# Improving the Security of Networked Systems

By Julia Allen, Christopher Alberts, Sandi Behrens, Barbara Laswell, and William Wilson
*Networked Systems Survivability Program, Software Engineering Institute, Carnegie Mellon University*

*As the Internet and other national information infrastructures become larger, more complex, and more interdependent, the frequency and severity of unauthorized intrusions is increasing. Therefore, to the extent possible and practical, it is critical to secure the networked systems of an organization that are connected to public networks. This article describes an emerging approach and set of activities for establishing and maintaining the security of networked systems.*

## Targeting the Problem

Networks have become indispensable for conducting business in government, industry, and academic organizations. Networked systems allow access to needed information rapidly, improve communications while reducing costs, enable collaboration with partners, provide better customer services, and conduct electronic commerce [1].

Organizations have moved to distributed, client-server architectures where servers and workstations communicate through networks. In addition, they are connecting their networks to the Internet to sustain a visible business presence with customers, partners, and suppliers. While computer networks revolutionize the way business is done, the risks they introduce can be fatal. Attacks on networks can lead to lost money, time, products, reputation, sensitive information, and even lives.

The *2000 Computer Security Institute/FBI Computer Crime and Security Survey* [2] indicates that computer crime and other information security breaches are still on the rise, and the cost is increasing. For example, 70 percent of the 585 respondents reported computer security breaches within the last twelve months, up from 62 percent in 1999. Furthermore, the financial losses for the 273 organizations that could quantify them totaled $265,586,240, a 100 percent increase over the $123,779,000 reported in 1999.

Engineering for ease of use is not being matched by engineering for ease of secure administration. Today's software products, workstations, and personal computers bring the power of the computer to increasing numbers of people to perform their work more effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, it is difficult to configure and operate many of these products securely. This gap between the knowledge needed to operate a system and that needed to keep it secure leads to increasing numbers of vulnerable systems [3].

Technology evolves so rapidly that vendors concentrate on time-to-market, often minimizing that time by placing a low priority on security features. Until customers demand products that are more secure, the situation is unlikely to change.

Users count on their systems being there when they need them, assuming that their information technology (IT) departments are operating all systems securely. This may not be the case. System and network administrators typically have insufficient time, knowledge, and skill to address the wide range of demands to keep today's complex systems and networks up and running. Additionally, evolving attack methods and software vulnerabilities continually introduce new threats to an organization's installed technology and systems. Thus, even vigilant, security-conscious organizations discover that security starts to degrade almost immediately after fixes, workarounds, and newly installed technology are put in place.

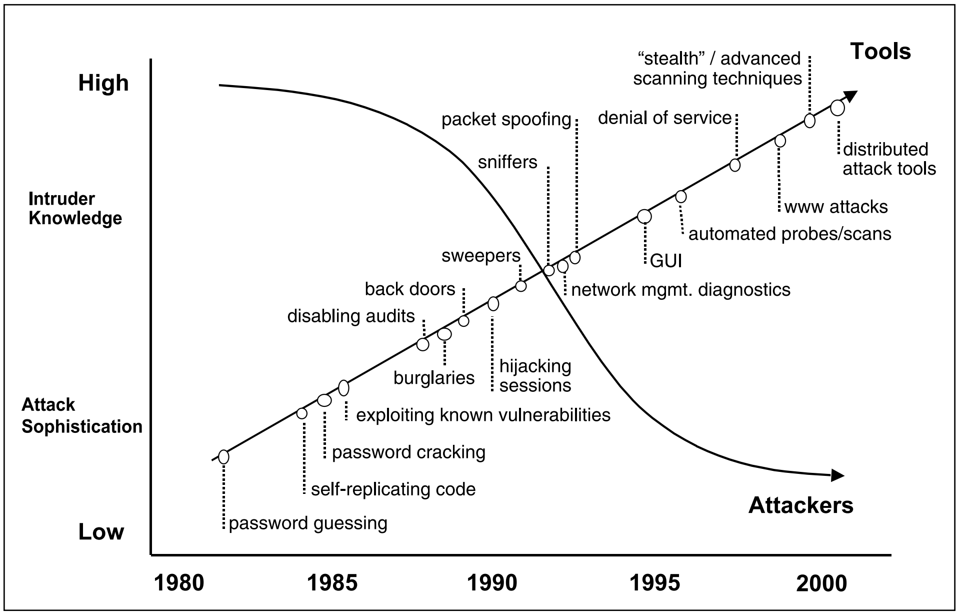
Inadequate security in the IT infrastructures can negatively affect the integrity, confidentiality, and availability of systems and data.

