



Responding to a Security Crisis and Reducing Future Risk

By Mike Theriault
President & CEO B2B Computer Products LLC

Surprisingly- when it comes to security risk mitigation and safeguards - studies show even the largest organizations skip or don't complete steps. Then they face the same problems again. The good news is that whether your organization has 50 or 5,000 computers, the methods for responding to a security crisis and reducing future risk are simple.

For most organizations, the biggest threat to their security isn't outside hackers, rather it's internal users. And most of the problems internal users cause aren't intentional. So, protecting a company's data largely centers on protecting itself from employees and protecting employees from themselves.

What follows is a concise guide to addressing security crises now and preventing security crises in the future. Although the steps are generally sequential, the order will depend on how tightly regulated your industry is and the types of security risks you face.

6 Steps - Responding to a Security Crisis

The goal is a quick, but considered response. Gather the facts as quickly as you can and act as soon as you have enough information to respond correctly. Don't take any action until you can accurately define the problem (not necessarily the cause) and know its scope.

1. Review Your Compliance Documents

In tightly regulated industries, organizations must document their compliance with government mandated security standards. If this applies, be sure you can demonstrate compliance in order to avoid fines and regulatory action.

2. Identify an Incident Response Team

Hopefully, you have a computer security incident response team ready to go. If not, assemble a team that (in addition to IT) may include: attorneys, C-suite executives, public relations, and a representative from each of the business lines affected – including HR if the breach involves employees. No matter how small your organization, don't allow one person to handle the situation. Having a team will reduce the chances of an erratic response.

3. Assess the Damage

Determine who and what is/may be affected and the potential effect on your business. An external attack on your public website might not be a big deal if it's an informational site, but it can break your business if you're dependent on e-commerce. Also, an insider attack on the company's personnel database may have a different impact than a hacker's theft of a client database.

4. Notify Stakeholders

Who you tell and when you tell them can make a difference as to whether you're able to quickly find and fix the problem. If yours is a highly regulated industry, you'll need to call government officials immediately. If a crime may have been

313 S. Rohlwing Road
Addison, IL 60101
p 630.396.6300
tf 877.222.8857
f 630.396.6322
www.B2BComp.com

committed, law enforcement will be one of the first calls. If you are planning to bring in third-party consultants, such as security or computer forensic experts, bring them in as early as possible.

Most states have specific deadlines for informing customers and others who may be affected by the breach (up to 30 days for disclosure). This means you'll have time to get the situation under control before the information becomes public.

5. Identify the Cause and Minimize the Damage

Many severe security problems appear mild at first. In fact, your IT staff may have seen it as a nuisance and applied a routine fix. For example, many insider attacks look like minor glitches until someone notices unusual or suspicious behavior and the situation escalates. Initial signs may include an increase in overall traffic – especially an unusual amount of outbound activity and an increase in help desk requests. More overt signs include crashing websites and internal sites. In the extreme, nothing will work at all.

Unless the breach is actively hurting your business, don't begin remediation until you fully understand the cause and its potential impact. In some cases, you shouldn't touch anything until a forensics team has finished collecting evidence.

If the breach is affecting your business, you'll want to limit damage immediately by doing such things as unplugging servers and storage systems that are being infected or penetrated. Other measures may include disconnecting media devices – especially if you suspect a malicious code is running. Generally speaking, the faster you disconnect the equipment, the better your chances of saving your data. Once you've taken these basic steps, don't do anything else without the help of experts.

6. Document the Incident

Lack of documentation will not only make it difficult to rebuild your systems, it can also hurt your chances of successfully prosecuting an attacker. Throughout the assessment and remediation process, you should record everything, from how the incident was detected to what the members of the response team did.

If the attack came from outside the company and your security hardware and software is up to date, documentation will occur automatically through firewall log files, IDS/IPS/IDP systems, and other security information management tools. Your job will be much easier if the tools you have in place are sophisticated enough to record the intrusion; the ensuing infections or downloads; and the configuration changes that stopped the attack.

Documentation is one of the most overlooked and time-consuming aspects of a security incident. However, documentation is critical for many things such as rebuilding systems that have been temporarily modified to halt an incident.

6 Steps - Reducing Future Risk

Security for external threats relies heavily on automated systems. Whereas, security for internal threats relies heavily on employee education and user checks like two-factor authentication. You'll want to be sure that both areas are covered with comprehensive security hardware and software.

If yours is a heavily regulated industry and your security measures aren't in compliance, this will be your obvious first step. Otherwise, follow the sequence below.

1. Perform a Thorough Security Risk Analysis

A thorough security audit or risk analysis will tell you exactly where your deficiencies lie. There is no getting around this first step. To skip it would be like building a house on bare ground without a foundation.

