

By Jeff Relkin

Security is not an area newly arisen in the wake of the 9/11 tragedy. There have always been reasons to be concerned: conflicting priorities, business environmental factors, information sensitivity, lack of controls on the Internet, ethical lapses, criminal activity, carelessness, and higher levels of connectivity and vulnerability. It's a tradeoff between limiting danger versus affecting productivity: 100 percent security equals 0 percent productivity, but 0 percent security doesn't equal 100 percent productivity.

No one wants to be controlled. It's demeaning and stifles productivity, and we resent the implication that we can't be trusted not to break our own networks. On the other hand, organizations have to decide how long they could operate without computers or networks and how reliant they are on the availability and accuracy of data. Absolute security is unattainable and undesirable, so proper security controls seek to reduce risk to acceptable levels.

## 1 System penetration threats

There are all kinds of ways in which systems can be compromised. A popular expression during World War II was "Loose lips sink ships," which was meant in a possibly somewhat paranoid way to heighten awareness that you never knew who was listening to you, even over a beer at the local pub. Most of us routinely have contact with other professionals whether at industry gatherings, social events, or any number of other venues. It's all too easy to accidentally disclose critical information that can be used, however unethically or even illegally, to benefit one organization at the expense of another.

Carelessly discarding access codes and other kinds of personal identification information without shredding them has made dumpster diving the number one method of obtaining this kind of data. Systems that are poorly or inadequately secured (single-level security, easily guessed passwords, unencrypted data, etc.) are an invitation to problems ranging from low data quality to unauthorized infiltration.

Networks can be easily breached due to poorly maintained firewalls and/or virus and spam filters. Security budgets must be adequately funded; management literally puts organizational survival at risk by viewing funding for security measures as a no-return or discretionary expense. Taking responsibility for our own actions (or inactions) coupled with a solid comprehensive security policy is the best defense to prevent breaches from occurring in the first place.

## 2 Internet security realities

Originally built for military use, the Internet today incorporates little inherent protection for information. Administrators at any Internet site can see packets flying by, and without adequate encryption, messages are subject to compromise. The Internet doesn't automatically protect organizational information—companies must do so independently. Without adequate control, and even with it, employees can access just about anything and bring it in-house. External intruders can access networks and PCs. External message sources typically can't be found, and message senders don't know who else, in addition to or instead of the intended recipient, is reading the message.

The hacking community is increasingly organized, and by cooperating with each other, networks can be even more easily, and profoundly, compromised. The Internet is an open, uncontrolled network that doesn't change to suit organizational needs. Identified exposures are not automatically fixed, and most security problems on the Internet are not really Internet problems. Organizations must assume a potentially hostile environment and protect themselves through full message encryption for sensitive information, digital signature for message authentication, high quality maintained firewalls and other filters, employee communication and awareness programs, and any inbound controls that are at least adequate without being excessive.

## 3 Portability of hardware

Corporate road warriors traveling with laptops represent a variety of security challenges. Larger, faster hard drives and more powerful processors provide the ability to download and use local copies of sensitive or confidential databases. Ubiquitous Internet access allow us to stay connected with the same networks and systems we use in the office. Web-based services such as Groove can be used to circumvent corporate document policies.

Laptops need to be secured with at least two-phase security controls consisting of a combination of encryption, local userid/password combinations, biometric devices, etc., and organizations need to implement and enforce strict policies on technology use while traveling.

## 4 Proliferation of new communication methods

Does your organization provide PDAs such as BlackBerrys or Treos with network connectivity? Are these devices secured in any way? Many companies have little understanding of just how big a security threat these handy little gizmos represent. Typically connected to central corporate services, such as Outlook or Notes, and providing continuous wireless automatic synchronization with e-mail, calendar, and contact lists, a lost device that's unsecured by a password can be used to gain authorized entry into those systems. At the very least, they can be used to run up a pretty impressive cell phone bill.

Corporations should require that despite the inconvenience, all such devices must have local passwords, subject to the same rules as those used to access the network, including format and frequency of change. They should also require by policy that lost devices be reported immediately so kill signals wiping all local data and rendering the device useless can be issued.

