



**INTERNET  
SECURITY  
ALLIANCE**

## **COMMON SENSE GUIDE FOR SENIOR MANAGERS**

Top Ten Recommended  
Information Security Practices

1st Edition - July 2002

## Internet Security Alliance Officers

**Dr. Bill Hancock** | Chairman, ISAlliance | Vice President, Security and Chief Security Officer | Exodus, A Cable & Wireless Service

**Allan Woods** | Immediate Past Chairman, ISAlliance | Vice Chairman and Chief Information Officer, Mellon Financial Corporation

**Doug Goodall** | Vice Chairman, ISAlliance | Chief Executive Officer, RedSiren Technologies

**John Shaughnessy** | Vice Chairman, ISAlliance | Senior Vice President, Visa, U.S.A.

**Dave McCurdy** | Executive Director, ISAlliance | President, Electronic Industries Alliance

**Dr. Steve Cross** | Deputy Executive Director, ISAlliance | Director, Software Engineering Institute, Carnegie Mellon University

## Internet Security Alliance Sponsors

American International Group (AIG)  
Booz Allen Hamilton  
Ceridian  
Exodus, A Cable & Wireless Service  
Frank Russell Company  
IBM Corporation  
ITT Industries  
Mellon Financial Corporation  
National Association of Manufacturers (NAM)  
Nasdaq

Norsk Tipping  
Nortel Networks  
Raytheon Company  
The Redleaf Group  
Sony Corporation  
SINTEF  
TATA Consulting Services  
TRW, Inc.  
Verisign, Inc.  
Visa, U.S.A.

# Contents

ii	<b>Introduction</b>
1	Practice #1: <b>General Management</b>
2	Practice #2: <b>Policy</b>
3	Practice #3: <b>Risk Management</b>
5	Practice #4: <b>Security Architecture &amp; Design</b>
6	Practice #5: <b>User Issues</b>
8	Practice #6: <b>System &amp; Network Management</b>
12	Practice #7: <b>Authentication &amp; Authorization</b>
15	Practice #8: <b>Monitor &amp; Audit</b>
17	Practice #9: <b>Physical Security</b>
18	Practice #10: <b>Continuity Planning &amp; Disaster Recovery</b>
19	<b>References</b>
20	<b>End Note</b>

# *Common sense ain't common.*

Will Rogers (1879-1935)

## INTRODUCTION

Over the past few months, several surveys have indicated that the challenges associated with information assurance and computer security are far from resolved. Attacks via the Internet are on the rise and the sophistication of these attacks continues to escalate at alarming levels. A recent Computer Security Institute (CSI)/FBI survey [8] polled computer security practitioners in large corporations and U.S. government agencies and found that 90 percent of respondents detected security breaches within the last 12 months. In addition, 80 percent acknowledged financial losses due to security breaches. These losses amounted to billions of dollars in lost revenue on a worldwide scale including costs associated with clean-up, loss of data, liability, and loss of customer confidence.

Today, organizations are coping with a barrage of intrusions and losses on a daily basis. Organizations strive for enterprise survivability as they attempt to manage risk in a more effective way. They must learn that security is not a one-time activity but rather a continuous, risk-managed process. An effective security process examines all aspects of operations and assets by one principle and one principle alone: information survivability.

The Internet Security Alliance (ISAlliance) was created in April 2001 to provide a forum for information sharing and thought leadership on information security issues. It represents industry's interest before legislators and regulators. It aims to identify and standardize best practices in Internet security and information survivability. It creates a collaborative environment to develop and implement information security solutions. The alliance is a collaborative effort among Carnegie Mellon University's Software Engineering Institute (SEI); its CERT® Coordination Center (CERT®/CC); the Electronic Industries Alliance (EIA), a federation of trade associations; and private and public member corporations.

The ISAlliance mission has always been clearly defined:

*To use the collective experience of the members of the Internet Security Alliance to promote sound information security practices, policies, and technologies that enhance the security of the Internet and global information systems.*

With this purpose and mission in mind, the ISAlliance created the Best Practices Working Group (BPWG) to develop, identify, promulgate, and encourage adoption of commonly accepted, good security practices. The BPWG identified 10 of the highest priority and most frequently recommended security practices as a place to start for today's operational systems. These practices address dimensions of information security such as policy, process, people, and technology, all of which are necessary for deployment of a successful security process. This initial set of practices is targeted toward executive leadership in industry. When adopted, these practices catalyze a risk-management-based approach to ensuring the survivability and security of critical information assets.

