

From Y2K to Security Improvement: A Critical Transition

Moira West-Brown, Julia Allen



The previous issue in this series discussed how the Internet community could better prepare to address major security incidents. In this issue I'm joined by Julia Allen, team leader for security-improvement practice development. We will compare Y2K and information technology (IT) security and suggest how your organization can build on its Y2K efforts to initiate or enhance an IT security-improvement program (SIP).

The Basis for Security Improvement

Many organizations have spent the past year preparing for the impact of Y2K. Unfortunately few of them are ready to address the risks associated with IT security incidents. The actions that must be taken to successfully deal with such incidents need to be a continuous, planned part of normal, day-to-day business operations. As in preparing for Y2K, IT security needs visible management sponsorship, investment, policies, procedures, processes, methods, tools, measures, standing teams, and assigned roles and responsibilities. This combination of people, technology, and processes is the basis for security improvement.

Y2K vs. IT Security—A Comparison

As the Y2K deadline looms ever closer, organizations find themselves in various stages of readiness for the big event. After years of work, some are still frantically attempting to complete their Y2K compliance testing, while others are preparing their crisis communications to monitor for and address Y2K failures and glitches when they do arise. However, as the new millennium dawns, organizations can expect to address more than just Y2K glitches and failures.

The tremendous energy that organizations have exerted to prepare for Y2K is understandable when you consider what is at stake. However, the risks associated with suffering an IT security incident or security breach can be just as devastating as those associated with Y2K non-compliance. Recent figures provided in the 1999 CSI/FBI computer crime survey indicate that the greatest losses from IT security incidents are associated with theft of proprietary information and financial fraud. But the survey also

points out that many organizations are unable to quantify losses from incidents. All too often organizations either don't know what information may have been lost or don't have processes in place to help determine how to quantify loss. For instance, what is the cost to an organization of losing its Internet connectivity for five hours?

Moreover, organizations may naively believe that IT security is under control if they have some security measures in place—such as

- a firewall to keep out intruders
- investment in PKI (public key infrastructure), VPN (virtual private network), or e-commerce solutions
- an IDS (Intrusion Detection System) to detect, alert, and possibly respond to intrusions
- strong authentication using technologies such as one-time passwords and smart cards

It is important to recognize that mitigating IT security risks is a complex issue that can neither be addressed overnight nor through technological solutions alone.

A survey by the SANS Institute of 1,850 computer-security experts and managers identified “Seven Top Management Errors that Lead to Computer Security Vulnerabilities.”

For some time, computer-security experts have warned of the possibility of intruders using the chaos and confusion of Y2K as a smokescreen under which they can camouflage attacks and other malicious activities. Recently the Gartner Group has asserted the potential for someone to steal up to \$1 billion during the Y2K chaos by installing back doors in software during Y2K compliance changes.

Unlike Y2K—fixing a one-off issue at a known time in the future—IT security incidents are a reality now, occur on a daily basis, and may prove at least as catastrophic for a company as Y2K. Keeping pace with changing business and technology demands results in dynamic IT environments with ongoing changes to platforms, tools, technologies, staff and policies. Keeping pace is difficult enough from a Y2K perspective; an IT-security perspective adds additional levels of complexity to the problem and correspondingly increases risk.

Although the risks of Y2K and IT security to an organization are comparable, recognition of this is not reflected in the associated level of investment needed to address these risks. No one knows the real global cost of Y2K, but figures available in the U.S. give an indication of the magnitude of the investment that companies are making to address this one-off event. Organizations have invested and continue to invest significant sums in their Y2K compliance efforts. In July 1999, for example, U.S. and Canadian airlines reported that their combined Y2K efforts totaled more than \$750 million. In December

1999, the total reported Y2K costs for U.S. federal agencies will reach over \$6.4 billion. Even considering the enormous sums reported, some experts claim that organizations are underreporting their real Y2K costs so as not to reduce customer confidence.

Figures on investment in IT security improvement are more difficult to obtain, but the little information that is available would indicate that global IT security investment is embarrassingly small in comparison with Y2K budgets. The Gartner Group estimates that most organizations spend as little as 1% of their operating costs on security when 5–8% is what is necessary. In a 1999 survey, *Information Week* showed that approximately 50% of information security professionals had an IT security budget of \$50,000 or less.

Y2K and security improvement are corporate-wide issues that could have serious repercussions if not adequately addressed. Just as with Y2K, launching and sustaining a successful security-improvement program requires visible advocacy by senior management, funding, follow-through, and long-term commitment of resources.

Initiating a Security Improvement Program

Initiating a security improvement program (SIP) is hard work, even if you've had a significant attack that has gotten everyone's attention. Sustaining an SIP 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, altered so as to hurt your operations, or revealed to your competitors. You can't protect everything equally so it is important to carefully select what you do choose to protect and how, based on its value to your organization.

Once you know your risks, you need to decide which ones are most likely to occur and have the largest potential impact. Impact could be in dollars, time, lost productivity, or loss of market share, customers, and reputation. But the work doesn't end there. Let's say you have a prioritized list of risks and an effective plan to mitigate them. The next day, you go into the office and find out your number one competitor has just launched a new e-commerce site and is ready to do business on the Internet—and you're still six months away from launching yours. Or a recently fired employee has successfully penetrated your strategic planning database and posted your plans for the next 18 months on an Internet news group. In other words, change and surprises introduce new risks that must be added to the ones you are already managing. And you need to have a way of adjusting where you invest SIP time and energy based on this very dynamic environment.

