

Information Security: An Executive Primer

Defending Critical Information Assets From Cyber-Criminals

Stan Stahl, Ph.D.
President & Chief Security Officer
Citadel Information Group, Inc.

© Copyright 2001. Citadel Information Group, Inc. All Rights Reserved.

The Executive Challenge

Your organization's information systems are under attack.

According to the 2001 FBI Computer Crime and Security Survey¹, 40% of surveyed companies reported that their systems had been penetrated from the outside, 91% reported employee abuse problems, and 94% reported problems with computer viruses.

- *Egghead.com*: Web site hacked and 3.5 million customers warned that their financial information may have been compromised²
- *University of Wisconsin Medical Center*: Health system database is hacked and 5,000 patient records are stolen³
- *Microsoft, CNN, Buy.com, eBay, ZDNet.com, E*Trade, Amazon, National Discount Brokers and Federal Bureau of Investigation*: Web sites shut down by hackers^{4 5}
- *Network Associates*: Security firm web site defaced⁶
- *Microsoft Corporation*: Source code stolen for software product under development⁷
- *US Navy*: Source code for missile guidance system stolen⁸
- *Code Red Worm*: Infects over 350,000 computers⁹

If you came home one evening and discovered the doors and windows of your house open, you wouldn't wait for someone to steal your TV before taking action. First, you'd rant and rave, maybe even cuss some. Then you'd lock up your house. The next morning you'd begin implementing appropriate policies and procedures to make certain this never happened again. You might invest in a new electronic security system that would notify a security patrol if a door or window was opened and, if you had expensive art or jewelry, you might even invest in a monitoring system allowing your security patrol to remotely monitor the house.

The doors and windows to your computer and information systems are open.

Not only are your systems under attack with their doors and windows wide open, but you've got the corporate crown jewels sitting right there in your information systems ... in your open information systems ... the ones that are under attack.

¹ *Computer Security Issues & Trends*, Computer Security Institute, Spring 2001.

² *Online Retailer Egghead.com Hacked*, AP Online, December 22, 2000

³ *Hospital Confirms Hacker Stole 5,000 Patient Files*, Computerworld, December 18, 2000

⁴ ABC News, <http://www.abcnews.go.com/sections/tech/DailyNews/webattacks000210.html>, February 10, 2000

⁵ ABC News, <http://www.abcnews.go.com/sections/tech/DailyNews/webattacks000225.html>, February 25, 2000.

⁶ *Security Firm's Site Defaced*, Wired News, November 30, 2000

⁷ *Microsoft Infiltrated By Hackers*, Washington Post, October 28, 2000

⁸ *Hackers Heist Navy's Missile Codes*. New York Post, March 3, 2001

⁹ *Return of "Computer Worm" Feared Today*, New York Times, July 31, 2001

- What could it cost your company if a cyber-criminal surreptitiously set himself up as a phantom supplier? How long might this go on with no one knowing?
- What if a hacker destroyed critical sales information?
- What if a key department couldn't function for a day while computer viruses were being removed from computers?
- What if an angry employee changed critical parameters in one of your process control systems?
- What could it cost you—in dollars and in good will—if your information systems were surreptitiously commandeered and used to steal money from one of your key customers?
- What if information you are required by law to keep private or confidential becomes public?
- What if you're sued by shareholders claiming management negligence led to one of these problems

Houston ... We have a problem.

Protecting critical information assets is a serious challenge, not so much because the probability of catastrophe is high, but because the consequences of catastrophe are potentially huge.

It's a challenge that you—as an executive responsible for the well-being of your organization—must take responsibility for.

Fortunately, it's a problem that is amenable to management attention.

The rest of this article explains how.

The Standard of Defense

Forget trying to keep all your information assets 100% secure. It can't be done. And even if it could, it wouldn't be worth the cost. The goal of information security is much more modest.

The goal of your organization's information security program is to cost-effectively provide the appropriate degree of security to critical information assets.

Fundamental to this goal is the (obvious) recognition that some information is more valuable than other. Your next quarter marketing plans, for example, are (hopefully) a great deal more valuable than the driving directions to the company picnic.

