Securing our networks is a huge task. To defend ourselves from cyber threats, private institutions, industry groups, and governments worldwide must make a strong commitment and cooperate at unprecedented levels

Information Assurance in the Twenty-First Century

Mike McConnell, Booz Allen Hamilton

In the early- and mid-1990s, telecommunications networks and the Internet drove business growth in the United States. The growing dependence on such networks, however, also increased US vulnerability to cyber exploitation. Indeed, by the end of the twentieth century, the US had become more vulnerable than any other nation to cyber attacks aiming to interrupt, degrade, or destroy vital services such as electrical power, banking, or stock trading. A determined terrorist group with cyber tools and knowledge gleaned from publicly available information could threaten the very money supply on which a free market depends.

As director of the National Security Agency from 1992 to 1996, I was in a unique position to see just how vulnerable the US had become. As the Cold War ended, NSA shifted its focus from Soviet-era targets to new national security concerns. The agency realized that the kinds of communications it needed to exploit were the very kinds of networks that were driving productivity and creating a higher standard of living in the US. Early successes against international communications targets revealed very little difference between the ability to passively exploit a target for intelligence purposes and the ability to degrade or destroy that target.

The dark side of progress

New vulnerabilities are the dark side of globalization and rapid information technology development. Securing our countries, our businesses, and our personal lives against cyber crime and terrorism requires an unprecedented change in laws, policies, culture, and attitudes about cyber security, which in our democracy will evolve over time. In addition, we need more public-private partnerships to protect us from these new threats.

The dawn of the new century revealed completely new threats to the US—from inside its borders. The country's national security apparatus, however, especially the military, is geared to fight international threats in international theaters. Indeed, NSA's mission is limited to foreign international targets, as it has no domestic or law-enforcement role. The tragic events of September 11th demonstrated that relatively low-technology attacks can cause massive casualties, extensive social and business disruptions, and huge financial burdens. Some of the lessons learned, however, demonstrate the potential for an even greater disaster resulting from cyber terrorism, especially if combined with physical attacks.

Security—or rather, lack of security—has consequently become a major issue for businesses and society. A recent Booz Allen Hamilton survey of the nation's top companies found that three-quarters of their CEOs are more concerned about protecting their businesses, employees, networks, and business operations than they were a year ago. In addition, concern about the convergence of noncomputer networks (physical networks such as supply chains, and trust networks such as partnerships) is growing.

A double-edged IT sword

The world is becoming more wired. While all countries have become more connected over the last few decades, network proliferation has been concentrated in the most developed countries, especially in the US. The US continues to computerize its public and private infrastructures, which now run everything from telecommunications and banking services to electric power generation and distribution.

Greater use…

The still-accelerating development, proliferation, and adoption of information and communications technologies have benefited the world enormously. We have made huge strides in science and medicine, and have greatly increased productivity. We accomplish more, with a greater sense of safety and efficiency. We maintain contact with many more people—by audio, video, and data link—to collaborate on work or study, pursue official or unofficial diplomatic relations, diagnose and treat disease remotely, or just stay in touch.

…breeds greater dependence

But as computers and networks become more ubiquitous, we grow more dependent on them. Thus, we become more vulnerable to criminals and terrorists who would use these systems against us. Just as technology has improved the efficiency and effectiveness of business operations, it has also increased terrorists' abilities to launch sophisticated attacks against our increasingly interdependent infrastructures.

"Knowledge is power." Information today is worth more than ever. Whereas in the past, attackers could only collect information while it was being transmitted from place to place, today our data is vulnerable 24 hours a day, wherever it's located. Our enemies no longer have to wait for the information they need to come their way. The September 11th hijackers attacked symbols of American power; cyber terrorists can attack the infrastructures that make that power possible, and with less difficulty.

Extending our reach

Dramatic world events of the past two decades have reshaped the balance of power and altered people's lives. Once-protectionist economies around the world are now more open, creating a free flow of goods and services. Consolidation and globalization have increased consumer options and opened up larger markets for corporations. New economic models have boosted competition, forcing corporations to continuously increase the value of their operations. They do this in part through innovative product lines, but also by increasing operation efficiency and effectiveness.

New business models

New business models have also emerged. Increasingly, companies are concentrating on their core competencies and outsourcing everything else, creating tightly integrated supply chains and just-in-time delivery of required manufacturing inputs. Partnerships, strategic alliances, and extended enterprises increase a company's product or service lines, or broaden its reach. Some companies have moved beyond simply outsourcing routine operations to creating new, virtual organizations.

