

The Myth of Secure Computing by [Robert D. Austin](#) and [Christopher A.R. Darby](#)

For two weeks in the summer of 2001, a tiny computer program known as the Code Red worm burrowed through a security hole in Microsoft's server software to infect hundreds of thousands of computers around the world. As far as computer viruses go, Code Red was fairly benign—it defaced Web sites but didn't directly corrupt or destroy files—yet it nevertheless did a great deal of damage. Many companies lost the use of their networks; some had to take their Web sites off-line. The total bill for cleaning up the mess has been estimated at a whopping \$2.6 billion.

If you're like most senior executives, you probably have only a vague memory of the Code Red worm, or of any of the other viruses or hacker attacks that have plagued corporate networks in recent years. Indeed, you probably don't pay a whole lot of attention to digital security in general. You know it's a problem—a potentially enormous one—but you avoid getting directly involved in dealing with it. For one thing, digital security is extraordinarily complicated, requiring all sorts of specialized technical knowledge. What busy executive has the time to learn the ins and outs of “buffer overflow” attacks, for instance? For another thing, the majority of security breaches actually originate with insiders—with careless or vindictive employees. Prevention requires a lot of nagging, something most executives don't like to do. Lastly, digital security is invisible; you know you've succeeded only when nothing happens. So there's little personal payoff for a job well done. Investors and directors are unlikely to pat you on the back and say, “Good for you! No serious security breaches for the past three years.” If anything, they'll scowl and say, “Wasting money again, like you did on Y2K? Why not let that money drop to the bottom line?”

It's therefore no surprise that senior managers routinely hand off responsibility for digital security to their technical people or to consultants hired to “make the organization impermeable.” But an arm's-length approach is extremely unwise given the high stakes involved. According to industry estimates, security breaches affect 90% of all businesses every year and cost some \$17 billion. Protective measures are expensive; the average company can easily spend 5% to 10% of its IT budget on security. Even more important, security breaches can have far-reaching business implications. They can disrupt operations, alienate customers, and tarnish reputations. Business managers, not just technical managers, are the ones who will have to deal with the consequences of a security breach, which is why they're the ones who should spearhead preventive measures, and fast. The sobering fact is, threats to security—be it from disgruntled employees or from cyberterrorists—are escalating in number.

The good news is that general managers don't have to learn about the more arcane aspects of their company's IT systems to establish crucial preventive measures. Unlike IT managers who may be directly involved in the cat-and-mouse games played with potential intruders, business managers should focus on the familiar task of managing risk. Their role should be to assess the business value of their information assets, determine the likelihood that they'll be compromised, and then tailor a set of risk-abatement processes to particular vulnerabilities. That approach, which views computer security as an operational rather than a technical challenge, is akin to a classic quality assurance program in that it attempts to avoid rather than fix problems and it involves all employees, not just IT staffers. The goal isn't to make computer systems completely secure—that's impossible—but to reduce the business risk to an acceptable level.

The Threats

Threats to digital security come in many shapes and sizes, but they essentially fall into three categories.

Network attacks are waged over the Internet. They can slow network performance, degrade e-mail and other online services, and cause millions of dollars in damages—all without breaching the internal workings of an IT system. Denial of service (DoS) attacks, for instance, disable computers by flooding them with an overwhelming number of messages. As the computers try to respond to each of the thousands of messages, their resources are consumed and they often crash.

In February 2000, DoS attacks against such high-profile targets as Yahoo, eBay, CNN, and the FBI caused damages estimated in excess of \$100 million.

DoS attacks are easy to mount and difficult to defend against. The average individual can download an attack program from the Internet in less than ten minutes. And even more sophisticated attacks—such as a distributed denial of service (DDoS) attack, which hijacks computers and uses them to launch further DoS attacks—can be started by people with only modest technical skills. Fortunately, new enterprise software tools can thwart most network attacks, and even if your systems are knocked out, the damage is rarely permanent.

Intrusions differ from network attacks because they actually penetrate an organization's internal IT systems. How do intruders do it? It's easier than you might think. User names are generally predictable: John Smith's user name is often jsmith, for example. As for passwords, people frequently use birthdays, children's names, or even "password." And as unbelievable as it may sound, many tape their passwords to their monitors so they don't forget them. (It's worth noting that the majority of intrusions are committed by insiders.) Even people who create hard-to-guess passwords will often give them up to an official-sounding caller pretending to be a company network engineer. Sometimes, intruders don't even need to steal passwords; they can get in through flaws in software code.

Once inside a network, intruders enjoy the same rights of access and control over systems and resources as legitimate users do. They can steal information, erase or alter data, deface Web sites, or pose as company representatives. In one instance, an intruder posted a press release about an earnings shortfall, causing a company's stock price to plummet. And intruders can use what's called sniffer software to eavesdrop on network conversations and acquire more passwords. Because traffic flows among companies, a sniffer can find passwords on other networks, too.

