



610 Securing Your Assets in a Connected World

Sean A. Bowen

Vice President & General Counsel
Internet Security Systems, Inc.

William H. Mohr

Former Assistant General Counsel
Datek Online Holdings Corp.

Joel Michael Schwarz

Trial Attorney—Computer Crime and Intellectual Property Section
U.S. Department of Justice

Faculty Biographies

Sean A. Bowen

Sean Bowen is vice president and general counsel of Internet Security Systems, Inc., a pioneer and world leader in software and services that protect critical information assets from an ever-changing spectrum of threats and misuse. Headquartered in Atlanta, GA, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. Mr. Bowen is part of Internet Security Systems' executive management team and manages its legal matters including those relating to corporate governance, regulatory compliance, commercial contracting, and mergers and acquisitions. The company's sales contracting group, order fulfillment group and loss prevention group also report to Mr. Bowen.

Prior to joining Internet Security Systems, Mr. Bowen was senior counsel with Eastman Chemical Company, which manufactures and markets plastics, chemicals and fibers worldwide. He was a partner in the Cleveland law firm of Kahn, Kleinman, Yanowitz & Arnson Co. L.P.A. until he joined Eastman. Kahn Kleinman represents entrepreneurs and growth companies (public and private), Internet and technology businesses, real estate owners and developers, as well as their capital sources and service providers.

Mr. Bowen received a BS from the Tulane University, A.B. Freeman School of Business and a JD from The Ohio State University, College of Law.

William H. Mohr

William H. Mohr serves as an assistant general counsel to Datek Online Holdings Corp. Datek is recognized as an innovator and pioneer in the electronic marketplace. It is the parent of Datek Online Financial Services LLC, the founder of The Island ECN, and the parent of Watcher Technologies LLC, a leading supplier of software for active trading. Since joining Datek his responsibilities have included regulatory matters, technology issues, and intellectual property. Among his counseling responsibilities are compliance with the Gramm-Leach-Bliley Act's privacy and security requirements (including web disclosures, information collection, and sharing practices and vendor contracts), web media and web content transactions, market connectivity (including ECN contracts) and market data products (Streamer®), enforcement of intellectual property, and anti-money laundering (USA PATRIOT Act) compliance. Mr. Mohr serves as a member of the NASDR eBrokerage Committee and the SIA's Online Brokerage and State Regulation of Securities Committees.

Prior to joining Datek, Mr. Mohr was deputy chief of the Investor Protection and Securities Bureau in the office of the New York Attorney General where he had a leading role in conducting its inquiry and drafting its November 1999 report, *From Wall Street to Web Street*, regarding the online brokerage industry. In both his role as deputy and as the Bureau's chief of enforcement, he played leading roles in cases addressing misleading stock and mutual fund sales practices, new issue frauds, and in obtaining a \$60 million national settlement in 1996 with the Lloyd's of London insurance market. He also represented New York in its regulatory relationships with the NASDR, SEC and NASAA. Prior to his public advocacy work, Mr. Mohr was in private practice for four years, specializing in general commercial and banking law matters.

Mr. Mohr was awarded a BA, cum laude, by Thomas More College and a JD by the Washington University School of Law.

Joel Michael Schwarz

Joel Michael Schwarz is an attorney in the United States Department of Justice's Computer Crime and Intellectual Property Section (CCIPS).


Previously, Mr. Schwarz served as counsel on eCommerce for MetLife, where he advised various MetLife lines of business on eCommerce issues, including privacy, security, and technology-related matters. As a former prosecutor with the Attorney General's Office, Mr. Schwarz was responsible for the investigation and prosecution of internet fraud and crime. He served as the New York State Attorney General's Special Counsel for internet matters, investor protection, and securities bureau, and as assistant Attorney General with the Attorney General's Internet Bureau.

