is a CSRC's liability if -- having undertaken to assist in the protection of Internet -- it fails to do so and someone is harmed as a result?

2. What is a CSRC's liability if it reports a software bug to a publisher or to users and the bug does not, in fact, exist?

3. Row should legal concerns shape a CSRC's planned collection and notification procedures, if at all?

II. Conclusion

Most of the liabilities facing a CSRC are in the nature of torts, that is, the civil liabilities the law imposes for intentional, reckless or negligent conduct that causes injury to another. As a general matter tort liability is imposed when (1) a person has a duty to another to act or refrain from acting in a certain way, (2) the person breaches that duty and (3) the other person is harmed as a result. The extent of the liability differs depending on the type of tort in question, the kind of harm suffered, the nature of the duty involved and the quantum of wrongful act involved (e.g., intentional misconduct, negligence, recklessness or malicious conduct). Likewise, the defenses available to an alleged tortfeasor varies depending on these same circumstances. In general, though, the concept from which much tort law analysis proceeds is that of foreseeability, namely, whether it is foreseeable to a reasonable person whether his or her conduct will result in harm to someone else. If such harm is reasonably foreseeable, tort liability often attaches on the theory that a person who can reasonably foresee harm to another from his or her actions is in the best position to prevent the harm from happening in the first place. Thus, if that person causes the harm to come about, he or she should compensate the victim.

Even though it is volunteering a useful service, a CSRC may face liability to software publishers, users or others if it performs its work negligently. It is also possible, although highly unlikely, that a CSRC could be exposed to liabilities for defamation or copyright or patent infringement.

A CSRC may be able to minimize its legal exposure by following a number of procedures set forth in section III .8 below. These measures would include carefully defining for publishers and users the services the CSRC will and will not provide, carefully and repeatedly articulating that the CSRC's purpose is to supplement, not supplant, the efforts of others in protecting the security of the Internet, adopting policies and procedures to assure that reasonable care is taken in receiving, processing and disseminating reports, and following certain procedures in preparation of its reports.

III. Discussion

Software publishers and a CSRC have a duty of care to those who use their products or rely on their services. This duty requires publishers and a CSRC to take reasonable actions to prevent conditions that can lead to harm and to correct those conditions where possible.

A. Liabilities Of Software Publishers

1. Tort Liability

Software publishers may face substantial liabilities if they fail to respond to a notice from a CSRC of a software defect. A publisher's failure to correct a shortcoming could result in substantial liability under tort law, or under the publisher's license agreements with users, if an unauthorized user exploited the defect to access a computer and then stole, destroyed or altered files.

The law of torts has been generally collected by the highly respected American Law Institute in the Restatement (Second) of Torts (1965) (the "Restatement of Torts"). Section 302A of the Restatement of Torts provides that:

> An act or an omission may be negligent if the actor realizes or should realize that it involves an unreasonable risk of harm to another through the negligent or reckless conduct of the other or a third person.

Likewise, Restatement of Torts Section 302 B states:

> An act or omission may be negligent if the actor realizes or should realize that it involves an unreasonable risk of harm to another through the conduct of the other or a third person which is intended to cause harm, even though such conduct is criminal.

A reasonable person is required to know the habits and propensities of human beings in circumstances he or she has intentionally created or should realize would be created by his or her conduct. Restatement of Torts §302 A commented.[1]

----

1 Restatement of Torts § 302 A comment and states in part:

> If the actor's conduct has created or continued a situation which is harmless if left to itself but is capable of being

An essential element of negligent conduct is "foreseeability." If the defendant could not reasonably foresee any injury as a result of his or her acts, or if his or her conduct was reasonable in light of what he or she could anticipate, there is no negligence and no liability. Boles v. La Quinta Motor Inns, 680 F.2d 1077 (5th Cir. 1982). Put another way, the basis of negligence is conduct that creates an unreasonable risk of injury to others; to be liable, the defendant must have known or should have known of the reasonable risk created. Rodrigue v. Dixilyn Corp., 620 F.2d 537 (5th Cir. 1980), cert. denied, 449 U.S. 1113 (1981).