Your organization's information security program is effective to the extent ¹⁰

¹⁰ Definition adapted from *Internet Security Glossary*, R. Shirey, Network Working Group, Request for Comments 2828, <ftp://ftp.isi.edu/in-notes/rfc2828.txt>, May 2000

- It enables you to **prevent** unauthorized or accidental access, change, destruction, transmission, loss, or use of critical information assets
- It enables you to **detect** potential unauthorized or accidental access, change, destruction, transmission, loss, or use of critical information assets and can be used to identify and investigate such events
- It enables you to **recover** from and the limit the damage caused by unauthorized or accidental access, change, destruction, transmission, loss, or use of critical information assets
- It enables you to protect information system assets so as to appropriately **comply** with laws, regulations, and contractual agreements ¹¹

Information security is concerned with the protection of *information assets*. As such, the effectiveness of an organization’s information security strategy is dependent on how well that strategy is integrated into—and made a part of—the overall strategy by which the organization manages its information assets.

While it is our networked computer systems that create modern opportunities for security warfare and even though technology solutions are a key ingredient to an effective security posture, information security is, first and foremost, a senior management responsibility and, second, a technology function. Where information security is concerned, management is the ‘horse;’ technology is the ‘cart.’ And we all know the danger of putting the cart before the horse.

The Logic of Information Security

Protecting critical information assets deals with four issues: *risks, threats, vulnerabilities* and *countermeasures*. The relationship between these variables is described by the “*Fundamental Equation of Information Security*”¹².

$$\text{Residual Risk} = \frac{\text{Threats} * \text{Vulnerabilities}}{\text{Countermeasures}}$$

Risks to Critical Information Assets

Risk can be viewed as the expectation that a particular threat will exploit a particular vulnerability with a particular harmful result.”

Typical risks to your information assets include such security incidents as:

- Theft of money, inventory, equipment, etc.

¹¹ Such as, for example, HIPAA and Gramm-Leach-Bliley

¹² *Fundamental Elements of Information Security*, F. Quigley, S. Stahl, TRW, 1987

- Unauthorized changes to personnel and other records
- External release of proprietary records, customer-private information, planning information, etc.
- Inability of employees to access and use information and information systems
- Illegitimate use of system resources, such as pirating software, downloading pornography, or inappropriate use of e-mail systems
- Use of your computer systems as a 'jumping-off point' for a 3rd-party *denial of service* attack
- Harmful consequences of a security incident, such as law suits or unpleasant publicity

Note that harmful results may be the consequence of deliberate action or of accident. It is the result that matters, not the deliberateness of its cause.

Threats to Critical Information Assets

A *threat* is “a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.”¹³

Managing information security requires managing two different, but related, categories of threat: *Threat Agents* and *Threat Consequences*.

Threats are carried out by *threat agents*. Threat agents may be physical: employees, hackers, criminals, espionage agents, etc.. Threat agents may also be 'virtual:' viruses, worms, trojan horses, attack scripts, etc. Indeed, it is these virtual threats that have the potential to do the greatest harm; imagine, for example, a computer program whose only function is to steal secrets from your organization's computers.

There are four categories of *threat consequences*¹⁴:

- **Unauthorized Disclosure:** A circumstance or event whereby an entity gains access to data for which the entity is not authorized, as, for example, when a hacker accesses the confidential client records of a law firm
- **Deception:** A circumstance or event that may result in an authorized entity receiving false data and believing it to be true, as, for example, when a criminal surreptitiously changes your accounts payable data so as to induce your finance department to cut him a check

¹³ *Internet Security Glossary*, R. Shirey, Network Working Group, Request for Comments 2828, <ftp://ftp.isi.edu/in-notes/rfc2828.txt>, May 2000

¹⁴ *Internet Security Glossary*, *op cit*

- **Disruption:** A circumstance or event that interrupts or prevents the correct operation of system services and functions, as, for example, through a denial of service attack like those that were recently launched against the White House
- **Usurpation:** A circumstance or event that results in control of system services or functions by an unauthorized entity, as, for example, occurred when more than 225,000 computers were used to launch a denial of service attack against the White House ¹⁵

Information System Vulnerabilities

*A vulnerability is a flaw or weakness that an enemy might exploit to cause harm to your organization.*¹⁶

Information system security vulnerabilities fall into two broad categories: management vulnerabilities and technology vulnerabilities.

Areas in which management structures are often vulnerable include

- Organizational accountability and responsibility; with inadequate management responsibility, controls are easily bypassed
- Individual accountability and responsibility; if employees don't have responsibility for their security actions, they will put their energies elsewhere
- Policies and procedures; if the organization doesn't have effective policies and procedures, it won't know what to do when attack threatens
- Security awareness, training and education; if employees aren't given appropriate training and education, how can they be expected to be responsible and follow procedures
- Contingency and emergency plans; without effective contingency and emergency plans, the impact will be more serious, recovery will be slower, and the cost greater

Technology vulnerabilities include

- Physical security vulnerabilities, including access to offices and equipment
- Computer and network operating system flaws
- Application software flaws
- Inherent access flaws; particularly security flaws inherent to computer networking and the internet

¹⁵ *Hackers Try to Shut Down White House Web Site, but Security Foils Their Attack* , Los Angeles Times, July 20, 2001

¹⁶ This definition expands upon the one in the *Internet Security Glossary* in that the *Glossary's* definition focuses attention exclusively on information system vulnerabilities

Available Countermeasures

Countermeasures are actions, devices, procedures, or techniques that reduce a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. ¹⁷

The following table illustrates the range of countermeasures available to management, indicating the security objective(s) of each.