Mr. Schwarz provides training on prosecuting and conducting internet investigations to law enforcement at both the domestic and international level. He is currently chairing a Committee for the International Association of Prosecutors in order to develop a guide on conducting Internet investigations. Mr. Schwarz has published numerous articles in the area of internet and eCommerce, including in the *Berkeley Technology Law Journal*, the *Michigan Telecommunications and Technology Law Journal*, the *Harvard Journal of Law & Technology*, numerous articles in the *Wallstreetlawyer.com*, and has authored an online Continuing Legal Education Course for *Lawyersed.com*. His most recent publication was the cover story in the February 2002 issue of the *ACCA Docket*.

Mr. Schwarz received his undergraduate degree with a certification in computer programming, and graduated cum laude from Albany Law School. He recently completed a certification in Advanced Information Technologies from New York University.

Securing Your Online Network


Sean Bowen
Vice President & General Counsel



**INTERNET
SECURITY
SYSTEMS**

Internet Security Systems, Inc. *The Power to Protect*

Agenda



- Business Needs
- The Threat Environment
- The Basic Technologies
- Best Practices
- Emergency Response Planning
- Public Online Resources

www.iss.net

Today's Business Needs




INTERNET
SECURITY
SYSTEMS


- Online access by remote employees, customers and suppliers
- Applications and data distributed across business units, locations and servers
- Goal of security to enable information flow and electronic commerce
- Business units want control over access to information
- And protection of information assets

www.iss.net


Threat Environment



INTERNET
SECURITY
SYSTEMS



Threat Spectrum



Management

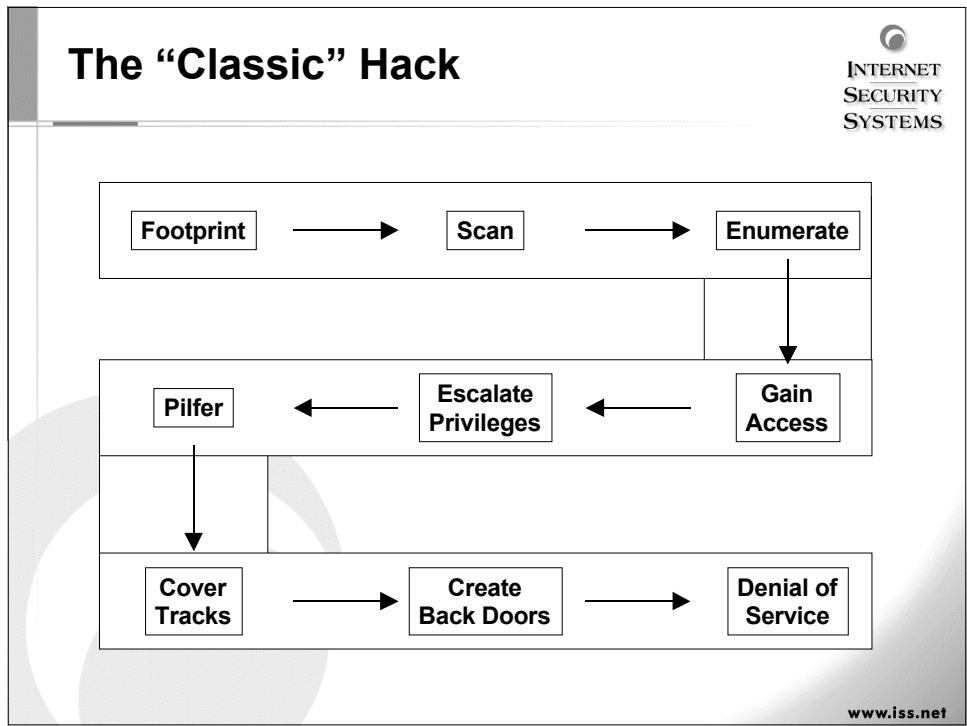
"Bad Out"

"Good In"

Intrusion Detection	Vulnerability Assessment	Anti-Virus /Blocking	Content Filtering	Forensics
VPN SSO	Encryption Authentication	BioMetrics SmartCards	Authorization Rights Mgmt.	
Router Switches	Databases Applications	Desktops Servers	Gateways Mobile Devices	