A. Potential Liabilities Of A CSRC

1. Liabilities To Publishers And Users

Even though a CSRC will have no contractual relationship with software publishers or Internet users, it still would have obligations to them to perform its work with reasonable care. If a CSRC were negligent in its evaluation or reporting of software deficiencies, it could be found liable to a user who was injured by a CSRC's failure to report or misreporting of a software hole to a publisher or to users generally.

As a general matter, tort law imposes no duty on a bystander who refuses to go to the assistance of another. See W.

----

made dangerous to others by some subsequent action of a human being or animal or the subsequent operation of a natural force, the actor's negligence depends upon whether he as a reasonable man should recognize such action or operation as probable.

Page Keeton, Prosser and Keeton on Torts 3735 (5th ed. 1984); Jackson v. City of Joliet, 715 F.2d 1200 (7th Cir. 1983), cert. denied, 465 U.S. 1049 (1984) (there is no legal duty imposed upon any person to affirmatively act to rescue a stranger). Once a person undertakes to assist another, however, the law requires that the samaritan act with reasonable care. The theory behind this distinction is that, by doing nothing, the samaritan has not exacerbated the victim's plight; by incompetently intervening, on the other hand, the samaritan, has simply made matters worse. See, e.g., City of Joliet, 715 F.2d at 1202-03 ("there is no general common-law duty to rescue a stranger in distress even if the rescue can be accomplished at no cost to the rescuer.... But if you do begin to rescue someone, you must complete the rescue in nonnegligent fashion even though you had no duty of rescue in the first place.")

Each CSRC intends to evaluate and report software problems to publishers so that the problems can be remedied in time to prevent harm to Internet users. Although there are several ways of looking at it, software publishers may be viewed as the direct beneficiaries of a CSRC's work and Internet (and perhaps non-Internet) computer users as the indirect -- although equally important -- beneficiaries of the CSRC. In either event, a CSRC's obligations are fundamentally the same, although there are technical differences in how that liability is determined.

(a) Liability to Publishers

Section 323 of the Restatement of Torts provides that:[2]

> One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of the other's person or things, is subject to liability to the other for physical harm resulting from his failure to exercise reasonable care to perform his undertaking, if
>
> (a) his failure to exercise such care increases the risk of such harm, or
>
> (b) the harm is suffered because of the other's reliance upon the undertaking.

It is worthwhile to pick this language apart. On its face, Section 323 resolves a number of threshold issues. First, it makes no distinction between those who are paid for their help and classic "good samaritans" like a CSRC.[3] Second, the section makes

----

2 Most cases that deal with this doctrine adhere to the Restatement of Torts version. Those that do not (See Indian Towing Co. v. United States, infra note 6) adhere, at least, to subsection (b) of Section 323, which imposes liability upon a samaritan who induces others to rely upon his help.

3 Numerous judicial decisions explain that bodies such as a CSRC that are organized to promote health, safety, security or efficiency fall within the scope of Section 323. In Peterson v. Multnomah County School District No. 1, 64 Or. App. 81, 668 P.2d 385 (1983), defendant Oregon School Activities Association (OSAA), was a private non-profit corporation that made recommendations regarding competitive sports among member schools. OSAA was sued by a football player who was paralyzed by a sport-related neck injury who alleged OSAA was negligent in not recommending certain safety measures. OSAA argued that it did not assume this duty and, even if it had, it could not be held liable for failing to take an act. The court rejected this argument and found OSAA could be found liable because it had voluntarily undertaken to make and disseminate safety recommendations. OSAA thereby assumed a duty to the football player that it could breach by a "negligent failure to perform, as well as by negligent performance."