Because a risk analysis is extremely complex and there is so much at stake, most companies will opt for an outside expert to perform it. However, the National Institute for Standards and Technology (NIST) publishes a set of recommendations that you can use as a baseline for information.

2. Develop a Crisis Plan

A good plan will outline the strategy for addressing the immediate crisis and safely recovering the system. The plan will also identify crisis response team members along with their responsibilities and identify the public spokesperson. Most importantly, it will also include steps for restoring customer relationships and rebuilding the brand.

3. Put Measures in Place to Detect and Prevent Attacks

The risk analysis will recommend security tools (both network and system-level defenses) for detecting and preventing future attacks. The tools will be specific to your company and your situation. Hopefully you already have a computer products channel partner that you trust to supply, install, and provide support for the security hardware and software you need (without trying to sell you what you don't need).

Some of the newer security tools are IDP (intrusion detection and prevention) systems, which are a combination of IDS (intrusion detection systems) and IPS (intrusion prevention systems). Because IDP systems protect and detect – they provide a system of checks and balances that neither IDS nor IPS can perform alone.

SIEM (security incident event management) systems are customizable hardware that correlates all security information into a single report – allowing users to resolve security issues quickly. While SIEM is costly - for many companies, especially those dependent on e-commerce, it's very cost effective.

Whether or not a security investment is cost-effective often comes down to proper implementation and post-sale support. A Harvard Business Review article concluded, "The companies that manage their IT investments successfully generate returns that are as much as 40 percent higher than those of their competitors."

4. Install Backups of Critical Data Systems

Assess your data back-up system. Look for any gaps. If your server crashes, you'll need to retrieve your company's backed-up data and put it onto a new server – you don't want the gaps to show up then. Once you're sure that you have a comprehensive data back-up system in place, regularly verify that it's working correctly.

5. Identify and Educate Everyone with Access to Network Data

Document everyone who has access to company data – name, job title, department, etc. Tell HR to update the information daily. Unfortunately, employees are usually the weakest links when it comes to security – this is especially true if employees are allowed to take company wireless devices off the premises.

Quoting Alan Rodger, a senior research analyst at the Butler Group, a BusinessWeek article noted, "Investment over the years has focused on security threats outside of the organization, but I believe companies now need to spend a lot more time looking at the threats from within."

The best way to ensure that employees are educated on security is by developing and distributing an Acceptable Use Policy and following up with training.

The Acceptable Use Policy

The policy should spell out acceptable behavior when using the network both on the premises and remotely. It should address both acceptable and non-acceptable use, and include (among other things) a strong password policy and rules governing Internet use, email, and social networking sites. A good way to determine what to include in the policy is to look at actual incidents that were especially flagrant and/or are recurring.

6. Continuously Test, Monitor, Adjust

Don't assume that everything is working well. Set up a regular schedule of testing, monitoring, and adjusting all security-related hardware and software. Keep up to date on security software advances and be diligent about downloading patches - code that fixes computer bugs and vulnerabilities in the system. Review your Crisis Plan regularly and revise your Acceptable Use Policy as new issues arise.

A 2003 study "The Economic Cost of Publicly Announced Information Security Breaches" concluded that, although there appeared to be no significant negative reaction when the security breach didn't involve confidential information, "We find a highly significant negative market reaction for information security breaches involving unauthorized access to confidential data," (e.g., the release of customer credit card numbers, bank account numbers, or medical records to unauthorized parties)

According to a recent survey conducted by the highly regarded Ponemon Institute, 19 percent of respondents ended their relationships with companies that reported security breaches, 58 percent said they lost trust; 59 percent said fear of identity theft was a major factor in brand trust diminishment; and 50 percent said notice of a data breach was a factor. If you follow the guidelines presented here, that won't scare you.

About B2B Computer Products

Award-winning B2B Computer Products LLC was identified by Inc. magazine as one of the fastest growing businesses of its type in the U.S. and by Crain's as one of the largest privately held companies in the Chicago metro area. B2B Computer is a single-source provider of products and manufacturer-certified services that include virtualization, VoIP systems, data deduplication, disaster recovery, SAN storage, server consolidation, energy-efficiency improvement, and testing environment implementation. B2B Computer's engineers can design, configure, install, and/or manage the products and systems they sell to their clients. As a national business-to-business reseller of computer hardware and software representing hundreds of manufacturers – B2B guarantees a best practice combination of competitively priced customized products and expert services. In addition to its Addison, Illinois headquarters and multiple distribution points, B2B Computer's offices are in Chicago; New York; Davenport, Iowa; Philadelphia; and San Francisco. To contact B2B Computer, call 1-877-222-8857 or visit www.B2BComp.com.