Network Infrastructure

www.iss.net



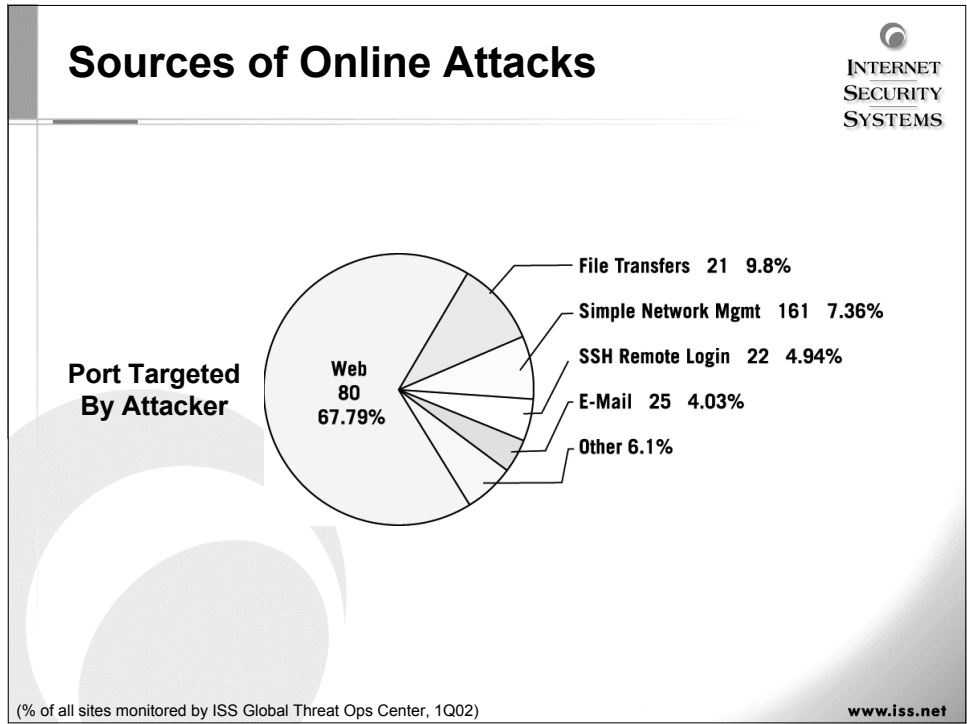
Automating Attacks

INTERNET SECURITY SYSTEMS

Automated attack tools require less knowledge while increasing an attack's sophistication:

- Self replicating code
- Stealth diagnostics
- Password cracking
- Packet spoofing
- Vulnerability exploits
- Automated scans
- Back doors
- Denial of Service Attacks
- Session Hijacking
- Distributed DOS Attacks
- Sweepers
- Morphing Malicious Code
- Sniffers

www.iss.net



The Cost Is Rising


Reported computer crime losses
1999 - \$124 Million 2002 - \$456 Million
(Source: CSI/FBI Computer Crime and Security Survey, 2002)

Incidents reported to CERT
1999 - 9,859 2002 - 43,136 thru June
(Source: Carnegie Mellon Cert Coordination Center)