Similarly, in Arnstein v. Manufacturing Chemists Association, Inc., 414 F. Supp. 12 (E.D. Pa. 1976), a worker died clear that it covers situations like a CSRC's, where a Samaritan "render(s] services to another which he should recognize as necessary for the protection of the other's person or things." Restatement of Torts §323 4 Section 323 finally imposes on a

----

allegedly due to long-term exposure to vinyl chloride. The court held that the defendant, a nonprofit trade association, could be sued for failure to disclose the dangers of vinyl chloride. Cf. Canipe v. National Loss Control Service Corp., 566 F. Supp. 521 (N.D. Miss. 1983), aff'd in part, rev'd in part 736 F.2d 1055 (5th Cir. '1984) (private safety inspectors not liable to injured employee of client because its actions did not increase the risk of harm and employer did not rely on the inspectors' recommendations); Ricci v. Quality Bakers of America Co-op Inc., 556 F. Supp. 716 (D.Del. 1983) (independent inspector not liable to injured employee of client where its omission did not increase the risk of harm).

Because of the variety of protective functions federal, state and local governments perform, they frequently are sued for failure to warn or negligent performance in giving warnings. In the case of Indian Towing Co. v. United States, 350 U.s. 61 (1955), for example, the Coast Guard was sued for failing to maintain a lighthouse, causing a shipwreck. Although the court found the Coast Guard was under no independent duty to build and maintain lighthouses, once the Coast Guard did provide lighthouse U service -- and thus induced ships to rely upon it -- it was required to act with reasonable care to make certain that the light was kept in good working order or to warn sailors if the light was not functioning. Id. at 69. The Court stated "it is hornbook tort law that one who undertakes to warn the public of danger and thereby induces reliance must perform his 'good Samaritan' task in a careful manner." Id. at 64-65.

In Adams v'. State, 555 P.2d 235 (Alaska 1976), the court held that the state assumed a duty when it inspected for fire hazards. Thus, when the state failed to give a hotel a formal notification of fire hazards it found, it breached that duty. The court recognized the rule that "one who assumes to act, even though gratuitously, may thereby become subject to the duty of acting carefully." Id. at 240.

4 There is a distinction between a samaritan's failure to initiate a promised service and his negligent performance of that service. Restatement of Torts Section 323 leaves open the question of "whether a mere promise, without in any way entering upon performance, is an undertaking sufficient to make the promisor liable under the rule stated in this Section." Id. com

samaritan a general duty "to exercise reasonable care to perform his undertaking." Id.5

Other questions are not answered on the face of the statute. Instead, it has been up to courts to resolve issues such as (i) the breadth of a samaritan's duty, (ii) what actions constitute reliance and (iii) the scope of a samaritan's exposure to damages.

(i) Scope of a Samaritan's duty. Courts have held that the scope of a Samaritan's duty is coextensive with the scope of his or her undertaking. In Patentas v. United States, 687 F.2d 707 (3rd Cir. 1982), for example, sailors injured by a shipboard

----

ment d. Although the distinction is one that still persists, it has become blurred in situations where the plaintiff's reliance upon the defendant's promise has resulted in harm to him. Id.

5 Section 323(a) also imposes liability upon a good Samaritan who increases the risk of harm to a victim in the course of attempting to help. It is unlikely that this element of the rule would apply here. In Patentas v. United States, 687 F.2d 707, 717 (3rd Cir. 1982), for example, the court rejected plaintiff 's claim that the Coast Guard had increased the risk of harm to sailors by failing to discover safety risks. The court said that in order to increase the risk of harm, there must be some "physical change to the environment[5] or "some other material alteration of circumstances." Id. In other words, in order to increase the risk of harm to another through negligence, the actor must commit a positive act, not omit to act because an omission does not increase the risk. Although failure to discover a defect may well constitute negligence, "the language of the Restatement assumes that the injuries result in fact from the defendant's negligent performance of his or her undertaking before it reaches the issue of increased risk." Id. See Feuge v. Texaco Inc, 634 F. Supp. 213, 217 (E.D. Tex. 1986) (Shipowner not liable to employee for negligence for voluntary offer of assistance in unloading the ship when his subsequent withdrawal of 'assistance in no way worsened plaintiff's position). See Radosevic v. Virginia Intermont College, 651 F. Supp. 1037, 1040 (W.D. Va. 1987) (maintenance company not liable to student injured by unsecured roof hatch because it never touched the roof hatch).