Who has this problem? The answer is just about everyone—anyone that uses information technology infrastructures that are networked, distributed, and heterogeneous needs to care about improving the security of networked systems.

## Why Improve Security?

Why should you care about this problem? Whether you acknowledge it or not, your organization's networks and systems are vulnerable to attack by both insiders and outsiders. Organizations cannot conduct business and build products without a robust IT infrastructure. In addition, users have an organizational and ethical responsibility to protect competitive and sensitive information. They must also preserve the reputation and image of their organizations and business partners. All of these can be severely compromised by successful intrusions.

Figure 1. *Attack Sophistication vs. Intruder Technical Knowledge*



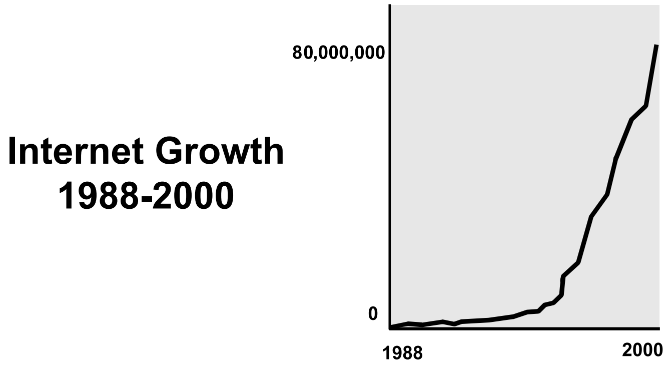
In the 1980s intruders were the system experts, as depicted in Figure 1. They had a high level of expertise and personally constructed methods for breaking into systems. Automated tools and exploit scripts were the exception rather than the rule. Today, absolutely anyone can attack a network due to the widespread and easy availability of intrusion tools and exploit scripts that can easily duplicate known methods of attack. While experienced intruders are getting smarter—as demonstrated by the increased sophistication in the types of attacks—the knowledge required on the part of novice intruders to copy and launch known methods of attack is decreasing. Meanwhile, as evidenced by distributed denial-of-service attacks and variants of the Love Letter Worm, the severity and scope of attack methods is increasing.

In the early to mid-1980s, intruders manually entering commands on their personal computers could access tens to hundreds of systems; today, intruders use automated tools to access thousands to tens of thousands of systems. In the 1980s, it was relatively straightforward to determine if an intruder had penetrated your systems, and discover what they did. Today, intruders are able to totally hide their presence, for example, by disabling commonly used services and reinstalling their own versions, then erasing their tracks in audit and log files. In the 1980s and early 1990s, denial-of-service attacks were infrequent and not considered serious. Today, for organizations such as Internet service providers that conduct business electronically, a successful denial-of-service attack can put them out of business. Unfortunately, these types of attacks occur more frequently each year.

Due to exploding Internet use the demand for individuals with necessary technical education far exceeds the supply required to meet the need (see Figures 2 and 3). This is true for both those in formal degree programs and those who have acquired on-the-job knowledge and skills. As a result, people who are not properly qualified are being hired or promoted from within to do the job. This trend is exacerbated by the fact that some skilled, experienced system administrators change jobs frequently to increase their salaries or leave the job market because of burnout.

Today's audit and evaluation products typically focus on the underlying system and network technologies without considering the organizational concerns (e.g., policies, procedures) and human aspects (e.g., management, culture, knowledge and skills, incentives) that can dramatically affect the security posture of IT infrastructures. As a result, incomplete or point solutions are implemented with the expectation that they will completely solve the problem.

Figure 2. *Internet Growth by Number of Hosts*



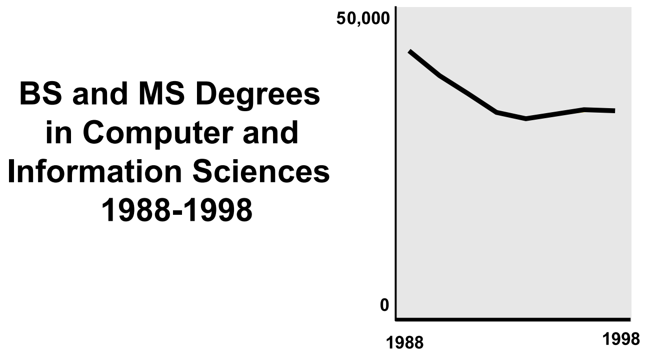


Figure 3. *Degrees in Computer and Information Sciences from 1988 to 1998*

## The Meaning of Improved Security

Improving security is hard work, even if you have had a significant attack that has gotten everyone's attention. Sustaining a desired level of security can be even harder. First, you need to identify the risks to your business if the security (confidentiality, availability, and integrity) of critical data, systems, and/or networks (assets) is compromised. By compromised, we mean that the asset has been destroyed, damaged, or altered in a way that hurts your operations, or has been revealed to your competitors.

