

WHY DO DISTRIBUTORS NEED TO WORRY ABOUT ONLINE SECURITY?

BY STEVE EPNER AND DAVID LOOBY

It is the call dreaded by all business owners. Your network is down and it appears you have a virus. Hundreds of thoughts run through your mind in an instant. "What happened?"

"Where is the techno guru when I need him?" "Who is responsible for this?" How are we going to run this business without computers?" "Will my software vendor get this fixed right away, or will it take days and thousands of dollars?" "Why did we ever let everyone use e-mail in the first place?"

There are many things you can do (or could have done) to protect your organization. It is like backing up your data, no one does

it until they get badly burned. Then they become

fanatical and never miss again. It is hard to understand why anyone would want to go through the pain and cost of repair when prevention is so easy.

Disasters can happen to anyone - and they do. There are many things that can be done to prevent or minimize the impact of most problems. Before the answers will make sense, one needs a vocabulary to discuss the issues. So, we will start with the basics. There are four basic

concepts that a business executive needs to understand.

First, every network is vulnerable. Even the government has been attacked successfully. Their systems are challenged every day. Other companies like AOL, Microsoft and CNN are targets because they can make a hacker's reputation. Even if you are not as visible as the big boys, it does not take much to become a target. What if you upset one of your competitors and they mention to a son or daughter who is technically competent: "I wish I could shut XYZ down just for a day to show them they are not so great." The kids may take

*DISASTERS CAN HAPPEN TO
ANYONE -- AND THEY DO*

it as a challenge. All of the sudden, YOU are the target.

Second, there is no amount of money that can be spent to make you perfectly safe. Everyone learns this sooner or later. All operations need to recognize that there is risk in being connected to the rest of the world. We must continually evaluate the cost of protection against the risk of occurrence to be able to determine the appropriate action.

Third, no matter how much

we might want to disconnect from the online world, in most cases, it is not an option. As AT&T said a long time ago, "the Internet is not about technology, it is a new dial tone." This is how the next generation of business executives is communicating. Unless we are willing to cut ourselves off from customers, suppliers and other business partners, we must have a presence online.

Finally, it is up to us, the leaders of our companies to take charge of the problem. The technical people will implement the solutions, but top management must make the decisions. You may use internal

people, system vendors, consultants or a variety of other resources,

but all of them need direction. They will bring you alternatives and then wait for YOU to prioritize and accept spending recommendations as well as deciding how to change the way your people work online.

So, where should we start? Vulnerability is a concept we need to recognize, measure and understand. We must evaluate where we have exposure. Is our organization one that lives online? Do we get a significant number of orders or

communication from partners over the Internet? Can our employees dial or connect in from remote locations? The more we rely on the Internet and e-mail, the more vulnerable we are.

More secure companies have networks for internal activity separated from the Internet. Then there are a limited number of manageable points where the internal network touches the external one. By using available technology (secure connections) and limiting the number of transactions that can cross the boundary, it is possible to secure internal data while providing access to the rest of the world.

In most operations, the weakest link (greatest vulnerability) in security has nothing to do with technology. It is 100% human. People who write down their passwords and post them on their machines, choose easy to guess passwords, employees who leave confidential information on their desks, field people who tell others about their dial-in capabilities, these are the leaks that open the secure doors to more companies than any other vulnerability.

It is important to step back and truly understand where you are vulnerable and why. If you use e-mail, but do not have any training or policies for your staff to follow, that is a vulnerability for which there is no excuse. If you have a shared password for every user that is a vulnerability for which there is no excuse.

Part two of developing a

SOME OF THE MOST COMMON VULNERABILITIES WE FIND:

1. *Staff are allowed to open e-mail attachments without limitation*
2. *There is no effective anti-virus software in place*
3. *Virus signatures are not updated daily*
4. *Passwords are either not used, or implemented in such a way as to be ineffective*
5. *Individual applications are not password protected*
6. *Access to system capabilities is not protected*
7. *Web access is provided without restriction*
8. *Remote access telephone numbers are published*
9. *Built in application or system security capabilities are not utilized effectively*
10. *Encryption techniques are not used for data / information available over external networks*
11. *Disaster recovery and business continuity strategies and plans are not defined*
12. *Disaster recovery and business continuity initiatives have not been tested recently*
13. *Intrusion Detection Systems (IDS) are not implemented to monitor incoming external network traffic*
14. *Software license documentation is incomplete or nonexistent*
15. *Physical assets and / or computer rooms are not "hardened" against environmental hazards (fire, water, etc.) and unauthorized access*
16. *System, application and data backups are not consistently performed or stored offsite on a regular basis*
17. *Backup personnel are not identified or prepared to be available in case of an emergency*
18. *System and network audit / security logs are not implemented (or reviewed if available)*
19. *Systems, applications and operating systems are not upgraded in a timely manner (causing system and vendor support issues)*

security plan is evaluating the cost to repair versus to the risk and cost of an occurrence. This is a more difficult question. We must first try to estimate the cost of an occurrence. "What would the cost be to the company if we lost the use of our systems for a whole day?" Next ask: "What would be the cost if our trading partners quarantined our e-mail for fear we might send them a virus?" Finally, try to estimate the cost if we could no longer access the Internet or e-mail for any business purpose for some period of time.