fire sued the Coast Guard for negligently inspecting the safety of their vessel. The court applied the "good samaritan" rule of the Restatement of Torts. Thus, the court explained that the "scope of a good samaritan's duty is measured by the scope of his or her undertaking." Id. at 716.6 In this case, a CSRC assumes the duty of evaluating and reporting software defects to publishers and, if necessary, computer users on a predetermined schedule. The CSRC therefore could be found liable for delaying unnecessarily in reporting a defect, in reporting the defect inaccurately or in reporting the defect to the wrong publisher.

(ii) What actions constitute reliance. Restatement of Torts Section 323(b) requires that the harm suffered by an injured party is harm suffered because of the injured party's reliance upon the samaritan's undertaking. In Patentas, supra, 'the court held that proof of reliance included proof that a victim had actual knowledge of the samaritan's undertaking. Id. at 717. A lack of knowledge prevented liability for the obvious reason that a victim cannot rely upon something he or she does not know. Id.

---

6 This analysis has been accepted by other courts. See Blessing v. United States, 447 F. Supp. 1160 (E.D. Pa. 1978) (where an inspector is not under an otherwise enforceable legal or contractual duty to inspect an employer's premises, the employee can recover for a negligently-performed inspection only where the inspector has physically undertaken to inspect the specific instrumentality causing the subsequent injury or the entire physical plant of which the specific instrumentality is part) See Brady v. Hopper, 570 F. Supp. 1333 (D. Colo. 1983), aff 'd, 751 F.2d 329 (10th Cir. 1984) (psychiatrist not liable for negligent diagnosis for injury to plaintiff due to former patient's attempt to assassinate the President where the psychiatrist's duty to protect third persons did not extend to plaintiff since it was not foreseeable that the patient would inflict the harm that he did.)

Thus, a software publisher that sued a CSRC for negligence would be required to demonstrate that it knew of the CSRC's work. See infra at 14-15 for a more detailed discussion of reliance.

(iii) Scope of a samaritan's exposure to damages. Restatement of Torts Section 323 imposes liability upon samaritans only for "physical harm." This has been found to include both personal injury and damage to property. See Neal v. Berland, 646 F.2d°1178 (6th Cir. 1981); S.A. Empresa De Viacao Aerea Rio Grandense v. United States, 692 F.2d 1205, rev'd, 467 U.S. 797, on remand, 744 F.2d 1387 (9th Cir. 1984); General Public Utilities Corp. v. United States, 551 F. Supp. 521 (E.D. Pa. 1982), rev'd on other grounds, 745 F.2d 239 (3rd Sir. 1984). See also Indian Towing Co., supra note 6 (applying common law rule, and not the Restatement, Supreme Court implies that government can 'be liable for damage to property).

As a practical matter, it is difficult to resolve the question as to what foreseeable physical harm would result from a CSRC's negligence in reporting a software defect. Even assuming that alterations to 'stored electronic data, modification of software or incapacitation of computer systems is "physical" harm, damages generally cannot be assessed unless they are foreseeable. Given the limitless range of mischief an intruder can cause, there would be good arguments in many cases that particular types of injury were beyond a CSRC's foreseeability.

There is, finally, a separate question whether a Samaritan can be found liable for consequential damages that result from its negligence. Although there is little authority on point, it would appear that a CSRC probably would not be responsible for consequential damages in the event it was negligent. Restatement of Torts Section 323 itself, of course, makes no mention of such liability and there are sound policy reasons not to saddle a samaritan with open-ended liability for consequential damages. The little direct authority there is also suggests that Restatement of Torts Section 323 does not extend to consequential damages. In Jones & Laughlin Steel Corp. v. Johns Manville Sales Corp., 626 F.2d 280, 287-88 (3rd Cir. 1980), the court stated that "[n]either the rule [Restatement of Torts Section 323) nor its accompanying commentary and illustrations extends liability for negligence to encompass economic losses."