Countermeasure	Prevent	Detect	Recover	Comply
Security Assessment	XXX	XXX		
Vulnerability Analysis & Penetration Testing	XXX	XXX		
Network Monitoring Services		XXX		
Intrusion Detection Systems		XXX		
Security Integration (Firewalls, Virus Control, Encryption, etc.)	XXX	XXX	XXX	XXX
Security Management (Organization, Policies, Training, etc.)	XXX	XXX	XXX	XXX
Physical Security	XXX	XXX		
Contingency Planning & Preparation			XXX	
Remediation Services (including, .e.g., <i>Patch Services</i>)	XXX	XXX	XXX	
Cyber-Surveillance		XXX		
Security Forensics			XXX	
Compliance Audit / Review	XXX	XXX		XXX

The next table indicates the extent to which the countermeasure is (primarily) a management or a technology one. This table, showing that fully 50% of countermeasures are management-focused, should remove any lingering doubt about the need for executive management to get involved with security.

Countermeasure	Management	Technology
Security Assessment	XXX	XXX
Vulnerability Analysis & Penetration Testing	XXX	XXX
Network Monitoring Services		XXX
Intrusion Detection Systems		XXX

¹⁷ *Internet Security Glossary, op cit*

Security Integration		XXX
Security Management	XXX	
Physical Security	XXX	XXX
Contingency Planning & Preparation	XXX	XXX
Remediation Services		XXX
Cyber-Surveillance		XXX
Security Forensics		XXX
Compliance Audit / Review	XXX	XXX

Six Action Steps for Managing the Information Warfare Challenge

In the *2001 FBI Computer Crime and Security Survey*,¹⁸ Patrice Rapalus, Director of the *Computer Security Institute*, writes

Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions. They also need to properly fund, train, staff and empower those tasked with enterprise-wide information security.

Achieving this “comprehensive approach” means accomplishing the following six action steps.

1. Personally accept that ultimate responsibility for the cost-effective management of the security of critical corporate information assets rests with you and your executive management team
2. Lead your management team in meeting its responsibility by (i) formalizing your organization’s information security program, including its security policies, (ii) providing the resources for carrying out the program, and (iii) creating the organizational culture and management infrastructure required to support the program
3. Require that all personnel be provided with awareness training and education in the organization’s information security program. Everyone must understand the challenges of security and their responsibility for assuring it.
4. Insist that details of implementing the security program be jointly determined by those who own and use information together with the IT personnel who provide and maintain the computer and communication systems on which information is stored, used, manipulated and transmitted. Their combined objective is to cost-effectively meet the real-world needs, goals

¹⁸ *Computer Security Issues & Trends*, Computer Security Institute, Spring 2001.

and objectives of users and IT personnel in a way that is consistent with the goals you, as executive management, have established.

5. Require IT personnel to adopt and apply appropriate “best security practices.” These must include (i) developing and maintaining a well-defined security architecture, (ii) establishing and enforcing clear security controls on system, personnel and other appropriate changes, (iii) tracking and implementing all security alert bulletins, (iv) staying current with, and applying, as appropriate, evolving “best practices.”
6. Trust ... but verify. Get regular ongoing objective feedback on the quality of your information security program through independent security assessments, vulnerability analysis and penetration testing, and compliance reviews and audits.

Summary

Your information systems are at risk. Threats are real and the likelihood is high that you are vulnerable. As a key executive, it is your responsibility to see to it that your organization effectively manages its security risk. The leverage you have lies in the countermeasures you employ. You must employ both management and technical countermeasure; neither alone is adequate. For greatest assurance, consider an objective 3rd-party assessment and review from an independent information security specialist.



Citadel Information Group ... Securing the critical information assets of middle market businesses, mid-sized government agencies, and the non-profit community.

To schedule a free no-obligation *Information Security Executive Briefing* or for additional information, please contact:

Kimberly A. Pease
VP / Sales & Marketing
323.397.5752
kpease@citadel-information.com