

Downstream without a paddle

Developing an IT Security Strategy

Security extends beyond your corporate boundary

Developing a sound Information Technology security plan is as important to a company as a sound business plan. IT security strategy consists of eight components.

Security:

1. supports the mission
2. is part of sound management
3. is cost effective
4. requires explicit roles and responsibilities
5. extends beyond the corporate boundary
6. is comprehensive and integrated
7. must be periodically reviewed
8. is constrained by social factors.

In the fifth of eight articles, understanding the eight basic principles of IT security will assist you in developing your IT security strategy and ultimately protect your profits.

Responsibilities Extend Beyond the Organization

A common response to the above statement is “How can I be responsible for what happens outside of my control?” There are several areas where your company can face legal liability, such as: data generated for outside clients is compromised, your network is used as a launch-pad for other attacks, and customer or vendors lists are exposed. If your company does E-business and your client credit card numbers are compromised, your problems are just beginning.

Let’s use your network as an example. On Monday, after working at home over the weekend, an employee inadvertently brings in a zero-day Trojan on a disk. The Trojan quietly infects all of the other computers on your network. Your vendors have a link to your site to check inventory and the Trojan passes to them. On Friday, the Trojan executes—all infected machines begin to attack a web-site, a classic Distributed Denial of Service (DDoS). The affected site loses significant revenue and a forensic analysis traces the attack back to you and your vendors. Weeks later the kid who wrote the Trojan is arrested. The attorneys for the affected web-site have several options to recoup the loss—go after the child’s parents for peanuts, or go after you for failing to secure your electronic boundaries by proving lack of “due diligence”. This is known as “downstream liability.”

Data owners who make available data to external clients must provide a method to ensure confidentiality, keep the data available, and protect its integrity. If your external interface connects to another organization’s external interface, you must protect yourself against

“downstream” liability. If you fail to take precautions, and your compromised system impacts the downstream organization, you may be exposed to liability for damages unless you can demonstrate “due diligence.” Here are two good examples:

"In *AT&T v. Jiffy Lube International*, 4 CCH Computer Cases para. 46,845 (U.S. Dist. Ct. Md. 1993), a corporate telecommunications customer, Jiffy Lube International, was held liable for the long distance telephone charges run up by hackers. Using PCs, the hackers dialed into Jiffy Lube's PBX system, broke the password that granted access to long distance telephone service, and placed a flood of long distance calls, running up almost \$56,000 in charges. Jiffy Lube argued the long distance carrier, AT&T, should be responsible for the damage, but Jiffy Lube lost its argument. The court reasoned: Jiffy Lube 'created the vehicle and mechanism by which those long distance calls became possible. But for Jiffy Lube's installation of a telephone system with a remote access feature, the disputed calls could not have been made.' "

Benjamin Wright, *Business Law and Computer Security*, published 1993 by SANS Institute

"Verizon learned this the hard way in April 2003, when the Maine Public Utilities Commission rejected its request for relief from \$62,000 fees owed to local carriers after the SQL Slammer worm shut down its networks. Verizon had applied for a steep break on the fees owed under its service agreement, arguing the worm "was an event that was beyond its control" -- like a lightning strike. The commission's rejection rested in part on comments submitted by competitors WorldCom (now MCI) and AT&T. They handled Slammer with minimal interruption, they said, because they did a better job patching their systems than Verizon. Why should Verizon get a break?"

http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss326_art604,00.html

Verizon failed to show “due diligence” in protecting itself from loss, whereas AT&T and WorldCom were protected by demonstrating reasonable and prudent measures in proactively patching their systems.

Have a plan for containment, mitigation and notification in the event a breach of your security occurs. You must notify connected partners, vendors and customers if you think their systems or information has been compromised. California has passed a law, (California Database Protection Act of 2003) requiring notification if you “transact business with California residents no matter how small or minimal”. Of course this law has far reaching implications because it does not limit responsibility to physical location, but now spans electronic boundaries rather than geographic ones.

<http://images.jw.com/email/Tech120803.html>

There are measures you can take to protect your company from downstream liability—such as segmenting off your network to protect against “zero-day” attacks, and having well established policies and procedures to address quarantine zones, vendor connection standards and incident response and notification plans. Don’t be caught “downstream without a paddle”. In order to show due diligence, your IT security policies, procedures and practices must not be just on paper – they must be defensible and demonstrable; they must be routinely applied and in use, and you will have to prove “due diligence” in court –perhaps against a hostile prosecutor searching for a punitive award.