INTERNET SECURITY SYSTEMS

www.iss.net

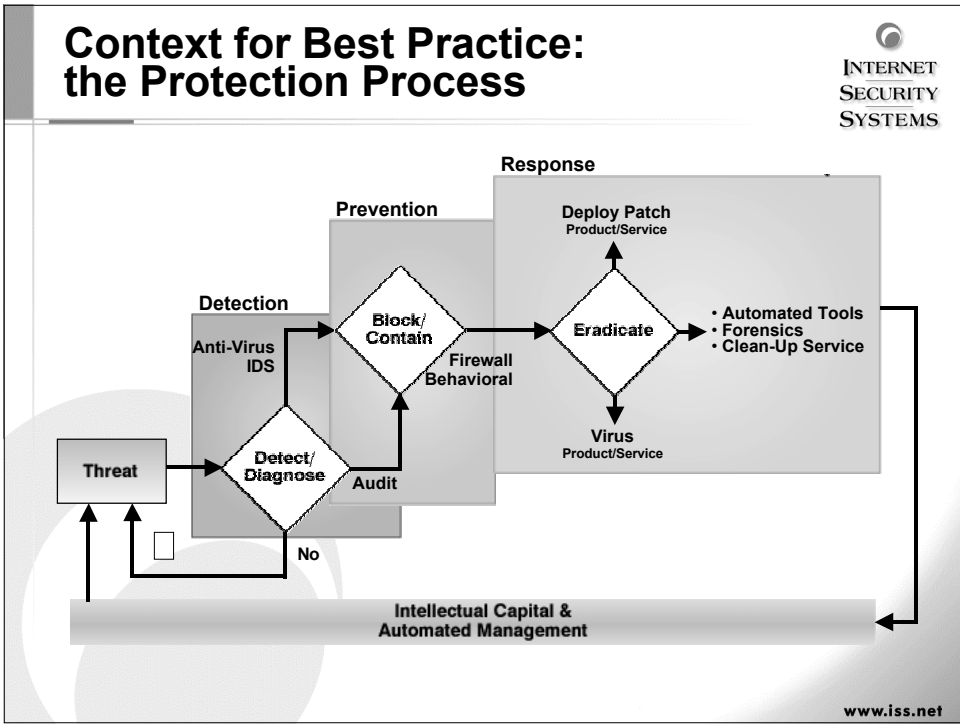
Security Technology

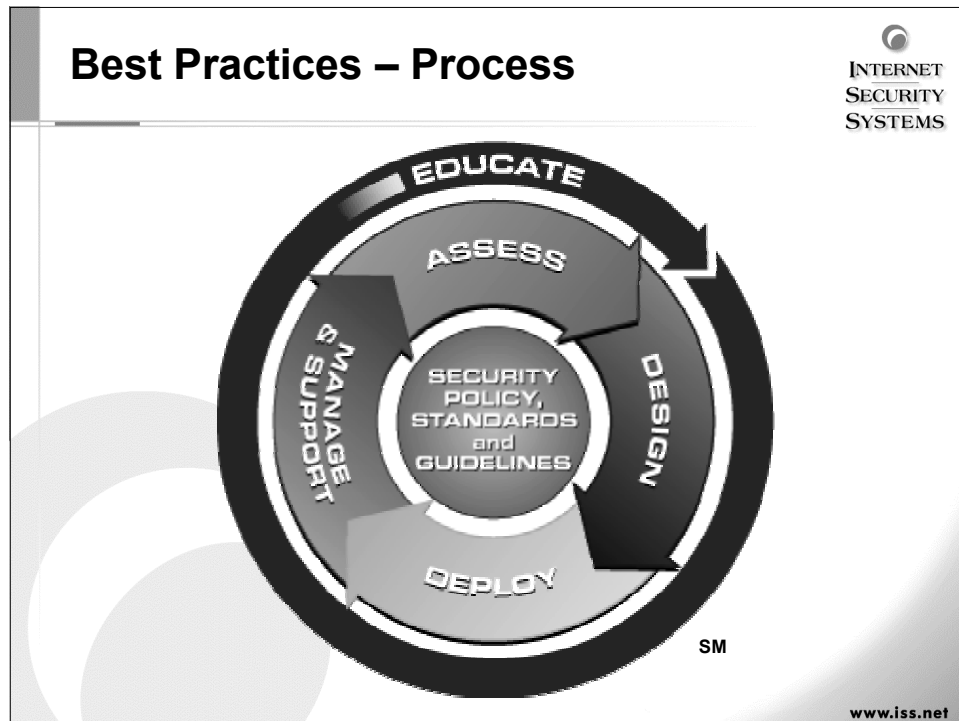


INTERNET
SECURITY
SYSTEMS

- **Firewalls**
- **Intrusion Protection**
- **Anti-virus**
- **Authorization and Authentication**
- **Virtual Private Networks (VPN)**
- **Private Key Infrastructure (PKI)**
- **Encryption**