One of the most difficult problems arising from intrusion is figuring out what, precisely, was done. Hackers take great pains to cover their tracks. They may make subtle changes in a system, open obscure "doors" that allow other hackers secret access in the future, or slightly alter data in ways that are difficult to detect. They can also deposit time bombs, seemingly innocuous bits of code that are scheduled to explode at a future date. And many intruders leave behind programs (with names like "Devil" and "Executer") that allow them to use the company's computers to launch other attacks.

While it can be costly for companies to uncover what, if any, changes were made, it's absolutely crucial. There's a very high public relations penalty for not knowing something consequential about your computer systems or, worse, for making false assurances about the security of your systems.

The final type of threat, *malicious code*, consists of viruses and worms. Although experts disagree about the precise definitions, a good rule of thumb is that viruses need help replicating and propagating (they rely on naive users to open an e-mail attachment, for instance) whereas worms do it automatically. Both types of malicious code move much faster than human hackers do. What's more, their targets can be random, making it impossible to predict where they'll hit next. The SQL Slammer, which struck in January 2003, attacked indiscriminately and took down the Finnish telephone service as well as more than 13,000 Bank of America ATMs. And because worms and viruses are often used to launch other strikes, their potential for

destruction is enormous. The Code Red worm, for example, not only invaded vulnerable systems but also deposited a program to launch DoS attacks against other computers.

Clearly, digital attacks—especially when used in combination—can bring a company to its knees. Consider the damage done by one disgruntled bank employee. During a holiday weekend, he launched a DoS attack against an internal network that connected important banking systems to the company's databanks. Knowing the IT staff would have its hands full restoring communication between systems and storage devices, he moved the battle to a second front. He knew which Web server software the company was running, and he knew (or suspected) that its security patches were not up-to-date. He researched the software's vulnerabilities and then downloaded programs created by the hacker community to exploit those flaws. He altered the bank's Web site so that visitors were diverted to a pornographic site.

Having created another diversion, the attacker started doing more serious damage. He knew which bank databases contained customer information, and he suspected that database applications had not been "hardened"—in other words, adjusted so that only required services were left running. The attacker used a service that was running unnecessarily to corrupt the databases and destroy client data.

By Tuesday morning, the bank was in chaos. Because the integrity of its systems couldn't be trusted, the bank was reduced to a pencil-and-paper operation. Although it recovered from most of the technical disruption in four business days, it was still working to restore client confidence six months later.

The Operational Approach

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

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 first have to figure out what your digital assets are (they're not always obvious). A team of senior managers from across the company should take an inventory of data and systems, assess how valuable each is to the company, and decide 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. When you're done with that, you'll have a blueprint that identifies precisely what your digital assets are, how much protection each merits, and who's responsible for protecting them.

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 left

unclear. 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.

Control access to your 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 a way to bar some people from your computer systems while letting others in. You need systems that determine 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 meet these requirements, but they’re only as good as the information that feeds them. They should be configured to reflect the choices you made when you defined your most critical assets and decided who had access to them. Of course, nontechnical 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 the 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.

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. Look at the wording of this contract between General Electric and software company GMI:

***Code Integrity Warranty* (source: www.freeedgar.com)**

GMI warrants and represents that the GMI software, other than the key software, does not and will not contain any program routine, device, code or instructions (including any code or instructions provided by third parties) or other undisclosed feature, including, without limitation, a time bomb, virus, software lock, drop-dead device, malicious logic, worm, Trojan horse, bug, error, defect or trap door (including year 2000), that is capable of accessing, modifying, deleting, damaging, disabling, deactivating, interfering with or otherwise harming the GMI software, any computers, networks, data or other electronically stored information, or computer programs or systems (collectively, “disabling procedures”)....If GMI incorporates into the GMI software programs or routines supplied by other vendors, licensors or contractors (other than the key software), GMI shall obtain comparable warranties from such providers....GMI agrees to notify GE immediately upon discovery of any disabling procedures that are or may be included in the GMI software, and, if disabling procedures are discovered or reasonably suspected to be present in the GMI software, GMI, as its entire liability and GE’s sole and exclusive remedy for the breach of the warranty in this section 7.3, agrees to take action immediately, at its own expense, to identify and eradicate (or to equip GE to identify

and eradicate) such disabling procedures and carry out any recovery necessary to remedy any impact of such disabling procedures.

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) costs the company \$1 million, and it releases as many as 12 a month. But 80% of these patches would be unnecessary if the company eliminated only one common type of coding error known as "buffer overflows."

Know exactly what software is running.

It's shocking how many companies don't follow this very obvious rule. Keeping track of what 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 reasons, 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 people to make changes quickly. Procrastinating on updating patches gives hackers an easy in. Both the Code Red and SQL Slammer worms affected only those companies that had not yet patched known flaws in their software. The fixes had been available from the vendor for more than a month in the case of Code Red and for more than six months in the case of SQL Slammer.

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 trade-offs between security and productivity are often incorrect. Security concerns can drive operational simplifications that pay efficiency dividends as well.

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 those 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 fun or profit 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 new weaknesses, suggest improvements, and help you decide how much protection to buy.