(b) Liability To Users

Similar principles govern the CSRC's liabilities to computer users. Restatement of Torts Section 324A, which governs a samaritan's duties to an indirect beneficiary, states:

> One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of a third person or his things, is subject to liability to the third person for physical harm resulting from his failure to exercise reasonable care to perform his undertaking, if
>
> (a) his failure to exercise reasonable care increases the risk of such harm, or
>
> (b) he has undertaken to perform a duty owed by the other to the third person, or
>
> (c) the harm is suffered because of reliance of the other or the third person upon the undertaking.

Section 324A is similar to Section 323 on its face, and not surprisingly, questions of scope, duty, standard of care and damages are largely the same. See Patentas , supra.

Two issues, though, are particularly important in reviewing a CSRC's liability to indirect beneficiaries such as computer users. The first is precise definition of the class of indirect beneficiaries a CSRC would owe a duty to. The second concerns the degree of reliance an indirect beneficiary must demonstrate.

(i) Definition of indirect beneficiaries. The range of' potential indirect beneficiaries of a CSRC's work is limitless, extending not only to computer users, but also perhaps to people who rely on the users for work, services or assistance. Restatement of Torts Section 324A adopts a pragmatic, although very general, approach to defining these beneficiaries. The section extends a samaritan's duty to any foreseeable beneficiary of the specific undertaking that the good samaritan has voluntarily assumed. See Patentas, 687 F.2d at 716 (crew members foreseeable beneficiaries of Coast Guard inspection; inspection was undertaken to determine the safety of continued cargo discharging and it was foreseeable that, if continued discharging was unsafe, appellants would be injured). Cf. Gunnells v. United States, 514 F. Supp. 754, 759 (S.D. W.Vaᵒ 1981) (government not be liable for flood damage to plaintiffs' homes where the inspections were specifically undertaken to benefit coal miners, and

homeowners were not foreseeable beneficiaries of the inspections).

(ii) Degree of reliance. Restatement of Torts Section 324A also requires specific reliance by the indirect beneficiary on the work of the samaritan. Under Restatement of Torts Section 324A(c) a samaritan can be liable "if the harm is suffered because of reliance of the other or the third person upon the undertaking." See Lemar v. United States, 580 F. Supp. 37, 40 (W.D. Tenn. 1984) (federal government not liable for a state agency's negligent vaccination where plaintiff never received a federal government pamphlet which allegedly contained false information). Thus, if an injured party cannot demonstrate that he or she knew specifically of a CSRC and its work, he or she cannot recover damages from the CSRC.

In addition to knowledge, a plaintiff also must prove that the samaritan's undertaking "induced [him] to forgo other remedies or precautions against (the] risk." Patentas, 687 F.2d at 717 (citing comment e of Restatement of Torts Section 324A). The rationale of this requirement is that, where the reliance has induced one to forgo other remedies, the "harm results from the negligence as fully as if the actor had created the risk." See Yoder Co. v. Liberty Mutual Ins. Co., 284 N.W.2d 810, 812 (Mich. App. 1979) (insurer liable to a worker for negligent inspection of workplace because employer had no organized safety program and had relied on the insurer's inspection in lieu of an internal safety program).

3. Other Potential Liability Issues

There are, finally, a group of residual liability issues. First, there' are questions whether a CSRC could face liability for wrongfully reporting a software defect that did not, in fact, exist. Second, a CSRC may be faced with copyright, patent or trade secret issues depending on how it went about reporting particular software defects.