www.iss.net





Emergency Response Planning

INTERNET SECURITY SYSTEMS

- Incident preparedness
 - Create a network security incident response team
 - Develop and incident response plan
 - Assess your network for security vulnerabilities
 - Eliminate known deficiencies
 - Maintain security system integrity
 - Educate your personnel regarding prevention, detection, evidence preservation and remediation
 - Maintain awareness of current threats
 - Review the plan and team periodically

www.iss.net

Emergency Response Planning



- Incident response
 - Determine need for privileged investigation
 - Determine need for forensics experts (next slide)
 - Reporting to law enforcement
 - Identify the source and cause of the incident
 - Take actions to take to stop or reduce the impact of the incident
 - Determine the effects and scope of the incident
 - Determine incident recovery procedures
 - Mitigate risk of incident re-occurrence
 - Prepare final incident report
 - Review and revise the plan if needed

www.iss.net

Emergency Response Planning



- Incident investigation
 - Specialized computer forensics techniques
 - "Computer Forensics" is not about computers; it's about rules of evidence, legal processes, evidence integrity and continuity, clear and concise testimony and expert opinion
 - Forensic investigation
 - Collection of evidence
 - Chain of custody
 - Expert testimony
 - Forensic analysis
 - Examination of evidence
 - Search for specifics
 - Reporting

www.iss.net

Public Online Information Resources



- National Infrastructure Protection Center (www.nipc.gov)
- NIPC sites list (www.nipc.gov/sites.htm)
- Carnegie Mellon, Software Engineering Institute, CERT Coordination Center (www.cert.org)
- DOE – Computer Incident Advisory Capability (www.ciac.org/ciac/)
- FBI – InfraGard Program (www.infragard.net)
- FBI (www.fbi.gov)
- DOJ – Computer Crime and Intellectual Property Section (www.usdoj.gov/criminal/cybercrime/)

www.iss.net

SampleCo

Computer Security Incident Response Plan

SampleCo Confidential

Copyright © 2000, Internet Security Systems, Inc.
Emergency Response Services

Table of Contents

- Table of Contents
- Introduction
- CSIRT Charter
 - Mission
 - Scope
 - Organizational and Team Structure
 - Information Flow
 - Services Provided
 - Primary (Reactive) Services
 - Secondary (Proactive) Services
- Computer Security Incident Definition and Declaration
 - Computer Security Incident Declaration
 - Computer Security Incident Severity
 - Use of the ISS Emergency Response Service
 - The CSIRP and Disaster Recovery
- Roles and Responsibilities
 - Team Member Roles and Responsibilities
 - CSIRT Officer
 - Alternate CSIRT Officer
 - CSIRT Manager
 - Alternate CSIRT Manager
 - CSIRT Decision Pool
 - WAN Services
 - LAN Services
 - Internet Operations
 - Mainframe Operations
 - Midrange Operations
 - Server Operations
 - Desktop Operations
 - Help Desk
 - Corporate Security
 - Legal
 - Human Resources
 - Media Relations
 - Disaster Recovery
 - CSIRT Response Team
 - CSIRT Recovery Team
 - Team Makeup by Job Title
 - CSIRT Officer & Manager
 - CSIRT Decision Pool
- Response Procedures

SampleCo Confidential

- Alert Phase
- Triage Phase
- Response Phase
- Recovery Phase
- Maintenance Phase
- Appendix A – Preplanned Response Procedures
- Appendix B – Sample Press Release
- Appendix C – CSIRT Contact Information
 - CSIRT Duty Phone/Pager
 - CSIRT Officer
 - CSIRT Manager
 - CSIRT Staff
 - CSIRT Decision Pool
- ISS Emergency Response Service
 - ISS ERS Contacts
 - ISS ERS Emergency Number

SampleCo Confidential

Copyright © 2000, Internet Security Systems, Inc.
Emergency Response Services

Introduction

Computer systems and networks are an integral part of SampleCo's business environment. Computers are used for research and development of products, marketing and public relations, electronic commerce, customer support, internal and external communications, and myriad day-to-day business operations. Unfortunately, in addition to the routine problems these systems are subject to, such as hardware and software failures, computer systems and networks are also frequent targets of malicious or criminal activity, including computer viruses, denial-of-service attacks, break-ins, theft or destruction of data, economic fraud, sabotage, and political terrorism.

