backups, then the entire connection could be disabled if the fibre path were to be backhoe'd up and killed. This has happened in many locations around the world. Diversified path services are available from many communications vendors to guarantee that there is more than one physical path to/from a specific location. Some telecommunications carriers even have agreements with competitive carriers to offer not only diversified physical path services, but also diversified carriers so that no commonality of components exists in the two or more paths to a site. While this may seem extreme, in many cases it is essential to ensure network up-time and reduce corporate risk in the case of a network outage.

Reduction of network risk sometimes is as simple as not using the network for extremely critical applications. There is nothing wrong with this approach and sometimes it is the only way in which to solve a network risk problem. I do not think anyone would fault the network designer of a nuclear reactor control system if he/she felt that direct rod control of the reactor was a more sound technical solution than communicating over a network to a rod-control system that was three routers away! While an extreme example, it serves the point that network corporate risk is sometimes reduced by eliminating the network dependency.

As networks become more integral to the operations of applications and systems, the need to configure and maintain network integrity and reduce risk of using the technologies involved in networking is becoming a critical aspect of security management. While this article has pointed out some specific examples and deficiencies of network use and reduction of risk, there is a host of other risk reduction efforts and technologies that need to be used for a safe and robust network environment. Take a hard look at how the network is being used and perform the simple test question of "if it failed, how bad could it be for the company". If the answer is REALLY BAD or DEAD IN THE WATER, you have a network risk management problem that needs to be promptly addressed.

Computer Viruses — Legal Options

Bernard P. Zajac, Jr.

Computer viruses are still a hot topic for network and computer security professionals. Nearly every computer conference has a session on computer viruses, their detection, and prevention, but never, the recourses one has when they are the victim of a computer virus.

When you are a victim of a virus, you have a tangible loss. You could be out of pocket by several thousand dollars in both software and time; time, both in personnel, and down time. But is this loss recoupable?

One software manufacturer, when asked what recourse did someone have if they found a virus in his software, answered, "You, as a user have a recourse, you just sue them (the software manufacturer)." Interesting, but can you?

Legal remedies

Unfortunately, there is no case law in the United States concerning computer viruses. There is one case (**United States v. Morris**), but that case dealt with a computer worm on a network, not a personal computer, so the question of what recourse does someone have if they are the victim of a computer virus was posed to a number of attorneys.

Kirk Tabbey, head of the Computer Crime Task Force and Assistant Prosecuting Attorney at the Jackson County Prosecutor's Office, Jackson, Michigan said, "You'll always have a criminal case if you can find the person who did it (created the virus) because a virus is a malicious act."

He went on to note that inserting a virus problem is, in itself a malicious act, and therefore a crime. However, this action is against an individual or individuals who created the virus, but what about the person who sold the software or the software manufacturer? Are they liable? If so, what damages are recoverable?

It seems damage recovery is possible, all be it not an easy task. James J. Ayres, a Chicago attorney who is well versed in the legal aspects of shrink-wrapped software and a part-time faculty member of Chicago's DePaul University's College of Law, notes recovery can be approached in several

different ways: it could be a pure contract case between two or more parties; a Uniformed Commercial Code[1] (UCC) case between a buyer and a seller; or a tort liability case, within tort liability it could be either a straight tort or a negligent tort, depending on the facts of each case, each providing its own unique advantages and disadvantages; or finally, a cause of action under the Electronic Communications Privacy Act of 1986[2].

Shrink-wrap licenses

When buying software today, the software is sold in a shrink-wrapped box and in the box, the software disks are usually sealed inside an envelope and on the envelope is printed the contract. Also, generally printed on the envelope is wording stating that if you open the envelope, you agree to all the terms of the contract.

The contract generally states that the software is sold 'as is' and the manufacturer/publisher is not liable for any defects and/or damages to your machine — hence the term, 'Shrink-Wrapped Software'.

Tabbey points out that there are certain liabilities you are always responsible for, "If I create a law that says, if you want to come into my yard, I will not be liable for slips and falls. I will not be liable for anything that happens at all on the premises. That law will be overly broad — You cannot contract away liability."

Robert I. Brown, of the Southfield, Michigan firm Provier, Lichtenstein & Phillips, noted that enforceability of a 'shrink-wrap' contract may be changeable, "A lot depends on if the contract is actually negotiated or a 'boiler plate' agreement, if it was entered into without negotiations, and there are a limited number of dealers in the area, then the court may have the discretion to disregard liability limitations", said Brown.

Ayres stated 'shrink-wrap' contracts are unenforceable. He noted that the State of Illinois once passed a 'shrink wrap' law providing for the enforceability of 'shrink wrap' contracts, only to be repealed in less than four months after heavy pressure from software manufacturers' lobbyists and end users.

Ayres cited that fact that the United States 5th Circuit Court did uphold Louisiana's Distinct Court's opinion striking down Louisiana's 'Shrink Wrap' law as being preemptive by the United States Copyright Act[3].

"I think you would be hard pressed to argue that any software that comes in a box is a service", said Ayres. He also said that the courts have held that information can be a saleable product.

Warranties

If software is a product then, as Ayres and Brown noted, the Uniform Commercial Code has warranty provisions[4]. The argument that the manufacturer or publisher of software has a responsibility that the product is 'virus free' is true to a point.

Ayres said, "Did the publisher know or should have known" the software contained a virus? If so, then they are probably liable.

However, Tabbey said, "If they can come into court and prove that they are 'state-of-the-art' for virus checking, and they missed this one. It'd be pretty tough to hold then liable at all!"

As you can see, the victim of a virus has several options available to them: go after the person who sold the software; go after the manufacturer of the software; and, if the creator of the virus could be found, pursue criminal charges.

Criminally charging someone with a virus or a computer crime is now new. It has been done and there is a body of case law supporting it. However, civilly charging someone is new. The courts have yet to address this.

It seems there is civil recourse under the UCC and under the concept of tort liability. However, this will not be an easy case, since there is no case law to use a precedent. There has yet to be a computer virus case to be tried, civilly, in US federal court. A case of this type would be blazing new legal ground.

As viruses become more prevalent and virulent, apprehension of the perpetrator harder, victims, both corporations and individuals, will start looking to software manufacturers and vendors for two things: a higher level of assurance that the software is 'virus free' and recovery for damages, should they fall victim to a virus.

[1]USC 17 $1 et seq.

[2]USC 18 $2510.

[3]USC 17 $1 et seq.

[4]UCC $2-312.