



New England's Environment

july/august 2004

vol. 10, issue 4

www.environews.com

Best Management Practices

Third Party Vendor Agreements: The Hidden Security Risks

by Carole Crawford,
The Saturn Partners, Inc.

Clients in the environmental arena have several security-oriented concerns in their everyday work, among them hazardous materials risks, OSHA regulations, and others. One area that should be closely examined is the area of Third Party Vendor Agreements.

First of all, when discussing security in the network environment, what is considered a Third Party Vendor? Well, from a security standpoint, a TPV could be any of the following:

- Software providers
- Hardware providers
- Internet service providers
- Telecommunications providers
- Electrical contractors
- HVAC contractors
- IT consulting firms

Depending on the nature of your business, there could be many others. One thing all TPVs have in common, however, is ACCESS – access to your network, computer rooms, electrical systems, electronic traffic, paper data, network maps, and all sorts of private and confidential/sensitive data.

One of the most interesting situations we experienced was during a security audit of a large New York law firm. We looked at security policies, disaster recovery plans, physical security around the network, and lastly, the Third Party Vendor Agreements. You would think that lawyers would be the toughest to please when it comes to contract language. Yet here are just a few examples of security holes we found in many contracts, some with the largest TPVs in the country. Some of them may even be buried in your own vendor contracts.

Liability Language Scenario 1: In several instances, agreements were discovered which placed all liability squarely on the client, and not the vendor, in case of disaster.

Liability Language Scenario 2: Also in several contracts, language was included holding the vendor harmless if data encountered in the scope of



work, whether physical or electronic, were compromised in any way.

Right-to-Substitute Skilled Labor:

This provision was found in contracts with a very large provider of installation or upgrades of software and hardware, and it can be very dangerous. The language allows for the vendor to “substitute without knowledge or permission” the personnel assigned to this work when “regular, full time company employees” in the technical positions “are not available.” In short order, this means that, on a moment’s notice, a contractor

can be swapped in that has not been background checked and who is not an employee of the vendor. Another risky part of this type of language in a contract is that, if the swapped-in technician does a good job on the surface but problems crop up later, you may have a hard time getting the vendor to adhere to contract if things malfunction later. This is due to the next item...

Substitute Labor/Not the Same Contract Liability:

In one contract, there was even a clause stating that if substitute technicians were used in an install or upgrade, that liability for work done on that system "would be considered on a case by case basis." This of course means that

a loophole in the language leaves the client (YOU) wide open for not only tampering, but systems failure and the potential loss of untold amounts of sensitive data, not to mention revenues. Incredibly, this contract had been signed by the client and had been in place for FIVE years!

The moral of the story is not to rip apart all your Third Party Vendor Agreements. But you may want to check with your attorneys and IT managers and be sure these agreements are scanned for liability language which can harm your network and business operations. Addendums can be written to attach to either new or existing agreements to make this adjustment less painful for both sides.

Whether the business is in chemicals, manufacturing, hazardous materials handling, law, health care, engineering or banking, it doesn't matter. What DOES matter is that you know what is IN those contracts gathering dust on the shelf and eliminate any areas of vulnerability. ■

Carole Crawford is president of The Saturn Partners, Inc., a Wisconsin-based firm that develops network and Internet security policies, delivers state-of-the-art design and implementation of network security architectures, and audits disaster recovery and business continuity plans.

For more information, contact Ms. Crawford at (262) 942-3626 or via e-mail at cacrawf@saturnpartners.com.

NETWORK SECURITY POLICIES: *The Reasons and the Results*

Whether it is having court-allowable evidence to prove fraud, theft or negligence, or simply bowing to regulatory pressure to have proper written network security policies in place, it is critical to have these policies not only in place but updated regularly.

Your policies are your blueprint in case of disaster; your path to follow when training employees in sensitive positions, your guidebook when it is time to roll out a new operating system or expand your enterprise or management team in any way.

Solid network security policies are not to be confused with any type of "office manual." Properly written policies should reflect all the state of the art technology in place at your organization and how to manage it, cope with it, protect it and react to disasters in the network and physical environment.

Most important is to realize that outside vendors can have access to private data and resources and that they too must have policies governing them in this process to protect you.

REASON 1: Expand information security budget and add more personnel.

RESULT: Policy development process shows management what is needed.

REASON 2: Establish top management communication path.

RESULT: Participation of management in the development process opens new channels.

REASON 3: Show definitive progress with minor investment.

RESULT: Only weeks are required to generate a credible policy document.

REASON 4: Establish information security effort credibility and visibility.

RESULT: A policy document should have a chief executive officer's signature on the cover page.

REASON 5: Shift worker attitudes and change perspectives.

RESULT: The support of all workers who interact with information systems is critical.

REASON 6: Harmonize and coordinate the activities of many workers.

RESULT: Consistent action is required if security is to be maintained.

REASON 7: Define the boundaries of permissible action.

RESULT: Workers will clearly understand the boundaries of designated responsibilities

REASON 8: Control security relevant events in advance.

RESULT: Increases chances that things will be done correctly the first time and reduces errors.

REASON 9: Exercise control by exception rather than micromanagement.

RESULT: Every action and decision does not need to be reviewed.

REASON 10: Overcome ambiguity that can lead to information overload.

RESULT: A policy document will focus workers' attention on the essentials.