As SampleCo's dependence on computer systems and networks increases, so does our risk of incurring serious business losses if the security of these systems and networks is compromised. SampleCo addresses this risk with policies, procedures, and tools that provide information security awareness, protection, and prevention. However, no prevention mechanism is perfect – technology changes, and new threats emerge. Therefore, it is imperative to prepare for the possibility that a serious security incident will occur despite current protection mechanisms.

The SampleCo Computer Security Incident Response Plan (CSIRP), contained in this document, provides guidance and documentation on computer security incident response handling and communication efforts. The CSIRP is activated whenever a computer security incident occurs, and guides the responses to all incidents whose severity is such that they could affect SampleCo's ability to do business, or undermine its reputation. Although contingencies exist to deal with lesser threats, the CSIRP is not designed for the resolution of typical systems or operational problems.

Implementation, testing, and maintenance of the CSIRP are the responsibility of the SampleCo Computer Security Incident Response Team (CSIRT). Managed by the I/T Security organization, the CSIRT is chartered with providing coordinated communications and response for all computer security incidents throughout the company.

CSIRT Charter

The SampleCo Computer Security Incident Response Team (CSIRT) is chartered with providing a coordinated response to computer security incidents throughout the company. The CSIRT Officer and CSIRT Manager have the authority to implement necessary actions and decisions during an incident.

Mission

The SampleCo CSIRT is the focal point for all computer security incidents. The mission of the SampleCo CSIRT is to:

- implement, test, and maintain the SampleCo Computer Security Incident Response Plan (CSIRP), a standard set of criteria for incident severity determination, responses to security problems, and protocols for interdepartmental communication during an incident;
- protect SampleCo computer systems and networks, and the data they contain, from the effects of computer security incidents;
- provide a central point of contact for the reporting and dissemination of information about computer security incidents;
- coordinate the activities of other SampleCo personnel in the investigation of, response to, and recovery from computer security incidents;
- minimize any negative impact of a computer security incident on SampleCo's business operations, financial state, and public image;
- minimize disruption to both internal and external customers; and
- collect necessary data and evidence for prosecution.

Scope

The constituencies served by the SampleCo CSIRT are the various I/T organizations within the company, and more specifically, the Office of the CIO.

The SampleCo CSIRP covers all computer systems and networks connected to the SampleCo corporate network, including those of existing and newly acquired subsidiaries. Business partners, vendors, and other external entities needing access to SampleCo information will be required to demonstrate compliance with adequate incident response and procedures to the CSIRT Manager before such access will be granted.

Organizational and Team Structure

The CSIRT is managed by the I/T Security organization. The team consists of permanent, affiliated, and temporary members.

Permanent members of the CSIRT include:

- **CSIRT Officer.** The CSIRT Officer reports directly to the Office of the CIO and serves as the liaison between the CSIRT and executive management. The CSIRT Officer is also responsible for activating the CSIRT Decision Pool.
- **CSIRT Manager.** The CSIRT Manager reports to the CSIRT Officer and supervises the day-to-day duties of the other CSIRT permanent members. The CSIRT Manager is responsible for activating the CSIRP when a computer security incident occurs, and for assigning an initial severity to the incident.
- **CSIRT Staff.** The CSIRT staff is composed of I/T Security organization personnel. The CSIRT Staff is responsible for performing the non-response services provided by the CSIRT (see below).