You cannot protect everything equally, so it is important to carefully choose the data you want to protect and then plan how to do so based on its value to your organization [4].

Once you know the risks to your networked system, you need to decide which ones are most likely to occur and which would cause the largest potential impact. The impact could be measured in money, time, lost productivity, or loss of market share, customers, or reputation. After deciding on a prioritized list of risks and an effective plan to mitigate them, there is still work to be done.

Suppose that a day after you create your plan, you find out that your main competitor has just launched a new e-commerce site and is ready to do business on the Internet—and you are still six months away from launching yours. Or suppose a recently fired employee has successfully penetrated your strategic planning database and posted your plans for the next 18 months on an Internet newsgroup. In other words, change and surprises introduce new risks that must be added to the ones you are already managing.

Since the technology and business environment is highly dynamic, an organization needs mechanisms for identifying critical information assets as conditions change. You need to have a way of adjusting where you invest time and energy for improving security based on this very dynamic environment.

## Information Security Risk Assessment

Information protection decisions are often incomplete or ineffective because they are based on the organization's prior experience with vulnerabilities and current threats. While managing information security risks helps ensure that information protection strategies are appropriate, most risk assessments are incomplete, or are conducted by external consultants who have little knowledge of the organization's unique requirements. In order to address the widening gap between current risk management practice and the need for flexible, effective information protection, the Networked Systems Survivability (NSS) Program at the Software Engineering Institute (SEI) is developing a comprehensive, repeatable technique for identifying vulnerabilities in networked systems through organizational self-assessment.

This self-assessment, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE$^{SM}$)[1] [5], enables organizations to develop appropriate protection strategies by considering policy, management, administration, and other organizational issues, as well as technologies, to form a comprehensive view of the information security state of that organization. This method is a key component of an overarching security and information protection framework that allows an organization to identify and pursue an appropriate security posture.

An effective risk management strategy requires more than an assessment of the existing information infrastructure. An organization needs to understand:

- Value of the assets that must be protected.
- Consequences of loss of confidentiality or operational capability.
- Vulnerabilities that could be exploited to bring about the losses.
- Existing threats that could exploit the vulnerabilities.
- Likelihood that a threat might occur.
- Availability and appropriateness of options and resources to address risks and concerns.

The OCTAVE method is composed of three phases that provide a systematic, context-driven approach to managing information security risks, and enables an organization to assemble a comprehensive picture of their information security needs. Phase 1 identifies information assets and their values, as well as threats to those assets and the security requirements to protect them. This is accomplished using staff knowledge from multiple levels within the organization along with standard catalogs of information. This information can then be used to achieve the Phase 1 goal, which is to establish the security requirements of the enterprise.

Phase 2 examines the information assets of the organization in relation to the information infrastructure components to identify those components that are high priority. Then, staff evaluates the vulnerabilities within the infrastructure. At the conclusion of Phase 2, the organization has identified the high-priority information infrastructure components, missing policies and practices, and vulnerabilities.

Phase 3 builds on the information captured during Phases 1 and 2. Risks are identified by analyzing the assets, threats, and vulnerabilities. Estimates of impact and probability of the risks are made, and the risks are then prioritized, ultimately resulting in the development of a protection strategy and a comprehensive, enterprise-wide plan for managing information security risks.

OCTAVE has many unique features that extend its impact far beyond a comprehensive risk assessment. First, OCTAVE provides an organizing framework as well as a method that capitalizes on the abilities, practices, and mission of the organization performing the self-assessment. Thus, it helps organizations understand what current strategies and practices are working effectively. It also reveals needed improvements and gaps existing in strategy, technology, staff knowledge, and in the organization's ability to protect key information assets in a constantly changing environment.

Second, OCTAVE requires effective communication among all levels of staff and management. This is one of the long-lasting benefits.

Third, OCTAVE helps provide a clear picture of gaps in internal capabilities, thus enabling a strategy to be built that can include appropriate use of specialized, external experts. Ultimately the goal of OCTAVE is to improve how well information assets are protected, thus putting organizations in a better position to achieve their missions.

Inherent in the OCTAVE method is the assumption that an organization is already working to meet its mission objectives by using many good protection strategies. There are many practices that are commonplace; some are effective and some are not. The NSS Program continues to define technology and management practices that provide practical guidance, which will help organizations address important problems in network security.