The BPWG structured the practices as a series of active statements followed by candidate questions that senior managers can ask to determine the presence, absence, and degree of implementation of the practices in their organizations. Some practices have multiple parts. The working group concluded each practice by mapping it to specific sections of industry-accepted references (see References, p. 19).

Practices #1, #2, and #3 establish the business context and decision-making guidelines for subsequent practices.

The BPWG is far from finished with its work. As technology changes, this publication must reflect the increasing challenges of ever-changing technology and greater sophistication in information security and data protection. This is an ongoing process, which the working group feels is a responsible call to action in today's high stakes, globally interconnected economy.

Please feel free to use and share this information. Through sharing and adopting commonly accepted, good security practices, all organizations can begin to successfully manage their security risks.

Kevin M. Nixon CISSP  
Chair

Julia H. Allen  
Vice-Chair

Best Practices Working Group  
Internet Security Alliance  
<http://www.isalliance.org>

**PRACTICE #1:**

# General Management

Managers throughout the organization consider information security a normal part of their responsibility and the responsibility of every employee.

Managers clearly define and assign information security roles and responsibilities and ensure adequate resources are allocated to fulfill these.

Manager actions include visible sponsorship and direction, written communications, and staff meeting time on this subject.

Managers create, enforce, and regularly review security policy. (See Practice #2.)



Questions for enterprise leaders, senior managers, and oversight boards

- Has senior management, including the corporate or organizational board of directors, established an appropriate information and Internet security policy and an auditing process?
- Is security viewed as an overhead activity or essential to business survivability? Are security considerations a routine part of your normal business processes?
- Are there legal or regulatory requirements that you should be complying with because of either contract commitments or the industry sector in which you operate?
- Do managers at each level of the organization understand their roles and responsibilities with respect to information security? How do you verify that? Do you understand your role?

**Mapping to references:**

- [1] SP3: Security Management; SP4: Security Policies and Regulations
- [2] 3: Security Policy; 4: Organizational Security; 12: Compliance
- [3] 3: Security Management Practices
- [4] SM11: Management Commitment; SM12: Security Policy; SM21 High-Level Control; SM32: Ownership

*One of the tests of leadership is the ability to recognize a problem before it becomes an emergency.*

Arnold Glasgow (1908-1970)

## PRACTICE #2:

# Policy

Develop, deploy, review, and enforce security policies that satisfy business objectives.

Create policies that address key security topic areas such as security risk management, critical asset identification, physical security, system and network management, authentication and authorization, access control, vulnerability management, incident management, awareness and training, and privacy. (For additional policy topic areas, see [1].)

Ensure that the intent of each policy is reflected in standards, procedures, practices, training, and security architectures that implement it.



Questions for enterprise leaders, senior managers, and oversight boards

- What are your organization's most important security policies—and what business objectives do they help satisfy?
- What is your role in ensuring that security policies are followed?
- What are the consequences for non-compliance?
- Is there potential liability for not exercising an appropriate standard of due care?
- If you are a publicly traded company and conduct business on the Internet, are risks to e-commerce revenues reported in annual SEC filings as required by law?

### Mapping to references:

- [1] SP2: Security Strategy; SP4: Security Policies and Regulations
- [2] 3: Security Policy; 4: Organizational Security; 9: Access Control; 12: Compliance
- [3] 3: Security Management Practices; 9: Laws, Investigations, and Ethics
- [4] SM12: Security Policy; SM13 Personnel Policies; SM41: Standards/Procedures; SM43: Data Privacy; IP41: Access Control Policies
- [5] Appendix B: Practice-Level Policy Considerations
- [6] 11: Implement an Information Security Policy

### PRACTICE #3:

# Risk Management

Periodically conduct an information security risk evaluation that identifies critical information assets (e.g., systems, networks, data), threats to critical assets, asset vulnerabilities, and risks.

Identify the adverse impacts when risks to critical assets are realized including financial, reputation, market position, time/productivity, etc. Quantify the financial impact to the greatest extent possible.

Develop and implement a risk mitigation plan resulting from the evaluation (update as needed).

Ensure that there is regular review and management of the risks to critical information assets.



Questions for enterprise leaders, senior managers, and oversight boards

- How does your organization identify critical information assets and risks to those assets?
- Are there any critical assets for which you are responsible?
- Is the frequency and scope of your risk evaluation sufficient to take evolving threats into account?
- Are risks to critical assets managed in a similar fashion to other key business risks? Are all critical assets reviewed in an annual SAS70 external audit?
- What are the potential financial impacts of a successful attack against these assets?
- Do you have adequate insurance policies such as cyber insurance<sup>1</sup> or Internet errors and omissions to mitigate and transfer potential losses for your information security risks?