(a) Reporting Of Nonexistent Software Defects

A CSRC may at some point report to a publisher a defect in software that is not a defect at all. Possibly, the report to the publisher could harm the career of employees who worked on the program. Likewise, if the report were made public (which would occur if the publisher insisted there was no defect) the publisher's own business might be harmed.

(i) Possible Liabilities To Publisher's Employees

(A) Intentional interference with employment. Tort law prohibits any person from intentionally interfering in the contracts or beneficial business relationships of another. Restatement of Torts § 766. Claims of tortious interference, however, would require the injured employee to demonstrate that a CSRC "intentionally and improperly" interfered with the his or her employment contract or his or her relations with his or her employer. This would require proof that a CSRC made its report to the publisher with the intention of adversely affecting the programmer who would be charged with the mistake. As a practical U matter, proof of such a claim would be difficult, since a CSRC would rarely know the identity of programmers, has no motive to interfere with any programmer's livelihood and could not foresee the particular harm. See Restatement of Torts § 766C comment a. In any event, mere negligence is insufficient to result in liability for tortious interference in the affairs of another. See Restatement of Torts § 766C.

(B) Defamation. A publisher's employee also could argue that a CSRC slandered or libeled him or her in submitting a false report of a software defect. "A communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him." Restatement of Torts § 559. As a general matter, the tort of defamation requires (a) a false and defamatory statement about someone, (b) unprivileged publication of that statement to a third party,[7] (c) negligence or intentional conduct by the person making the statement and (d) harm. Restatement of Torts § 558. "A communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him." Restatement of Torts § 559.

---

7 The term "publication" in the law of defamation refers simply to the making of a statement, whether orally or in writing.

A CSRC’s exposure to claims of defamation would be severely narrowed by the fact that a CSRC’s reports would not identify anyone by name. However, it still is possible, to defame an individual without specifically naming him or her. Defamation may occur if from the description or circumstances, the identity of such person can be reasonably be or is actually inferred by some third party. Gnapinsky v. Goldyn, 23 N.J. 243, 128 A.2d 697 (N.J: 1957). In other words, if a CSRC’s incorrect report of a software defect was specific enough to permit a publisher to identify the programmer who caused the supposed defect, the report could be defamatory.[8]

(ii) Possible Liabilities To Software Publishers

(A) Defamation. Publicizing a software defect that in fact does not exist, may also raise the issue whether a CSRC defamed the publisher. Under Restatement of Torts Sections 561 and 562, companies, like individuals, are capable of being defamed. Restatement of Torts Section 561 provides that:

----

8 Even if it made this mistake, a CSRC might have strong arguments that its publication of ’the report was privileged Or that the report was not derogatory to any individual. A CSRC’s work is something favored by public policy and may receive some defense in this context. In any event, a CSRC can take steps to minimize its liability for defamation simply by prefacing its reports with language stating that it has been told of a "possible" or "potential" software defect.

One who publishes a defamatory matter concerning a corporation is subject to liability to it

(a) if the corporation is one for profit, and the matter tends to prejudice it in the conduct of its business or to deter others from dealing with it, or

(b) if, although not for profit, it depends upon financial support from the public, and the matter tends to interfere with its activities by prejudicing it in public estimation.

Restatement of Torts Section 562 provides that:

One who publishes defamatory matter concerning a partnership or an unincorporated association is subject to liability to it as if it were a corporation.

As a general matter, the tort of defamation against a corporation, partnership or association requires the same elements as a defamation against an individual. See Restatement of Torts § 558. A corporation is not defamed by communications defamatory to its officers, agents or stockholders unless they also reflect discredit upon the method by which the corporation conducts its business. Restatement of Torts § 561 comment b.

°The most likely factual circumstances in which a defamation claim could be made by a publisher would be those where a CSRC and the publisher disagree whether a software bug is, in fact, a defect or whether the bug is serious or not. In that case, the CSRC may well inform users of the report to the possible detriment of the publisher's business. Although it will be much more difficult, if not impossible, for a CSRC to identify a software bug without identifying the publisher, the CSRC can limit its liability by its choice of language in the report. See infra § III.B.3.