The Internet and related technologies have increased the speed, quality, and ease of communications between business partners. As Figure 1 illustrates, these technologies also enable higher levels of collaboration across the product-delivery value chain. They allow organizations to structure operations globally and take advantage of regional core competencies, thus maximizing the value proposition to their stakeholders. Increased information flow across and between continents combined with more efficient transportation lets companies optimize their supply chain to maximize revenue potential and support growth.

Virtual organizations include vendors and external partners early in the process—from product design through delivery and support. Competitors sometimes cooperate to complement each other's capabilities. The defense industrial sector is a classic example: multiple manufacturers collaborate on contracts because of project size, complexity, and the need for multiple specialized services. One manufacturer might team up with another that is also collaborating with its competitors. For example, an automotive supplier producing seats might be working with several competing auto manufacturers on future designs. Such a business model means that company outsiders need greater access to information traditionally held within organizational boundaries.

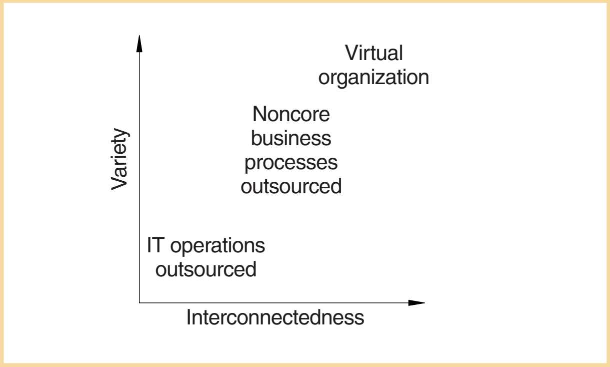

Figure 1. As an organization increases the size of its network, the variety of inputs, potential outputs, and markets increases.

Everyone's an insider

Today, everyone connected to the Internet is a potential virtual insider in your organization. A virtual organization that includes external vendors, trading partners, and even customers changes the "insider" definition and forces greater focus on information security policies. You need to consider not only your organization's policies, but also the policies of your networked associates.

Traditionally, in a noncomputing environment, authorization for information access is based on well-defined roles that clearly identify users and their access privileges. In today's computing environment, however, roles continually evolve and are often less well defined.

The wolf within

Imagine our day-to-day lives without reliable or adequate electric power, telephone services (including 911 emergency service), or railroads. Public utilities, government agencies, and private businesses are all under threat of attack—from denial-of–service to information theft to operation disruption. A recent study by the Center for Strategic and International Studies, a Washington, D.C.-based think tank, asserts, "A properly prepared and well-coordinated attack by 30 computer virtuosos located around the world, with a budget of less than $10 million can bring the United States to its knees."

Moore's Law predicts that computing power will double every 18 months for the foreseeable future. This prediction has essentially been borne out over the past two decades, and it shows no sign of slowing. But increased computing power isn't only in the good guys' hands; the same increases in power—now destructive power—are available to criminals and terrorists. For every new defense, a new offense is designed, and vice versa. And neither market forces nor the need to produce saleable goods constrain these criminals. Couple this with the ubiquity and interdependence of our networks, and our reliance on them for critical day-to-day functions: the wolf is not at the door, but already inside.

Half measures

The information security models prevalent in most organizations are point-defense solutions that protect the perimeter because in the past,

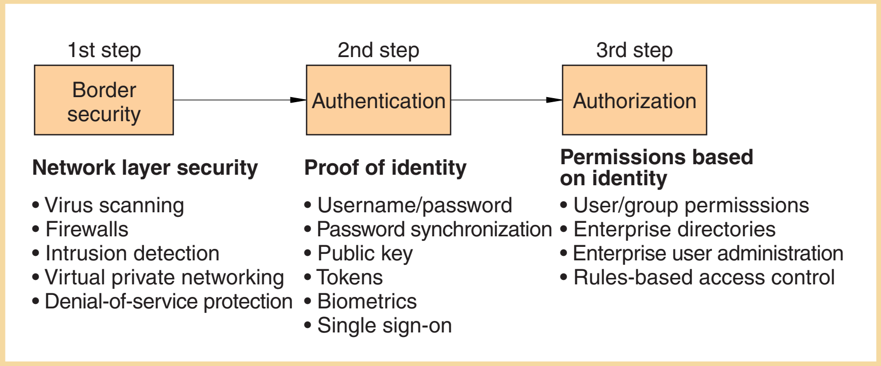

Figure 2. A layered defense allows an appropriate set of users to access the network and provides robust security throughout the enterprise's extended network.