#### Mapping to references:

[1] SP3: Security Management

[2] Introduction

[3] 3: Security Management Practices

[4] SM31: Security Classification; SM33 Risk Analysis; CB22: Risk Analysis; IP64: Risk Analysis; CN44: Risk Analysis

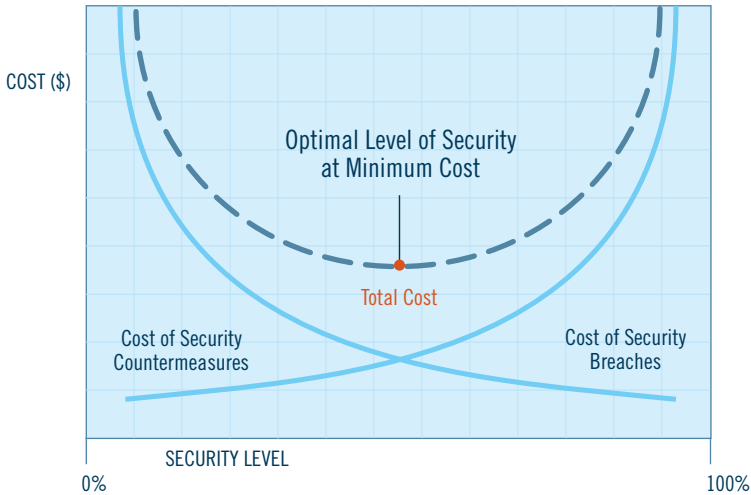
<sup>1</sup>Cyber insurance is a “stand-alone” speciality insurance policy which provides both first and third party coverage for claims arising from network security failures, cyber-extortion, web content intellectual property infringement, as well as direct loss from intangible property damage and Internet business interruption. Internet errors and omissions (E&O) is a narrower form of the policy that provides E&O liability coverage only.

# In cases of defense 'tis best to weigh the enemy more mighty than he seems.

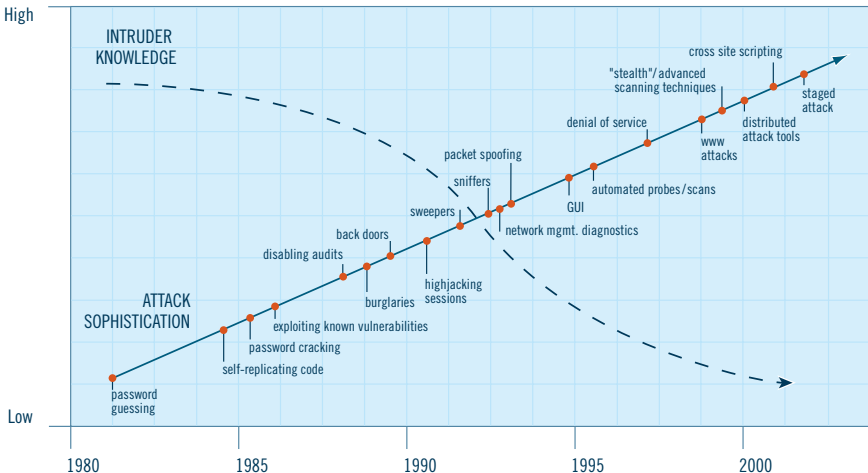
William Shakespeare  
(1564-1616)

**Balance the cost of security investment with the losses due to security breaches to match enterprise tolerance for risk.**

*Data from Dr. William M. Hancock, Exodus, A Cable and Wireless Service*



**Increases in the sophistication of attack tools requires decreasing intruder technical knowledge.** *Source: CERT® Coordination Center*



**PRACTICE #4:**

# Security Architecture & Design

Generate, implement, and maintain an enterprise- (or site-) wide security architecture, based on satisfying business objectives and protecting the most critical information assets.

Deploy a layered approach (i.e., network, host, application, data) including the practices that follow.

Use diversity and redundancy solutions (power supplies, telecommunications, hardware, operating systems, applications) for high risk/high reliance systems.



Questions for enterprise leaders, senior managers, and oversight boards

- What are the primary components of your organization's security architecture? Does your due diligence and due care process include reviews of outsourced resources?
- What business objectives does your security architecture help satisfy?
- Do you have a process to determine the security impact of linking new systems to your enterprise-wide architecture?
- What assets are most securely protected and why? What are the five most critical business functions that depend on these assets?
- If you don't know, whom do you ask?