(B) Copyright and patent law. It is possible that a software publisher could claim that a CSRC's report of a software defect was so detailed as to violate copyright, patent or trade secret protection. Once again, however, this is a liability the CSRC can control by the level of specificity it chooses to include in its report.

Generally, copyright protection exists in ''original work's of authorship fixed in any tangible medium of expression ... from which they can be perceived, reproduced, or otherwise communicated either directly or with the aid of a machine or device." 17 U.S.C. § 102(a) (1977). Computer software may be copyrighted. Johnson Controls, Inc. v. Phoenix Control Systems, Inc., No. 87-15088 (9th Cir. October 3, 1989) (LEXIS, Genfed Library, Courts file) ("Nonliteral components of computer software may 'be protected by copyright where they constitute expression, rather than ideas"). Subject to certain exceptions discussed below, the owner of a copyright has the exclusive right to reproduce the copyrighted work- in copies and to distribute copies of the copyrighted work to the public by sale or transfer of ownership, or by rental, lease, or lending. 17 U.S.C. § 106.~ 9

----

9 Anyone who violates the exclusive rights of the copyright owner is an infringer of the copyright. 17 U.S.C. § 501(a) (1977). In order to prove that a copyright has been infringed, a party need only show that it owns the copyright and that the party, against whom the action is being brought, copied the protected material. Nimmer, Nimmer on Copyright § 13.01 (1989).

An infringer of a copyright is liable for, at the election of the copyright owner, for either: (l) the copyright owner's actual damages and any additional profits of the infringer; or (2) statutory damages in an amount to be determined by the court of

Even copyrighted material, however, is subject to the doctrine of "fair use," which allows a holder of the privilege to use copyrighted material in a reasonable manner without the consent of the copyright owner.[10] As a general matter, classroom instruction, literary criticism and similar non-commercial uses of copyrighted work is considered fair use. Given the use to which

----

not less than $500, or more than $20,000 or, in the event of a willful infringement, an amount not more than $100,000. In the event the infringer is found not to be aware and had no reason to believe that its acts constituted an infringement, a court may reduce statutory damages to a sum not less than $200. 17 U.S.C. § 504 (1977).

10 The doctrine of fair use provides:

> ''Notwithstanding the provisions of Section 106, the fair use of a copyrighted work, including such use by reproduction in copies or phono records or by any other means specified by that section, for purposes such as criticism, comment, news reporting[1] teaching (including multiple copies for classroom : use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include --
>
> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
>
> (2) the nature of the copyrighted work;
>
> (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
>
> (4) the effect of the use upon the potential market for or value of the copyrighted work."

17 U.S.C. § 107 (1977). The factors enumerated in Section 107 are not meant to be exclusive, and each case must be decided on its own facts. Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 560 (1985).

the CSRC would put this information, there are strong arguments that its report is protected by the fair use doctrine.

Software may also be patented. Diamond v. Diehr, 450 U.S. 175 (1980). A person infringes a patent in the event such person makes, uses, or sells such patented invention without authority. 35 U.S.c. § 271(a) (1977). It is unlikely, however, that the CSRC's publication of patented software would be a "making" or a "use" of the software, since the CSRC will not be producing any operational software or causing the software to function.[11]

B. Measures A CSRC Can Take To Limit Its Liability

There are several measures a CSRC can follow to narrow its exposure to liability. We would recommend that the organizing documents of a CSRC and any publicizing materials contain the following protections:

1. Definition of specific duties.

Since a CSRC cannot be held liable unless a plaintiff demonstrates he or she knew of the CSRC's work, the CSRC can limit

---

Il Finally, software may also be protected under trade secret law. As a general matter, software's trade secret protection may be compromised if it is copyrighted, since the public copyright filing at least partially destroys the secrecy of the software. Moreover, the law of trade secrets has been increasingly preempted by federal law. See Bonito Boats, Inc. v. Thunder Craft Boats, ___ U.S. ___, 109 S.Ct. 971, 103 L.Ed. 2d 118 (1989). Once again, moreover, the CSRC would be liable for disclosing trade secrets only if its report were made to the public and were so detailed as to disclose the substance of the software.

