



Best Practices

Nov/December 2007

Computer Security is For Managers, Too

Companies need to have smart technicians who stay abreast of emerging digital threats and defenses, of course, but IT technicians shouldn't be calling the shots. General managers need to take the lead in building processes that will lessen the likelihood of a computer attack and mitigate damage. Most organizations already have some of these processes in place, but they rarely develop and manage them in a coherent, consistent way. Here are eight things that your company and managers should be working on to protect your digital assets.

1. Identify your company's digital assets and decide how much protection each deserves. You don't hire armed guards to prevent the occasional non-business use of copy machines, nor do you keep your company's cash in a filing cabinet. You protect each corporate resource in proportion to its value. The same principle applies to digital security.

To begin, you have to identify what your digital assets are (they're not always obvious). A team of managers from across the company should take an inventory of data and systems, assess how valuable each is to the company, and determine how much risk the company can absorb for each asset. That will tell you the level of protection each warrants. A bank, for instance, might assign the greatest amount of protection to the database that stores its customers' financial information. For a pharmaceutical company, it might be the research servers that hold data on promising drug compounds. Internal Web servers that contain general information about benefit programs probably warrant less protection.

The next step is to review the people, processes, and technologies that support those assets, including external suppliers and partners. You'll now have a blueprint that identifies precisely what your digital assets are, how much protection each deserves, and who's responsible for protecting them.

2. Define the appropriate use of IT resources. All companies have policies explaining the appropriate use of resources. For example, employees know what kinds of things can be charged to expense accounts. But use of company computer systems is often less clear. Managers need to ask, "Who should have remote access to the corporate network? What safeguards must be in place before employees can connect to the corporate network from a remote location?" These aren't technical questions; they're people and process questions that will help you identify the normal behaviors for particular jobs and what employees should and shouldn't be doing on their systems (such as sharing passwords).

Because even the best security policy will be ineffective if users and business partners ignore it, it's important for companies to explain their rationale for the limitations they place on computer usage.

3. Control access to IT systems. You don't allow just anyone off the street to wander in and use your company's fax machines or sit in on a strategy session. In a related vein, you need to bar some people from your computer systems while letting others in. You need systems that control who gets access to specific information, and you need a way to ensure critical communications aren't overheard.

Certain technologies—firewalls, authentication and authorization systems, and encryption—are used to control access, but they're only as good as the information that feeds them. They should be configured to reflect the choices made when you defined your company's digital assets and decided who has access to them. Of course, non-technical managers won't be doing the actual configuration work, but they will inform the process by asking questions like "How do we keep suppliers from accessing our payroll data?"

Just as companies keep an eye on their equipment and supplies by conducting scheduled audits and random spot checks, so should they monitor the use of their IT systems. Monitoring and intrusion-detection tools routinely log computer activity on company networks and highlight patterns of suspicious activity, changes in software, or patterns of communication and access. Some companies turn off activity-monitoring functions because they can slow network performance, but that's exceedingly shortsighted; the cost of not knowing enough about a security breach is much, much greater.

4. Insist on secure software. All well-run operations tell their materials suppliers exactly what specifications to meet. Similarly, companies should demand reasonable levels of security from software vendors. If your company develops software, make sure your developers are following secure coding and testing practices. Those who aren't may be costing your company large sums of money. One multinational database supplier estimates that releasing a major patch (a fix for a problem in already-deployed code) can cost the company \$1 million. But 80 percent of patches would be unnecessary if the company eliminated only one common type of coding error known as "buffer overflows."

5. Know exactly what software is running. It's shocking how many companies don't follow this rule. Keeping track of what software versions and fixes have been applied is as fundamental to digital security management as keeping an accurate inventory of physical assets is to plant management.

We're not saying that this is easy—software configurations change all the time. Maybe a program isn't running correctly, or an important customer demands a change, or a software vendor releases a new patch—the list can go on and on. But no matter the reason, it's crucial to document every modification. That way, if your computers are breached, you'll have current records to determine when and where the hacker struck. And, if you prosecute the intruder, you'll have digital forensics to establish a chain of evidence.

You should also ensure that you have a process that allows your IT personnel to make changes quickly. Procrastinating on updating patches gives hackers an easy in.

Keeping a close eye on changes in your configurations has an important side benefit: it allows you to make a real commitment to continuous improvement. As any experienced operations manager knows, it's impossible to identify and eradicate a problem's root cause if you don't have clear snapshots of your operations over time. The operational discipline involved in tracking configuration changes will pay off over the long run. As many companies discovered with quality management and industrial safety programs, perceptions of tradeoffs between security and productivity are often incorrect. Security concerns can drive operational simplifications that pay efficiency dividends as well.

6. Test and benchmark. Security professionals have a terrible habit of starting with a dramatic security audit—a staged attempt to defeat a company's defenses. But companies should save their money because the results of a "penetration test" are always the same: the bad guys can get in. What you really need to know is how easy was it? Which systems or programs were compromised or exposed? The answers to these questions depend on how good your operational plans are and how well you are executing them. Basically, when the bad guys get in—and you know they will—you want them to look around and see that there's not much of value to be had so that they'll leave in search of better prospects.

Relying too heavily on audits is problematic for the same reason that relying on inspections to improve quality is: discovering the problem after the fact doesn't keep it from happening in the future. But it is wise to hire external security auditors periodically to benchmark your security standards and practices against industry state-of-the-art, once you have solid operational practices in place. Benchmarking can identify weaknesses, suggest improvements, and help you decide how much protection to buy.

7. Rehearse your response. When security is breached, the whole organization goes into crisis mode, and managers have to make difficult decisions fast. It helps to have procedures in place that will guide diagnosis of a problem, guard against knee-jerk decisions, and specify who should be involved in problem-solving activities. It also helps to have practiced your response to a security breach. Rehearsing enables decision makers to act more confidently and effectively during a real event. If you know, for instance, exactly how quickly you can capture images from disk drives, or if you have backup software that's ready to be deployed, or how long it will take to rebuild a system, you'll be in a better position to make thoughtful, deliberate decisions.

8. Analyze the root causes. Whenever a security problem is found, the organization should conduct a detailed analysis to uncover the root cause. The tools needed are no different from those used for years in quality assurance programs. They include fishbone diagrams, eight-step processes, and plan-do-check-act cycles. Toyota, a world leader in quality manufacturing, uses an approach called "The 5 Whys" to get to the bottom of production and quality problems. To put that in a digital security context, the investigation might sound like this:

- Why didn't the firewall stop the unauthorized entry? Because the attacker had an authorized password.
- Why did the attacker have an authorized password? Because an employee revealed his password to someone posing as an employee.
- Why did the employee reveal his password? Because he didn't realize the danger in doing so.
- Why didn't the employee realize the danger? Because he had not seen a security bulletin that addressed the subject.
- Why hadn't the employee seen the security bulletin? Because there was a problem in the distribution process.

Toyota has found that the answers to the final questions almost always have to do with inadequacies in the design of a process, not with specific people, machines, or technologies. Using tools like this to investigate digital security incidents drives continuous operational improvements that ultimately lower risk.

*Article by Robert D. Austin, associate professor in the Technology and Operations Management unit at Harvard Business School, and Christopher A.R. Darby, CEO of an internet security company. Excerpted with permission from "The Myth of Secure Computing," **Harvard Business Review**, Vol. 81, No. 6, June 2003.*