**Mapping to references:**

- [1] SP2: Security Strategy; OP2.7: Security Architecture and Design
- [2] 9: Access Control
- [3] 6: Security Architecture and Models
- [4] SM42: Security Architecture
- [5] 1: Introduction

**PRACTICE #5.1:**

# User Issues:

## Accountability and Training

Establish accountability for user actions, train for accountability and enforce it, as reflected in organizational policies and procedures. Users include all those who have active accounts such as employees, partners, suppliers, and vendors.

All users consider information security to be a normal part of their day-to-day responsibilities.

Prior to receiving an account, users receive training in all policy topics such as password selection and protection, file access permissions, expectations of privacy, safe Web browsing, and social engineering.

Users receive training in consequences and sanctions related to policy violations including legal ramifications.



Questions for enterprise leaders, senior managers, and oversight boards

- When was the last time you and other senior managers, including your board, received a briefing or attended user training on information security as practiced in your organization?
- Is your corporate audit function included in security policy and practices reviews? Is there an auditable process with defined exception policies to limit the corporation's liability if an employee uses computing resources for malicious or illegal purposes?
- What are your responsibilities to ensure that these practices are followed?

**Mapping to references:**

- [1] SP1: Security Awareness and Training; SP4: Security Policies and Regulations; OP3.2: General Staff Practices
- [2] 6: Personnel Security
- [3] 3: Security Management Practices
- [4] SM24: Security Awareness; SM25: Security Education; CB43: User Awareness; CN42: Security Awareness; IP43: User Authorization; IP62: Security Awareness
- [5] Appendix B: Practice-Level Policy Considerations

**PRACTICE #5.2:**

## **User Issues:**

# **Adequate Expertise**

Ensure that there is adequate in-house expertise or explicitly outsourced expertise for all supported technologies (e.g., host and network operating systems, routers, firewalls, monitoring tools, and applications software), including the secure operation of those technologies.



Questions for enterprise leaders, senior managers, and oversight boards

- Whom do you call when you have problems with your operating system, laptop, access to new project data, passwords, security applications, or custom applications that have been developed in house?
- Whom do you call when your corporate firewall blocks access to a service that you need?

**Mapping to references:**

[1] SP1: Security Awareness and Training

[4] SM25: Security Education

*A chain is only as strong as its weakest link.*

Proverb

**PRACTICE #6.1:**

# System & Network Management: Access Control

Establish a range of security controls to protect assets residing on systems and networks.

Use access controls at network-, system-, file-, and application-levels as required.

Use data encryption and virtual private network technologies as required.

Use perimeter and internal security applications (including firewalls) that implement security policy.

Use removable storage media for critical data so that it can be physically secured.

Deploy a system discard process that eradicates all data from disks and memory prior to disposal.



Questions for enterprise leaders, senior managers, and oversight boards

- How do you ensure that each employee only has access to the files, directories, and applications commensurate with their job responsibilities and their need to know? How often are permissions reviewed for appropriateness and accuracy?
- How do you create a public/private key pair to encrypt sensitive information?
- How do you share your public key with others and how do they share their keys with you?

**Mapping to references:**

- [1] OP2.1: System and Network Management; OP2.6: Encryption
- [2] 5: Asset Classification and Control; 7: Physical and Environmental Security; 8: Communications and Operations Management; 9: Access Control; 10: System Development and Maintenance
- [3] 1: Access Control Systems and Methodology; 2: Telecommunications and Network Security; 5: Cryptography; 7: Computer Operations Security
- [4] SM52: Use of Cryptography; CB41 Access Control; IP32: Handling Computer Media; CN22: Traffic Filtering
- [5] 2: Securing Network Servers and User Workstations; 3: Securing Public Web Servers; 4: Deploying Firewalls
- [6] 1: Install and maintain working firewall to protect data; 3: Encrypt stored data accessible from Internet; 4: Encrypt data sent across public networks; 9: Track access to data by unique ID
- [7] G5: Not filtering packets for correct incoming and outgoing addresses

**PRACTICE #6.2:**

# System & Network Management: Software Integrity

Regularly verify the integrity of installed software.

Regularly check for and eradicate all viruses, worms, Trojan horses, other malicious software, and unauthorized software.

Regularly compare all file and directory cryptographic checksums with a securely stored, maintained, and trusted baseline.



Questions for enterprise leaders, senior managers, and oversight boards

- What is the responsibility of users, including senior management, to safely operate systems?
- How often do you scan for viruses on your desktop and laptop systems?
- What actions do you take if you discover a virus?
- How do you recover compromised files?
- How do you contain the damage caused by a virus?
- How do you avoid propagating a virus to others?
- How do you verify that a recently created file has not been tampered with?
- Do your administrators regularly scan for the presence of viruses, worms, Trojan horses, and denial-of-service agents?