its exposure by clearly declaring what it is and is not purporting to do. At the time a CSRC is announced, the CSRC should make clear that (a) its sole purpose is to evaluate and report software defects, (b) it will not be in the business of independently uncovering software defects, (c) it does not purport to displace the obligations ’software publishers have to computer users, (d) its efforts should be viewed as mere supplements to the efforts of Internet users and beneficiaries to protect Internet, (e) it encourages users to purchase software maintenance from publishers and to remain in contact with publishers and (f) it is undertaking these duties for the purpose of assisting publishers, users and other beneficiaries in protecting the viability of the Internet network and not attempting to protect the security of any particular computer system or user.

2. Reasonable care.

A CSRC will face several distinct obligations of reasonable care. First, a CSRC is required to make itself available to receive reports of software defects. Second, a CSRC is responsible for accurately recording and reporting those defects. Third, a C$RC is obligated to accurately rank the seriousness of the defects. Fourth, a CSRC is required to report those defects to the proper publishers or, failing that, to users groups. Finally, a CSRC is obliged to perform this work in a timely manner.

The duties a CSRC must meet are those of reasonable care, not perfection. A CSRC accordingly can minimize its liability if it (a) adopts policies requiring notification of security defects to be confirmed in writing to eliminate misunderstandings, such writing to be filed in a file to be maintained for a reasonable period of time, (b) adopting procedures that eliminate or reduce premature disclosure of internal communications, (c) adopting procedures that eliminate or reduce premature disclosure of communications to third parties, (d) adopting procedures for double-checking the reports it sends to publishers or users to reduce the possibility of errors, (e) requires publishers to confirm receipt of the reports, (f) have questions of seriousness (particularly determinations that a defect is not serious) reviewed by a panel of experts to reduce mistakes, (g) adopting written procedures requiring a CSRC to respond to reports within reasonable time frames and (h) widely disseminate a detailed description of its policies on notifying publishers, users and the public of software defects. Given the deference that a court is likely to give to a group with a CSRCs technical expertise, these measures should materially limit the CSRC's legal exposure.

3. <u>Language of reports</u>

A CSRC finally can avoid most copyright, defamation, patent and trade secret issues by its choice of language in its reports. All descriptions of proprietary materials should be in narrative form only. No proprietary information should be disclosed in a way that violates the copyright, trade secret, patent or other proprietary rights of another. For example, if a CSRC obtains possession of source code, the source code should not be disclosed without the permission of the owner. Descriptions of defects should contain the minimum amount of information necessary to describe and pinpoint the problem.

We would recommend that in soliciting reports of software defects from users, a CSRC should choose value-neutral words to describe what it is seeking. We would recommend that a CSRC define the defects it is looking for as "possible software deficiencies" or "potential security issues." It is unlikely that a CSRC could be held liable for internally reporting a software anomaly that is expressly labelled as only a possible flaw. Similarly, in reporting these defects to software publishers, a CSRC could narrow its potential liability considerably by characterizing its report as a "request for further information" or as a "preliminary inquiry." Particularly if a publisher is given the opportunity to respond to a CSRC's inquiry -- which we understand is a procedure a CSRC itself favors -- a CSRC's possible liability is very much reduced.

As explained above, it is unlikely that a CSRC will report the defect in such detail to violate a copyright or patent. Even if it did, however, it is unlikely they would be liable. To further protect itself, a CSRC should take steps to assure that no republication of the reported defect occurs except to the publisher; in that case, there would be no actionable infringement. Likewise, if a CSRC is required to report the defect to users generally, it can shield itself from liability by avoiding detailed descriptions of the software codes in question and by characterizing the defect as a possible or potential one and directing users to contact the publisher directly.