- organizational boundaries were clearly defined,
- securing the perimeter was much easier than securing every system, and
- only insiders were considered trustworthy.

This model has been turned on its head: virtual organization boundaries are often amorphous, defense of a changing and largely unknown perimeter is impossible, and insiders cannot necessarily be trusted. For instance, while most financial services CIOs believe they have the right technology to protect their companies' perimeter, they also acknowledge that 70 percent of the threat is internal and almost impossible to monitor. More generally, the FBI reports that insiders commit as much as 75 percent of all cyber crime—and this assessment is based only on reported security breaches.

Without clear role definitions, companies must develop a broad set of rules and constantly evolving roles, which results in higher administrative overhead. The emergence—or recognition—of the insider threat has driven many companies to create complex rule sets that completely segregate users, not only keeping "inside outsiders" out of proprietary areas, but also screening much of the information used by their partners from true insiders.

While organizations have increased the security inherent in their virtual reach across their network of partners, security mistakes continue to surface. Below I've listed the eight most common mistakes companies make as information security management creates strategic business challenges. These mistakes are not new, but their impact increases as unknown interdependencies in the infrastructures proliferate.

- *Undervalued information*. Few organizations analyze the contributions that specific information assets make to the bottom line.
- *Lack of risk management processes.* Because organizations often have no institutionalized means of evaluating threats and vulnerabilities, the security implications of corporate procedural changes, or the likelihood and impact of IT security-related risks, risk management is haphazard at best.
- *Narrowly defined security boundaries.* Organizations focus internally, neglecting to evaluate and understand the security practices of their supply-chain partners.
- *Lack of appreciation for information security.* Information security gets attention only when a problem occurs, creating an attitude that it distracts from "what's important."
- *Dated security management processes.* Security managers often mistakenly view security risks as static, when in fact they change constantly as the organization, network configuration, and technology change.
- *Lack of communication about security responsibilities.* Companies view security as an exclusively technical issue, considering it the purview of the information systems organization. Organizational accountability is dispersed.
- *Crisis-security policy.* A reactive approach permits serious damage to the organization and ignores risks that have not yet caused harm.
- *Poor security awareness and training.* Technical personnel knowledge and skills become dated, and other staff members are not sufficiently informed of security risks and good practices.

Security solutions providers can no longer afford to focus on border security. Tools such as firewalls, virus scanners, and intrusion detection systems are rapidly maturing, but rapid technology advances, a plethora of nonsecure products, and the growing complexity of corporate networks diminish their effectiveness. To appropriately respond to their increased vulnerability, virtual corporations must focus on building a layered defense to secure the information assets. Figure 2 shows the three steps of an in-depth defense plan.

New questions, new approaches

To address their particular security needs, companies are now grappling with such questions as

- What level of information security is right for the organization?
- How much should we spend on information security?
- What portfolio of tools, technologies, and processes will optimize our information security system?

Organizations must take a holistic approach, shown in Figure 3, when creating and managing an information security program. The program must constantly evaluate and address emerging vulnerabilities and threats to the organization. End users must recognize that information security is as vital as physical security and adopt responsible behavior. Senior leaders need to clearly articulate and visibly support the information security program.

A comprehensive security assessment will help companies understand their vulnerabilities and establish a security baseline. The resulting security plan must address risks to their information assets, enforce and audit compliance, and create metrics to track returns on security investments. Training and communication programs are crucial to the success of any security program. End users must clearly understand their roles and responsibilities in securing the organization's information assets.

The collaborative environment extends beyond organizational boundaries and often spans national boundaries. Technical solutions supporting this collaborative environment must consider a variety of national laws and policy implications. Export controls, for instance, limit software exchange and data communications between countries, and infrastructure availability limits the solutions that can be implemented in each venue.