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 the problem, guard against knee-jerk decisions, and specify who should be involved in problem-solving activities. It also helps to have practiced; rehearsing enables decision makers to act more confidently and effectively during real events. 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.

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 another company employee.*
- Why did the employee reveal his password? *Because he didn't realize the danger in doing that.*
- 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 your risk.

The Bottom Line

Companies cannot afford to respond to every security threat with equal aggressiveness. Even if they could, it wouldn't make business sense. Instead, managers need to sort through which risks are most likely to materialize and which could cause the most damage to the business, then spend their money where they think it will be most useful. It's not a calculation that happens just once, of course, since new threats and new capabilities are always emerging. But the process for thinking about them doesn't change.

Managers need to sort through which risks are most likely to materialize and which could cause the most damage to the business, then spend their money where it will be most useful.

This is not to say that the logic of risk management is uncomplicated. For some companies, it can be very complicated, indeed. Managers' attitudes toward risk are often complex, and that psychological wrinkle needs to be acknowledged. A further complication arises from the difficulty of estimating costs and probabilities. Not all risks can be countered with well-defined management actions. Sometimes no possible action can address a particular serious risk. Other times, addressing a serious risk is prohibitively expensive.

The important thing to realize is that every case is about making business trade-offs. When viewed through an operational lens, decisions about digital security are not much different from other cost-benefit decisions general managers must make. There is no reason to be overwhelmed by the technology involved or the

expensive quick-fixes that experts want to sell. The tools you bring to bear on other areas of your business are good models for what you need to do in this seemingly more difficult space.

When airtight clauses like these become common in software contracts, exploitable flaws will become rare.

Securing the Small to Midsize Enterprise

The processes we advocate in this article may sound like they're beyond the reach of small to midsize businesses, but, if streamlined intelligently, they shouldn't be. You'll want to identify your digital assets; probably only a few will be critical. Be sure to include external service providers when you map the people and processes that affect critical assets. You'll also need to concern yourself with the other principles in the framework: security policies, tools and techniques, secure software, configuration management, and so on. Fortunately, you can handle most of these with a few simple actions:

Secure the perimeter. Build a secure perimeter around your company's computers by installing three components: a firewall, virtual private network (VPN) software for remote access, and virus detectors on your mail server. Mail should be the only non-VPN traffic you allow to cross the perimeter inbound (firewall settings will allow you to do this). If you don't have internal staff to handle these three things, you can hire a security service provider to do them for you. You'll need such professionals to monitor your perimeter once it is established and to test your environment periodically. If you have publicly accessible applications, you might also ask the security provider to do occasional penetration testing.

Lock down computers. Install antivirus and personal firewall software on all laptops, desktops, and servers; these are inexpensive and are available at most computer stores. Turn off unneeded functionality on all machines (again, get help from a security service provider if no one in your company knows how). Turn on auto-update, so that Internet-connected computers can automatically acquire and install fixes as vendors make them available. And use the vendor's lockdown guide (often available on its Web site) to configure your computers and their software in a secure mode.

Communicate and enforce policies. Make sure that everyone in your company is aware that they should not run unapproved network applications: P2P file sharing (for example, many popular music-sharing services), instant messaging, and the like. Have your IT person monitor security bulletins from vendors for the products you're using. And have a checklist ready so that when employees leave, your IT people will immediately take action to deactivate their passwords and VPN access.

Earnings Versus Security

In recent years, CEOs have felt extraordinary pressure to keep their profits marching "to the northeast corner." Spending on digital security doesn't figure easily into that context. Suppose a CEO spends aggressively to protect his company against the possibility of a serious security breach and that his competitors do not. Suppose further that nobody in the industry experiences a major security breach for a couple years. The CEO will have nothing to show for his investment, and the company's earnings will be considerably lower than those of competitors. The CEO who persists too long in investments that result in nothing happening might soon be out of a job.

A basic reality of financial mathematics accentuates the problem of balancing security risks and profitability pressure: Rare, catastrophic events, when they do occur, have costs that greatly exceed the costs at which

they enter into the math of financial justification. Traditional financial analysis scales the costs associated with such events in terms of “expected value,” in proportion to their infrequency. Hence, a \$1 million loss that is judged only 0.1% probable will enter financial calculations as only a \$1,000 loss ($\$1,000,000 \times 0.001$). When there is uncertainty about the level of uncertainty—that is, when it’s unclear whether the loss-making event will happen with 0.01% probability or 0.001% probability—it becomes even harder to justify spending a lot of money to avoid the loss.

High-level policy makers have begun grappling with how to protect the U.S. IT infrastructure, which is composed largely of the individual infrastructures of many companies. Some officials believe that businesses should invest in security because “it’s the right thing to do.” CEOs may feel that this position is naive, when markets remain so willing to punish companies for not showing steady growth. CEOs need some form of cover to spend on security—it could come in the form of insurance coverage, and it could come in the form of regulation (most business leaders would not be enthusiastic about that solution, we suspect). But until executives and policy makers figure it out, our national infrastructure will remain at significant risk.