## Recommended Security Practices

One of the most important parts of adopting recommended security practices is selecting those that will allow you to mitigate your most critical technical risks. When considering who could most benefit from pragmatic, concise, how-to guidance about security (practices), it became obvious that the audiences with the greatest need were network and system administrators and their managers. They face the most daunting challenges as a result of the growth and complexity of their IT infrastructures, which they must keep in operation around the clock, seven days a week. They are constantly being asked to add new IT systems, networks, applications, and data to keep pace with changing business and technology demands.

Based on the actions successful organizations were taking to deal with these demands, the NSS program has developed step-by-step guidance that does not rely on a particular operating system or platform. The intent was to make the information as useful as possible. In addition, the NSS program developed UNIX- and Windows NT-specific implementations for many of the practices. All of this information can be found at the CERT® Coordination Center[2] (CERT/CC) Web site on the security improvement page.[3]

Each practice contains:

- A brief description that expands the title of the practice.
- An explanation of why the practice is important (what casualties can occur if you do not implement the practice).
- A step-by-step description of how to perform the practice.
- A collection of related policy topics that support deploying the practice successfully.

As data becomes available from organizations implementing recommended security practices, the practices will also provide:

- The cost/benefit analysis information for selecting among alternative approaches, and
- The means to measure implementation success (did it solve the problem it purported to solve, and were the benefits of the investment worth the cost?).

Some of the more frequently referenced sets of practices (each set is called a module) include Preparing to Detect Signs of Intrusion, Detecting Signs of Intrusion, Responding to

Intrusions, Securing Desktop Workstations, Securing Network Servers, Securing Public Web Servers, and Deploying Firewalls. The modules contain practices such as:

- Establishing requirements, policies, and procedures.
- Establishing secure architectures and configurations.
- Identifying and installing tools.
- Setting up logging options, examining what they produce.
- Setting up user authentication and file access control mechanisms.
- Determining how to deny network traffic that you do not want coming into your system.

Many of the practices are starting to appear in training materials and are being referenced by other web sites.

## Curriculum and Certification Standards

Information systems security training at the SEI uses a variety of source material and experience in developing courses, including recommended practices and implementations. Relevant data from CERT/CC incident response and vulnerability analysis operations are used to provide current information on trends and emerging threats. CERT/CC experience in helping to foster the creation of other incident response teams around the world provides the core content for the suite of incident handling courses [7]. Research in the areas of security risk management and information survivability similarly provide core content for course development.

Comprehensive solutions for the survivability of information systems require that senior executives and managers, as well as technical staff, develop strong and diverse skills. Senior management must establish a clear sense of priority levels and appropriate policies, as well as risk-mitigation strategies, for securing various information assets. They share this guidance with technical staff responsible for the secure administration of networked systems. The first-line managers of technical staff must be able to articulate the technical implications of these decisions so cost-benefit tradeoffs can be performed.

The NSS program is in the process of developing security curricula for managers and system administrators. As a result of course development in the areas of Internet security, e.g. incident handling, secure system administration, and risk management activities, current offerings[4] include two sets of courses. One set is built around computer security response teams and incident handling. This set includes Managing Computer Security Incident Response Teams and Computer Security Incident Handling for Technical Staff [Introductory and Advanced].

The second set is built around fundamental concepts and selected practices for Internet security. This set includes Concepts and Trends in Information Security, Information Security for System Administrators, Managing Risks to Information Assets, and The Executive Role in Information Security: Risk and Survivability. Selected, tailored training courses have also been developed to accompany security improvement modules and practices for implementation at customer organizations.

Arguably, current training for system and network administrators, their managers, and users does not sufficiently address requisite knowledge, skills, and abilities for securing networked systems unless an organization has clearly identified its critical information assets and defined a set of protection strategies that guide the appropriate training. Since the technology changes rapidly, people need to update their skills frequently. Consequently, course content needs to be dynamic as well. Thus, any systematic effort to train and certify system and network administrators must account for changing technical requirements and course content.

There is a growing demand to establish a minimum set of core competencies or certification standards for system and network administrators. Several efforts are underway to address this problem. For example, the *Information Technology Security Training Requirements: A Role- and Performance-Based Model* [6] outlines an information technology security body of knowledge, topics, and concepts. Integrated Space Command and Control[5] offers the designation of Certified Information Systems Security Professional. System Administration Networks and Security[6] offers Levels 1 and 2 certification. USENIX System Administrator's Guild[7] is currently examining certification approaches and conducting job analyses to establish standards [8].

## Summary

This article described the growing problem of protecting networked systems connected to public networks such as the Internet. We presented an emerging structure for improving the security of networked systems that includes conducting an information security risk assessment, which produces a recommended set of risks to be managed and protection strategies intended to mitigate those risks. Implementing protection strategies includes adopting recommended security practices. Both assessment and practice deployment require appropriate training, which, in the future, will hopefully build upon a set of security certification standards.