**Mapping to references:**

- [1] OP2.1: System and Network Management
- [2] 8: Communications and Operations Management; 10: System Development and Maintenance
- [3] 7: Computer Operations Security
- [4] SM51: Protection from Malicious Code; IP35: Virus Protection
- [5] 2: Securing Network Servers and User Workstations
- [6] 5: Use and regularly update anti-virus software

### PRACTICE #6.3:

# System & Network Management: Secure Asset Configuration

Provide procedures and mechanisms to ensure the secure configuration of all deployed assets throughout their life cycle of installation, operation, maintenance, and retirement. (For further details, see [1].)

Apply patches to correct security and functionality problems.

Establish and maintain a standard, minimum essential configuration for each type of computer and each type of service.

Create a network topology diagram and ensure it is kept up to date.

Enable adequate levels of logging.

Consider the security implications for all changes to systems and networks.

Perform vulnerability assessments on a periodic basis, and address vulnerabilities when they are identified.



Questions for enterprise leaders, senior managers, and oversight boards

- How do you know that your desktop and laptop configurations and the servers you access are as secure as they need to be? Whom do you ask?
- How do you find out about necessary and critical software updates? How do you monitor the progress of the installation of these changes across your enterprise infrastructures?
- Can users download their own software from home?

#### Mapping to references:

- [1] OP2.1: System and Network Management; OP2.2: System Administration Tools; OP2.5: Vulnerability Management
- [2] 5: Asset Classification and Control; 8: Communications and Operations Management
- [3] 4: Applications and Systems Development Security; 7: Computer Operations Security
- [4] SM61: Security Audit/Review; CB42: Workstation Configuration; IP22 Host Configuration; IP23 Workstation Configuration; IP47: Access Logging; CN34: Change Management
- [5] 2: Securing Network Servers and User Workstations; 5: Setting Up Intrusion Detection and Response Practices
- [6] 2: Keep security patches up to date; 8: Don't use vendor supplied defaults
- [7] G1: Default installs of operating systems and applications; G4: Large number of open ports; G6: Non-existent or incomplete logging; G7: Vulnerable CGI programs

**PRACTICE #6.4:**

# System & Network Management: Backups

Mandate a regular schedule of backups for both software and data.

Validate software and data before backup.

Validate software and data after backup.

Verify the ability to restore from backups.



Questions for enterprise leaders, senior managers, and oversight boards

- What do you do when you want to retrieve a backup file that you inadvertently deleted? How long does this take?
- What is your role in backing up the user data on your desktop and laptop?

**Mapping to references:**

- [1] OP2.1: System and Network Management
- [2] 8: Communications and Operations Management
- [3] 7: Computer Operations Security
- [4] CB54: Back-up; IP33: Back-up; CN36: Back-up
- [5] 2: Securing Network Servers and User Workstations; 5: Setting Up Intrusion Detection and Response Practices
- [7] G3: Non-existent or incomplete backups

**PRACTICE #7.1:**

# Authentication & Authorization: Users

Implement and maintain appropriate mechanisms for user authentication and authorization when using network access from inside and outside the organization. Ensure these are consistent with policies, procedures, roles, and levels of restricted access required for specific assets. (Also see Practice #6.1.)



Questions for enterprise leaders, senior managers, and oversight boards

- What means of identification and authentication do you need for accessing the systems you use every day? For accessing critical, more highly protected systems that you may need to use from time to time?
- If you don't know, whom do you ask?

**Mapping to references:**

- [1] OP2.4: Authentication and Authorization
- [2] 9: Access Control
- [3] 1. Access Control Systems and Methodology
- [4] IP42: Access Control Arrangements; IP43: User Authorization; IP44: Access Privileges; IP46 User Authentication
- [5] 2: Securing Network Servers and User Workstations
- [6] 6: Restrict access by need to know; 7: Assign unique IDs to each person with access
- [7] G2: Accounts with no passwords or weak passwords

**PRACTICE #7.2:**

# Authentication & Authorization: Remote and Third Parties

Protect critical assets when providing network access to users working remotely and to third parties such as contractors and service providers. Use network-, system-, file-, and application-level access controls and restrict access to authorized times and tasks, as required. (Also see Practice #6.1.)

Use data encryption and virtual private network technologies, as required.