Affiliated members of the CSIRT include:

- **CSIRT Decision Pool.** The CSIRT Decision Pool is comprised of senior managers representing the individual I/T organizations and other internal business functions. I/T organizations represented include WAN Services, LAN Services, Internet Operations, Mainframe Operations, Midrange Operations, Server Operations, Desktop Operations, and Help Desk. Internal business functions represented include Corporate Security, Legal, Human Resources, Media Relations, and Disaster Recovery. The CSIRT Decision Pool is responsible for allocating resources and assigning personnel to serve on CSIRT Response Teams and CSIRT Recovery Teams.

Temporary members of the CSIRT include:

- **CSIRT Response Team(s).** A CSIRT Response Team will be assembled on a per-incident basis, depending on the skill set needed to effectively respond to the incident. Members will be assigned from the staffs of the various I/T organizations and internal business functions represented in the CSIRT Decision Pool, as well as from the permanent CSIRT Staff. For the duration of the incident, all members of the CSIRT Response Team report to and take direction from the CSIRT Manager. The CSIRT Response Team is responsible for providing analysis and containment of compromised systems and eliminating the cause of the incident.
- **CSIRT Recovery Team(s).** A CSIRT Recovery Team will be assembled on a per-incident basis, depending on the skill set needed to restore normal operations on the systems and networks affected by the incident. Members will be assigned from the staffs of the various I/T organizations and internal business functions represented in the CSIRT Decision Pool, as well as from the permanent CSIRT Staff. For the duration of the incident, all members of the CSIRT Recovery Team report to and take direction from the CSIRT Manager. The CSIRT Recovery Team works alongside the CSIRT Response Team to restore affected systems and services to normal operation.

Information Flow

The CSIRT may be alerted to a potential security incident from a variety of sources. Some examples include:

- An automated intrusion detection system reports suspicious network traffic directed at the web server from an unknown Internet site.
- The log files on the firewall show a large volume of “denied” packets from several Internet sites, with patterns suggesting a determined attempt to gain access.
- A user reports, through the Help Desk, that his system appears to have been infected by a computer virus.
- Reports in the popular press suggest that a fast-spreading computer virus/worm has been discovered, causing widespread shutdowns of corporate electronic mail systems.
- The web administrator receives an anonymous e-mail from a “hacker” threatening to shut down the web server.
- Human Resources reports that an employee has recently been terminated for cause, and has threatened retaliatory action.
- Media Relations receives a telephone call from a reporter seeking comment on another site’s claims that SampleCo’s systems were used to break in to their web server.

Regardless of the source of the alert, first notification of the incident is delivered to the CSIRT through a duty phone/pager held by a CSIRT Staff member, and answered 24 hours a day, seven days a week. The duty person’s first task is to notify the CSIRT Manager, who will then coordinate and direct the response.

The CSIRT Manager will provide the CSIRT Officer with regular updates about new incidents and the status of existing incidents. The CSIRT Officer will communicate this information to executive management through the Chief Information Officer.

When appropriate, information about a security incident may be communicated to SampleCo employees or the public. Any statements of this nature will be coordinated by Media Relations and/or Human Resources, and reviewed by Legal before their release.

Services Provided

The CSIRT will provide the following services.

Primary (Reactive) Services

The CSIRT’s primary function is to manage and respond to security incidents. During an incident, the actions of the CSIRT are broken down into five broad categories:

1. *Alert.* The CSIRT Manager receives the initial incident report, gathers supporting information, and assigns an initial incident severity. If the incident severity dictates, the CSIRT Officer and CSIRT Decision Pool are alerted.
2. *Triage.* The CSIRT Manager and CSIRT Decision Pool assess the criticality of the situation, allocate resources, and assign personnel to the CSIRT Response Team and CSIRT Recovery Team.
3. *Response.* The CSIRT Response Team implements CSIRP procedures to provide analysis and containment of compromised systems, and eliminate the cause of the incident.