Given the potential costs, it is important to try to estimate the risk. Risks come from many different places. Some of the primary risks to consider are:

1. Unhappy or terminated employees
2. Unfriendly or unethical competitors
3. "Public eye" (a high public profile that might generate an attack)
4. Family or other insiders that may have a grudge
5. Man made disasters (arson, theft, power failure, etc.)
6. Natural disaster (fire, floods, hurricanes / tornadoes, lightning strikes, etc.)

Once you have a list of risks, it is possible to begin to determine a potential that any of the risks might happen. If your operation is in "tornado alley", there is a greater likelihood of being hit with that type of storm than if you are in Alaska.

Putting the risks and their probabilities together with the cost to the firm if one should occur, it is possible to begin to establish a budget that is justified to protect your assets and operation. Then you are in a position to work with the "techno gurus" to develop a work plan and select the strategies that will work best in your environment.

Many of the things that you should do are obvious from the lists above. A few key items are listed below. In all cases, make your decisions to proceed based on an accurate understanding of the risks, probabilities and costs. There is no reason to just guess.

Please do not think that only big companies get hacked. Remember, you may just be unlucky and get targeted by

some kids for practice. You could become a target of convenience. As part of an assignment, one of our consultants drove into a client's parking lot, turned on his laptop and within seconds discovered they had a wireless network. Tony Munns, Manager of the Privacy and Security Group at Brown Smith Wallace points out it would only have taken a few minutes to be able to get access into their network. Some kid on the way home from high school could break in as a lark.

It really is not difficult to cause havoc just on a whim. The important thing is to expose the weaknesses in the network before there is trouble. Then you will be able to correct the situation and reduce the

EASY STEPS TO IMPROVE SECURITY TODAY

1. Establish policies, procedures and rules for purchasing, installing and maintaining software of all types.
2. Establish policies, procedures and rules for the use of e-mail and the Internet by all employees and contractors using company equipment and network facilities.
3. Establish policies, procedures and rules for the creation and use of passwords.
4. Establish policies, procedures and rules to be executed whenever there is employee turnover.
5. Implement good anti-virus software and update it nightly or more frequently.
6. Back up the system daily and keep copies in a safe place off site.
7. Begin to raise the awareness of the necessity of security with all employees.
8. Begin the process of evaluating your vulnerabilities, risks and costs so you can build a detail plan to improve the security of your network resources.

opportunity for random hackers. Tony likes to point out that we have methods of protecting information assets even if an organization wants or needs a wireless network. It is not difficult if you know what is vulnerable and how to protect it.

If a company is really concerned about how secure their networks are, a penetration lab is used to test all entry points into a system. This type of testing always requires written permission before we start. Our goal is to look at your situation as a hacker would see it. We think like and attempt to identify the weaknesses in your network as if we

wanted to get in. The big difference is that we will not cause any havoc once we do.

In one instance, our security expert was able to crack a sophisticated client's first password in 18 seconds. It took a day and a half to crack the root password. We could have been in even quicker if we had started with our Spanish word dictionary sooner. The client was a bit surprised, but is now able to correct the situation based on our very specific recommendations.

Larger clients and those that rely heavily on technology often begin their security analysis with a General Controls Review of all uses of technology. All aspects of their infrastructure are examined against "best practice" databases. That includes everything from firewall protection to passwords,

physical security of the servers, administrative controls, operational controls and backup and recovery plans.

The American Institute of Certified Public Accountants has established a more complex and complete procedure for service providers referred to as a SAS 70. It is meant to assure users of outsourced systems that proper controls are in place to secure information and provide accurate results.

Even if you do not need all

IN ONE INSTANCE, OUR SECURITY EXPERT WAS ABLE TO CRACK A SOPHISTICATED CLIENT'S FIRST PASSWORD IN 18 SECONDS.

aspects of an IT controls review, many improvements can be easily identified and made. For example, a solid back up procedure can be used to minimize the effect of hardware failure. This may be the most cost effective way for a mid-size company to react to specific technology threats.

Based on the complexity and scope, security and control reviews can take from several days to multiple months to complete. A project may be narrowly focused or it can include virtually every aspect of the way a company uses technology. The costs can run from under \$4,000 to whatever you want to spend.

Do not let cost be the deciding parameter of action or inaction. Considering the risk to the organization, security projects can be money well

spent. When the Sobig-F virus hit a Midwest company, they called us to see how fast we could be at their site.

We arrived and began to address the immediate issue of getting their servers up and running. It may have only taken several hours to accomplish the task, but during that time they were virtually out of business. The virus had really knocked them out.

Instead of waiting for something horrible to happen,

companies should take a more proactive approach to this situation. As business leaders become more aware of how easy it is to protect against common risks, resolution is becoming part of their normal IT planning process. Do not rely on luck that something won't happen to you.

The Brown Smith Wallace Consulting Group is a St. Louis based advisory firm. They are recognized experts in the world of distribution and are called upon by many of the largest national distribution associations to assist their members. From companies with IT budgets in the thousands of dollars to Fortune 500 giants, they have helped their clients implement specific programs to protect information assets and computing environments.