Questions for enterprise leaders, senior managers, and oversight boards

- How do you access your organization's network and systems when you are working from home or when traveling? Are you allowed to dial directly into modems attached to desktops or servers?
- Is your access restricted compared to what you can do when you are in the office?
- Do you have decision processes and supporting procedures in place to permit third party access, manage each type of relationship with the appropriate level of security, and retire or update accounts when partnerships terminate?
- If you don't know, whom do you ask?

**Mapping to references:**

- [1] SP5: Collaborative Security Management; OP2.4: Authentication and Authorization
- [2] 4: Organizational Security; 9: Access Control
- [3] 1. Access Control Systems and Methodology; 2: Telecommunications and Network Security
- [4] SM54: Remote Working; SM55: Third Party Access; CB61: Third Party Access; CN23: External Access
- [5] 2: Securing Network Servers and User Workstations

***There is one safeguard known generally to the wise, which is an advantage and security to all...What is it? Distrust.***

Demosthenes (c. 384-322 B.C.)

**PRACTICE #8:**

# Monitor & Audit

Use appropriate monitoring, auditing, and inspection facilities and assign responsibility for reporting, evaluating, and responding to system and network events and conditions.

Regularly use system and network monitoring tools and examine the results they produce.

Regularly use filtering and analysis tools and examine the results they produce.

Respond to events that warrant a response action.

Ensure that all employees are aware of whom to contact when they notice suspicious behavior.



Questions for enterprise leaders, senior managers, and oversight boards

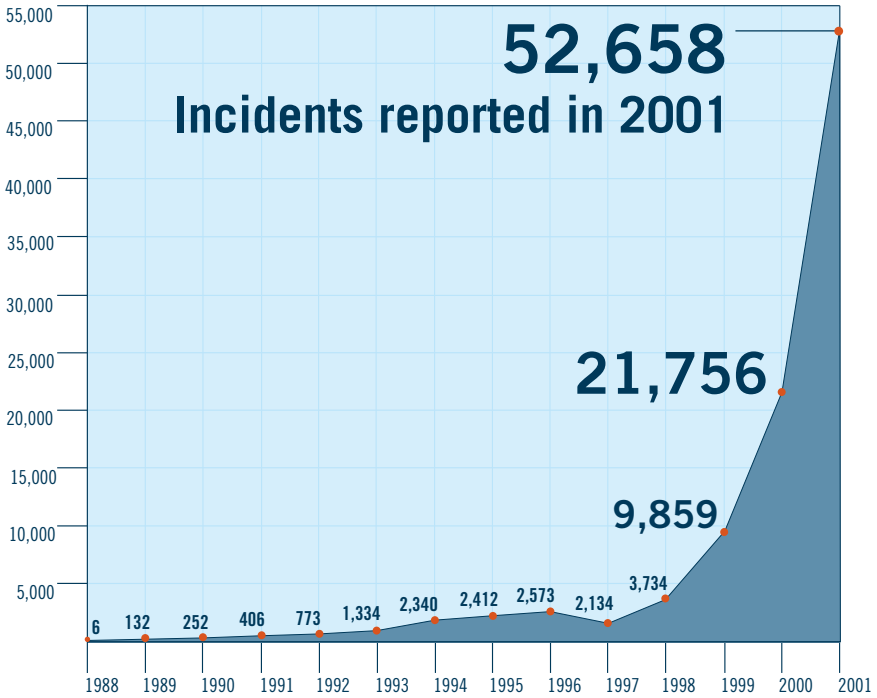
- When something doesn't look quite right on your system, whom do you call and what information do you need to provide to describe the problem?
- Have your systems ever been compromised? How do you know?
- Whom do you call to find out how your email and Web access are being monitored?
- Do your system and network administrators have an active contact list of peers for the primary networks with which yours interface?
- Are your administrators up to date on the latest threats, attacks, and solutions? What resources do they use?

**Mapping to references:**

- [1] SP1: Security Awareness and Training; OP2.2: System Administration Tools; OP2.3: Monitoring and Auditing IT Security; OP 3.1: Incident Management
- [2] 6: Personnel Security; 8: Communications and Operations Management; 9: Access Control; 12: Compliance
- [3] 1. Access Control Systems and Methodology; 2: Telecommunications and Network Security; 3: Security Management Practices; 7: Computer Operations Security; 9: Laws, Investigations, and Ethics
- [4] SM61: Security Audit/Review; SM62: Security Monitoring; CB35: Incident Management; CB36: Security Audit/Review; IP15: System Monitoring; IP34: Incident Management; IP65: Security Audit/Review; CN32 Network Monitoring; CN33: Incident Management; CN45: Security Audit/Review
- [5] 5: Setting Up Intrusion Detection and Response Practices; 6: Detecting Signs of Intrusion; 7: Responding to Intrusions
- [6] 10: Regularly test security systems and processes

Security incidents have more than doubled each year since 1988. Computer Economics of Carlsbad, California estimates that the Code Red virus—a single incident—cost \$1.1 billion in lost productivity.