We welcome your feedback and look forward to hearing about your experiences as you improve the security of your organization's networked systems and work to sustain them.◆

## References

1. Allen, Julia. *Securing Networked Systems: A Technology Improvement Process.*1999 Software Engineering Process Group Conference, Carnegie Mellon University, Software Engineering Institute, March, 1999. Available at www.cert.org/sepg99/index.htm

2 Computer Security Institute, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Issues and Trends*, Vol. VI, No. 1, (Spring 2000).

3. Pethia, Richard. *Internet Security Issues: Testimony Before the U.S. Senate Judiciary Committee.* Carnegie Mellon University, Software Engineering Institute, May 25, 2000. Available at www.cert.org/congressional_testimony/Pethia_testimony25May00.html

4 West-Brown, Moira and Allen, Julia. SEI Interactive. Pittsburgh, Pa.: Carnegie Mellon University, Software Engineering Institute, September 1999. Available at http://interactive.sei.cmu.edu/Columns/Security_Matters/1999/September/Security.sep99.pdf

5. Alberts, Christopher; Behrens, Sandra G.; Pethia, Richard D.; and Wilson, William R. *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE$^{SM}$) Framework, Version 1.0.* (CMU/SEI-00-TR-017). Pittsburgh, Pa.: Carnegie Mellon University, Software Engineering Institute, June 1999. Available at www.sei.cmu.edu/publications/documents/99.reports/99tr017/

99tr017abstract.html

6. Wilson, William, ed. *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (Publication 800-16). National Institute of Standards and Technology, U.S. Department of Commerce, 1998.
7. West-Brown, Moira J.; Stikvoort, Don; and Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams* (CMU/SEI-98-HB-001). Pittsburgh, Pa.: Carnegie Mellon University, Software Engineering Institute, 1998. Available at www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

8 Laswell, Barbara; Simmel, Derek; and Behrens, Sandra G. *Information Assurance Curriculum and Certification: State of the Practice* (CMU/SEI-99-TR-021). Pittsburgh, Pa.: Carnegie Mellon University, Software Engineering Institute, July 1999. Available at www.sei.cmu.edu/publications/documents/99.reports/99tr021/99tr021abstract.html

## Notes

1. Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.
2. CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office.
3. See www.cert.org/security-improvement
4. The current description of public offerings is available at www.sei.cmu.edu/products/courses/courses.html  
   The current schedule of public offerings is available at www.sei.cmu.edu/products/calendars/calendar.html
5. See www.isc2.org
6. See www.sans.org
7. See www.usenix.org

## About the Authors

**Julia Allen** is a senior member of the technical staff working in security improvement. She has an master's degree in electrical engineering from the University of Southern California.

**Christopher Alberts** is a member of the technical staff working in information security risk management. He has an master's degree in engineering from Carnegie Mellon University.

**Sandi Behrens** is a senior member of the technical staff working in information security risk management. She has a doctorate degree from the University of Pittsburgh with an emphasis on instructional technology and cognitive science.

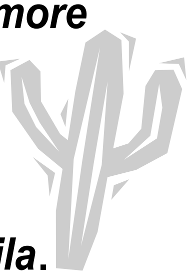
**Barbara Laswell** is the technical manager of practices development and training. She has a doctorate degree from Stanford University in the design and evaluation of educational systems.

**William Wilson** is currently managing the survivable network management team. He has a master's degree in computer systems management from the University of Maryland.

Carnegie Mellon University, Software Engineering Institute  
4500 Fifth Ave.  
Pittsburgh, Pa. 15213  
Voice: 412-268-6942  
Fax: 412-268-6989  
Email: Julia Allen: jha@sei.cmu.edu  
Christopher Alberts: cja@sei.cmu.edu  
Sandi Behrens: sgb@sei.cmu.edu  
Barbara Laswell: blaswell@sei.cmu.edu  
William Wilson: wrw@sei.cmu.edu  
Internet: http://www.sei.cmu.edu, http://www.cert.org

# Quote Marks

***Those who can, compute.***  
***Those who cannot, program.***  
***Those who can't program, write manuals.***  
***Those who can't write manuals, sell computers.***  
***- Anon.***



***A computer lets you make more mistakes faster than any invention in human history, with the possible exception of handguns and tequila.***

***Mitch Ratcliffe, "Technology Review" (1992)***

***Computer accomplishments will be of ultimately greater significance to civilizatio than those of space technology or nuclear physics.***  
***Walter F. Bauer***