## 5 Complexity of software

The fact that systems and applications have many integrated components that are difficult to individually secure is a poor excuse for not requiring multiple levels of security. Users who have been authenticated for general network access do not necessarily deserve authorization for specific functional components of that network or even within a single integrated environment, such as an ERP. Studies and surveys tell us that employees consider too many different passwords a valid reason for leaving an organization; some large corporations require users to memorize in excess of 15 userid/password combinations. Single sign-on techniques provide the ability to secure systems one component at a time on the basis of one individual access, so there's no reason to make security onerous to the user community.

## 6 Degree of interconnection

This is just another form of complexity and requires a recognition of the realities of the public access Internet. Supply chain processes connect raw material providers, manufacturers, assemblers, and retailers. As the saying goes, a chain is only as strong as the weakest link. Even if individual organizations within the supply chain have proper security controls in place, one lapse by one of the partners can bring the entire operation to a halt.

Consider a situation in which a parts supplier's network is infiltrated and/or compromised. All the downstream component processes can be negatively affected, either by the delay or loss of a critical ingredient or by a contaminated input, in the same manner that a glitch at the start of an assembly line brings the entire operation to a screeching halt. Organizations need to conduct a comprehensive risk assessment and try to require their partners and suppliers to adhere to adequate security controls, or at the very least, develop contingencies around the possibility of losing access to critical partnerships.

## 7 Density and accessibility of media

Information is currency, and knowledge is power. Knowing this, we're all responsible for maintaining the integrity and security of the corporate data to which we have authorized access. New forms of higher density portable media make it even more necessary to take this responsibility seriously. CDs, DVDs, flash drives, and other dense portable media are capable of storing multi-gigabytes of data in a form that all too often grows legs and walks away.

Corporate users should be circumspect about how they use these media. IT security policy should require that any data moved through USB ports or any other method of creating media do so on an encrypted basis. Policy, and common sense, should also dictate that these same media types never be used for single copies of any data, especially mission critical or business confidential, and limit their use to temporary movement of data from one location to another.

## 8 Centralization

Single points of failure can be security nightmares. As important as it is to secure corporate networks, systems, and data, it's especially critical to do so when those assets are centrally located. Smaller organizations with limited technology resources are particularly vulnerable because they typically have one LAN room or one server rack, which is the entire network for the whole organization.

Unauthorized access, power problems, communications glitches, protocol incompatibilities, and questionable system philosophies can all contribute to catastrophic consequences. When technology assets are centralized either as a result of limited resources or simply due to a valid design consideration, attention must be given to special security requirements to ensure continuous operation.

## 9 Decentralization

The opposite situation comes with security considerations of its own. Multiple copies of individual systems or databases all must be equally well secured; one compromised copy renders the entire application suspect. One of the more difficult situations to deal with in global organizations with presences in various countries occurs where Internet access is neither robust, consistent, nor reliable. In this case, the best solution is often to install a distributed DNS server for offline synch with the main corporate network, providing a local facility that while not real time, is at least a comprehensive copy no more than one half day old of necessary data. Since this requires putting sensitive or confidential information out into the field, policies and procedures must be enforced that provide the same level of security for the decentralized facility as that for the main corporate network to avoid the same risks of infiltration and compromise.


## 10 Turnover

Employees changing jobs represent a particularly difficult security challenge. A generation ago, you'd simply turn in your keys and go on with your life, but it's not so easy to do that when the keys are virtual entries into secure systems.

Every access granted to individual employees has to be tracked so that at departure time, those accesses can be turned off. In some cases, security systems will have to be cycled for everyone remaining with an organization when a key employee having a deep level of access goes elsewhere.

*[Jeff Relkin](#) has 30+ years of technology-based experience at several Fortune 500 corporations as a developer, consultant, and manager. He has also been an adjunct professor in the master's program at Manhattanville College. At present, he's the CIO of the Millennium Challenge Corporation (MCC), a federal government agency located in Washington, DC. The views expressed in this article do not necessarily represent the views of MCC or the United States of America.*

## Additional resources

- TechRepublic's [Downloads RSS Feed](#) 
- Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- Sign up for our [Network Security NetNote](#)
- Check out all of TechRepublic's [free newsletters](#)
- "[10 ethical issues confronting IT managers](#)" (TechRepublic download)
- "[10 ethical issues raised by IT capabilities](#)" (TechRepublic download)
- "[Establish and implement effective security policies](#)" (TechRepublic download)

## Version history

**Version:** 1.0

**Published:** September 6, 2006

## Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team