Source: CERT® Coordination Center



**PRACTICE #9:**

# Physical Security

Control physical access to information assets and IT services and resources.

Use physical access controls (e.g., badges, biometrics, keys), where required.

Use password-controlled electronic locks for workstations, servers, and laptops that are enabled upon login and after specified periods of inactivity.

Control access to all critical hardware assets (e.g., routers, firewalls, servers, mail hubs).



Questions for enterprise leaders, senior managers, and oversight boards

- What means of identification and authentication do you need for accessing the primary facility where your office is? Critical facilities that you are required to visit from time to time?
- What assurances do you have that physical security access restrictions are being followed? How are violations reported to you?
- Do you know whom to contact if you detect suspicious letters, packages, or other items sent by mail or a delivery service? What is considered suspicious?

**Mapping to references:**

- [1] OP1.2: Physical Access Control; OP1.3: Monitoring and Auditing Physical Security
- [2] 5: Asset Classification and Control; 7: Physical and Environmental Security
- [3] 10: Physical Security
- [4] SM44: Physical Protection; IP27: Physical Access; CN35: Physical Access
- [5] 6: Detecting Signs of Intrusion
- [6] 12: Restrict physical access to information

**PRACTICE #10:**

# Continuity Planning & Disaster Recovery

Develop business continuity and disaster recovery plans for critical assets and ensure that they are periodically tested and found effective.



Questions for enterprise leaders, senior managers, and oversight boards

- Do you have a mission assurance plan in place that addresses business continuity and operational and disaster recovery? Is this plan regularly tested and found effective?
- If Internet e-commerce access into your corporation was lost for four to five days, would the impact cause financial instability?
- What do you do and whom do you call when there is a fire in your facility?
- Whom do you contact in the event of a natural disaster to determine how to fulfill your work responsibilities?
- How do you function effectively if the network you generally work on is unavailable?

**Mapping to references:**

[1] SP6: Contingency Planning and Disaster Recovery

[2] 11: Business Continuity Management

[3] 8: Business Continuity Planning and Disaster Recovery Planning

[4] SM45: Business Continuity; CB37: Business Continuity; IP71: Contingency Plans; IP72: Contingency Arrangements; CN37: Service Continuity

*Even if you are on the right track,  
you'll get run over if you just sit there.*

Will Rogers (1879-1935)

# References

- [1] **Albert, Christopher; Dorofee, Audrey; Allen, Julia** | *OCTAVE<sup>SM</sup> Catalog of Practices, Version 2.0*. | CMU/SEI-2001-TR-020 Carnegie Mellon University: Software Engineering Institute, October, 2001 | Available at <http://www.cert.org/archive/pdf/01tr020.pdf>.
- [2] *ISO/IEC 17799 Information Technology Code of Practices for Information Security Management, First edition* | ISO/IEC 17799:2000(E). December 2001.
- [3] **Tipton, Harold F.; Krause, Micki** | *Information Security Management, 4th Edition* | Auerbach, 2000.
- [4] **Information Security Forum** | *The Forum's Standard of Good Practice: The Standard for Information Security* | November 2001 | Available at [http://www.isfsecuritystandard.com/index\\_ns.htm](http://www.isfsecuritystandard.com/index_ns.htm).
- [5] **Allen, Julia** | *The CERT<sup>®</sup> Guide to System and Network Security Practices* | Addison-Wesley, June 2001.
- [6] **Shaughnessy, John** | presentation "Cardholder Information Security Program" | *ISAAlliance Conference* | Myrtle Beach, SC, April, 2002 | Available at [http://usa.visa.com/business/merchants/cisp\\_index.html](http://usa.visa.com/business/merchants/cisp_index.html).
- [7] **System Administration, Networking and Security Institute** | *SANS Top 20, Version 2.504* | May 2, 2002 | Available at <http://www.sans.org/top20.htm>.
- [8] **Computer Security Institute**, "2002 CSI/FBI Computer Crime and Security Survey," | *Computer Security Issues and Trends, Vol. VIII, no. 1*, | Spring 2002.

®CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office.

<sup>SM</sup>Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

## End Note

These recommendations address security practices for today's fielded, operational systems and networks and present a top-down management perspective that an organization can use to assess its information security posture.