In concert with the CERT/CC® community and several leading government and commercial organizations, we have spent some time thinking about how to launch an

SIP¹. One of the key components of an SIP is the definition and adoption of improved security practices that will allow you to mitigate your most critical technical risks.

When considering who could most benefit from pragmatic, concise, how-to guidance on what to do (practices), it became obvious that one of the audiences with the greatest need was network and system administrators and their managers. They face the most daunting challenges as a result of the growth and complexity of the IT infrastructures they are responsible for keeping up and running 24 hours a day, seven days a week. And 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 what successful organizations were doing to deal with these demands, we developed specific step-by-step guidance that did not rely on a particular operating system or platform, making the information as broadly useful as possible. In addition, UNIX- and Windows NT-specific “implementations” for many of the practices have been developed. All of this information can be found on the [CERT security improvement Web site](#).

Each practice contains

- a brief description that expands the title of the practice
- an explanation of why the practice is important (what bad things can happen if you don't do it)
- a step-by-step description of how to perform the practice
- related policy topics that support successfully deploying the practice

Planned future additions include

- cost/benefit analysis information for selecting among alternative approaches
- the means by which to measure success of implementation (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](#), and [Deploying Firewalls](#). The modules contain practices such as identifying and installing tools, setting up logging options and examining what they produce, setting up user authentication and file access control mechanisms, and determining how to deny network traffic that you don't want coming into your system.

(Many of the practices are starting to appear in training materials and are being referenced by other Web sites. We don't have any feedback yet on how organizations are

¹ See our [1999 SEPG presentation on Securing Networked Systems](#)

using them but we would love to hear from you if you are. We are launching our first significant set of pilot tests this year. So stay tuned and watch for new materials.)

Transitioning Y2K Resources

As Y2K efforts wind down and resources associated with them free up, many projects that have been on hold or have been placed on the back burner will be competing for those resources. It is important to plan for the future now and ensure that IT security improvement is a major focus of those plans. In addition to redirecting Y2K resources to other development projects, this is an excellent opportunity to transition some of those resources to the formation of an SIP effort and to supplement these resources with IT-security expertise. This approach is preferable to resourcing SIP from scratch, as the people coordinating Y2K efforts in organizations are likely to be familiar with many of the issues that you need to address for SIP including

- establishing a crisis center
- a good understanding of the nature and level of risk across the organization
- identifying critical resources
- establishing contacts across business units

Some organizations are already considering this approach².

Security improvement won't happen overnight; it will result from an ongoing effort. Organizations need to be prepared to address IT-security incidents every day. However, every organization should also consider the heightened possibility of security incidents coinciding with Y2K. We encourage you to alert your Y2K crisis center to be prepared for possible security problems disguised as Y2K issues or anomalies that may coincide with apparent Y2K problems. Have IT security staff on alert to address any such issues as they arise.

Many organizations scrambled to address the Melissa macro virus incident earlier this year. Some have indicated that they were in some way thankful for the experience Melissa gave them as they were then better prepared when the potentially more severe explore.zip worm struck just months later. Organizations should take little solace from such news—clearly this is not an effective or appropriate way to address security risks. Y2K has taught us that having a deadline to shoot for can help us to focus our attention and make significant progress toward addressing a major problem. We don't deny that

² See recent issues of *Federal Computer Week* articles ([Y2K](#) and the [CIO Council](#)).

security improvement is a much more complex and difficult nut to crack than Y2K. However, to retain control of corporate assets and continue to enhance the nature of the business conducted on the network while maintaining customer confidence, we must tackle security improvement head-on.

About the Authors

Moira J. West-Brown is a senior member of the technical staff within the CERT® Coordination Center, based at the SEI, where she leads a group responsible for facilitating and assisting the formation of new computer security incident response teams (CSIRTs) around the globe. Before coming to the CERT/CC in 1991, West-Brown had extensive experience in system administration, software development, and user support/liaison, gained at a variety of companies ranging from academic institutions and industrial software consultancies to government-funded research programs. She is an active figure in the international CSIRT community and has developed a variety of tutorial and workshop materials focusing mainly on operational and collaborative CSIRT issues. She was elected to the Forum of Incident Response and Security Teams Steering Committee in 1995 and is currently the Steering Committee Chair. She holds a first-class bachelor's degree in computational science from the University of Hull, UK.

Julia Allen has more than 25 years of managerial and technical experience in software engineering. She is currently a senior member of the technical staff within the Networked Systems Survivability Program at the Software Engineering Institute, leading the team responsible for developing security improvement practices. Prior to this technical assignment, Allen served as acting director of the SEI for an interim period of six months as well as deputy director for three years. She started the Industry Customer Sector at the SEI in 1992. Before joining the SEI, Allen was vice president at Science Applications International Corp., and was responsible for starting a new software division specializing in embedded systems software for government customers. Before that, she worked for 10 years with TRW. Allen received a BS in Computer Science from the University of Michigan, as well as an MS from the University of Southern California and an executive business certificate from the University of California at Los Angeles. Her professional affiliations include ACM, IEEE Computer Society, and the Internet Society (ISOC). Her publications include four modules within the SEI's security improvement series as well as various presentations and papers on the SEI's strategic plan and technical program.

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

® CMM, Capability Maturity Model, Capability Maturity Modeling, CERT, and CERT Coordination Center are registered in the U.S. Patent and Trademark Office.

SM ATAM, Architecture Tradeoff Analysis Method, CMMI, CMM Integration, IDEAL, Interim Profile, Personal Software Process, PSP, SCE, Simplex, Team Software Process, and TSP are service marks of Carnegie Mellon University.