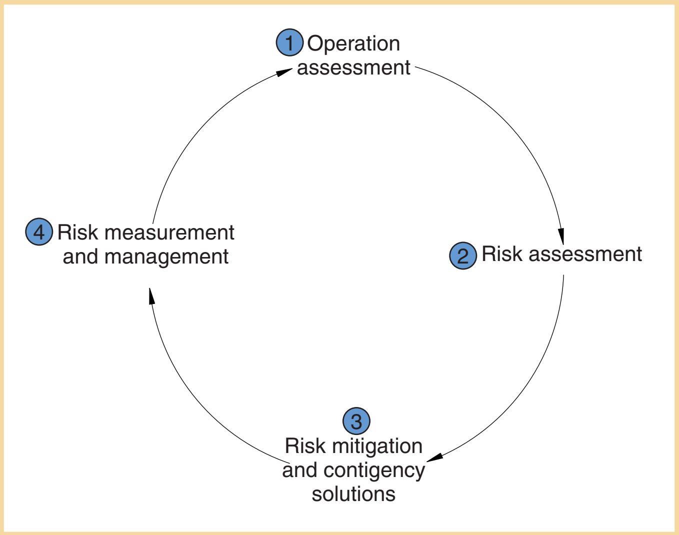
1 Operation assessment
2 Risk assessment
3 Risk mitigation and contigency solutions
4 Risk measurement and management

Figure 3. Enterprise risk-management lifecycle. A cyclic, holistic approach to information assurance maintains an organization's security posture in parity with changing threats and vulnerabilities.

Developing a comprehensive information assurance solution to address the changing threat environment and support future business needs requires significant cooperation among industry groups and associations, information security solutions providers, and clients in both the public and private sectors.

Industry groups, professional associations such as the IEEE Computer Society (www.computer.org), and public-private forums like the National Information Assurance Partnership (niap.nist.gov) have traditionally been instrumental in creating standards, raising awareness of the issues, and proposing best practices for addressing these issues. They also provide a vital link between the government and private industry in setting cyber policies and procedures.

Although securing our networks is a huge task, a strong commitment from key stakeholders is the best way to defend ourselves from cyber threats. To secure our future, we need private institutions, industry groups, and governments worldwide to ally in unprecedented levels of cooperation.

Mike McConnell is a vice president with Booz Allen Hamilton and the former director of the National Security Agency. Contact him at mcconnell_jm@bah.com.

News Briefs

Are Businesses Protecting Privacy?

Consumers and organizations that do business over the Internet want assurance that their transactions remain secure and that no outside parties can access sensitive personal data. Yet although the technology exists to secure personal and business communications and data, many companies that collect consumers' personal data have neglected to implement the necessary data security practices.

A 2000 study by Georgetown University's Health Privacy Project, for example, revealed that many online health sites don't follow their stated privacy policies and may share visitors' health information with business partners without consent. Many Web sites also passively mine personal information from visitors' computers, such as IP address, sites visited, name and email address, and other information available through users' browsers, without users' knowledge or consent.

Some consumers are turning to software designed to block Web marketers from mining personal information from their computers.

Once consumers offer personal information in a transaction, however, it's out of their hands. Also, privacy advocates contend that "opt out" provisions for online profiling and data sharing are largely ineffective because of the "lack of almost any kind of reasonable notice" on most Web sites, said Richard M. Smith, an Internet security consultant.

In addition to providing completely secure transaction processing, Gartner analyst Arabella Hallawell suggests that organizations safeguard data privacy by clearly informing site visitors about how their data may be used and letting them choose how their personal data is shared for marketing and service purposes. Companies should implement such processes not just to enhance customer data security and address privacy concerns but as part of "a broad strategy that strengthens the customer–business partnership," Hallawell added.

Security Think Tank Established

The New Jersey Institute of Technology and Princeton University have formed the Center for Wireless Networking and Internet Security to develop new network security technologies. The New Jersey Commission on Science and Technology has provided $2.6 million to fund the center, located at NJIT. Center director Atam Dhawan said he also anticipates further funding from corporations and the US government.

NJIT and Princeton students will work on research projects such as one that will allow the US military to instantly recognize a cyber attack and trace its source. Other projects include developing computer systems that can predict and prevent cyber attacks on wired and wireless multimedia networks.

Wireless systems are especially vulnerable because hackers can exploit their location-aware services, data transmission methods, and encryption flaws. Researchers hope to develop more robust ways to protect systems from unauthorized detection and tracking of users and the information they exchange.

The center will also seek new ways to protect Internet users from consumer fraud, a difficult problem because the networking technologies at the Internet's core were designed for open access. Because of this design, Dhawan said, "we now have few standards to protect information." Research will focus on building strong user and data authentication mechanisms into internetworking technologies.