We encourage readers to distribute this brochure widely in the interests of helping organizations manage their security risks and adopt effective security practices. Security continues to grow as a critical concern within the Internet community. The ISAlliance stands prepared to update the *Common Sense Guide for Senior Managers* to meet the evolving needs and is committed to continuing its work in the practices area. We encourage your participation within the ISAlliance as part of this important effort.

We welcome your comments. Please email them to [commonsense-guide@list.isalliance.org](mailto:commonsense-guide@list.isalliance.org).

## Authors

**Julia H. Allen** | Senior Member of the Technical Staff, Carnegie Mellon University, Software Engineering Institute

**Edward F. Mikoski, Jr.** | Vice President, Technology Strategy & Standards, Electronic Industries Alliance

**Kevin M. Nixon** | CISSP, Senior Director, Security Business Strategy, Exodus, A Cable & Wireless Service

**Donald L. Skillman** | Director of Internet Policy, ISAlliance

## Contributors

**Michael Aisenberg** | Director of Policy, Verisign Corporation

**Dr. Bill Hancock** | CISSP, Vice President, Security in Chief Security Office, Exodus, A Cable & Wireless Service

**Susan Koski** | AVP & Manager, Network and Perimeter Defense MISD/TAS/Corporate Information Security, Mellon Financial Corporation

**Yoram Maliniak** | Director, Knowledge Management & Information Security, Raytheon Company

**Ty Sagalow** | Chief Operating Officer, AIG E-Business Risk Solutions

**John Shaughnessy** | Senior Vice President, Visa U.S.A

**Nigel Willson** | Practice Director, TCS E-Security Labs, TATA Consultancy Services

# Join the ISAlliance today and...

## BE FIRST

Fight security breaches from the moment they're discovered instead of waiting to find out if you've been hit.

## BE SECURE

As an ISAlliance member, you'll improve your security posture, mitigate cyberthreats, and ensure continuity of business operations.

## BE HEARD

The ISAlliance increases your access to lawmakers, regulators, and news media, advocating your interests and amplifying your viewpoints.

## BENEFITS OF MEMBERSHIP

Each membership level includes an increasing number of certificates to the CERT®/CC Restricted Knowledgebase as well as an increasing discount on conferences, publications and CERT®/CC courses.

### ASSOCIATES US\$3,000/year

- 1 certificate
- 5% discount on conferences, publications, and CERT®/CC courses

1. Participation in ISAlliance working groups (currently Best Practices, Mission Assurance, and Public Policy)
2. Strategic and technical analysis on trends, incidents, prevalent vulnerabilities, best practices, and business risk

### MEMBERS US\$25,000/year

- 5 certificates
- 10% discount on conferences, publications, and CERT®/CC courses

3. Help desk support and consultation for vulnerabilities, alerts, and the CERT®/CC Restricted Knowledgebase
4. Analyst briefings on critical issues such as emerging threat patterns and new legislation

### SPONSORS US\$70,000/year

- 28 certificates
- 20% discount on conferences, publications, and CERT®/CC courses

5. Executive Committee membership
6. Host privileges for executive and committee meetings
7. Working group/sector chair privileges



# A NEW MEASURE OF CORPORATE RESPONSIBILITY



**INTERNET  
SECURITY  
ALLIANCE**

2500 Wilson Boulevard  
Arlington, Virginia 22201-3834  
United States of America  
+1 703 907 7709

**[www.isalliance.org](http://www.isalliance.org)**



# Have you and your senior managers considered the following questions?

Do you view security as essential to business survivability or as an overhead activity that needs to be regularly defended?

What is your role in ensuring security policies are followed?

How do you know when your systems are under attack? Do you know the financial impact to your business of a failure of network security?

Do you have a process to determine the security impact of linking new systems to your enterprise-wide architecture (through mergers, acquisitions, new business partnerships)?

When was the last time you and other senior managers, including your board, attended user training on information security as practiced in your organization?

What is the responsibility of users, including senior management, to safely operate systems (scanning for viruses, backing up user data files, following password policy, reporting suspicious behavior, etc.)?

Do you have decision processes and supporting procedures in place to permit third party access to your networks, manage each type of relationship with the appropriate level of security, and retire or update accounts when partnerships terminate?

What assurances do you have that physical security access restrictions are being followed and how are violations reported to you?

Do you have a mission assurance plan that addresses business continuity and operational and disaster recovery and is this plan regularly tested and found effective?





+1 703 907 7709

2500 Wilson Boulevard  
Arlington, Virginia 22201-3834  
United States of America

[www.isalliance.org](http://www.isalliance.org)