4. *Recover.* The CSIRT Recovery Team works alongside the CSIRT Response Team to restore affected systems and services to normal operation.
5. *Maintenance.* Post-mortem analysis of the incident is performed to identify its cause(s) and determine areas for improvement. An after-action review of the CSIRP and response procedures is performed, and changes made where necessary.

Secondary (Proactive) Services

When not responding to active security incidents, the CSIRT Officer, Manager, and Staff provide several proactive security-related services to the SampleCo community:

- *CSIRP Maintenance.* Develop and maintain the Computer Security Incident Response Plan and the response and recovery procedures associated with it. Conduct annual tests of the CSIRP through mock incident drills.
- *Policy Development.* Develop and maintain information security policies related to the Internet and Internet technologies.
- *Compliance Testing.* Perform security vulnerability assessments of SampleCo I/T resources, and coordinate the elimination of discovered problems.
- *Announcements.* Disseminate information about protective measures to take against existing and upcoming security threats to SampleCo I/T organizations.
- *Education.* Provide training of SampleCo employees, and conduct security awareness programs.

Computer Security Incident Definition and Declaration

A *computer security incident* is any occurrence of unauthorized access or use of SampleCo computer resources with the potential to compromise the confidentiality, availability, or integrity of those resources or the data stored on them. Computer security incidents are more than just a nuisance; they have the potential to cause serious financial loss and/or damage to SampleCo's public image.

Computer Security Incident Declaration

The CSIRT Officer and CSIRT Manager are the only personnel authorized to formally declare a computer security incident and activate the CSIRP. The CSIRT Officer is the only person authorized to convene the CSIRT Decision Pool.

Computer Security Incident Severity

The CSIRT Manager is responsible for initially assessing an incident's impact, and assigning a severity to the incident. This initial severity assignment dictates the level of response to the incident. As response to the incident progresses, it may be determined that the incident is more (or less) severe than originally realized, and a new severity may be assigned.

Computer security incidents are divided into five levels of severity based on their potential to negatively impact SampleCo's operations, finances, or public image. The characteristics in the table below are intended to serve as general guidelines only, and should not be interpreted as absolutes.

Incident Severity	Incident Characteristics	Activate CSIRP	CSIRT Officer Alerted	CSIRT Decision Pool Alerted
1	<ul style="list-style-type: none"> ▪ Small numbers of system probes, scans, and similar activities detected on internal systems ▪ Isolated instances of known computer viruses or worms, easily handled by deployed anti-virus software 	NO	NO	NO
2 INCREASED RISK OF ATTACK	<ul style="list-style-type: none"> ▪ Small numbers of system probes, scans, and similar activities detected on external systems ▪ Intelligence received concerning threats to which SampleCo systems may be vulnerable 	NO	ROUTINE UPDATE	NO
3 SPECIFIC RISK OF ATTACK	<ul style="list-style-type: none"> ▪ Significant level of network probes, scans and similar activities detected indicating a pattern of concentrated reconnaissance ▪ Penetration or denial of service attack(s) attempted with no impact to SampleCo operations ▪ Widespread instances of a known computer virus or worm, easily handled by deployed anti-virus software 	YES	ALERT	ROUTINE UPDATE

Incident Severity	Incident Characteristics	Activate CSIRP	CSIRT Officer Alerted	CSIRT Decision Pool Alerted
	<ul style="list-style-type: none"> ▪ Isolated instances of a new computer virus or worm that cannot be handled by deployed anti-virus software 			
4 LIMITED ATTACK(S)	<ul style="list-style-type: none"> ▪ Penetration or denial-of-service attack(s) detected with limited impact on SampleCo operations: <ul style="list-style-type: none"> ○ Minimally successful, easy to control or counteract ○ Small number of systems compromised ○ Little or no loss of confidential data ○ No loss of mission-critical systems or applications ▪ Widespread instances of a new computer virus or worm that cannot be handled by deployed anti-virus software ▪ Small risk of negative financial or public relations impact 	YES	ALERT	ALERT
5 GENERAL ATTACK(S)	<ul style="list-style-type: none"> ▪ Successful penetration or denial-of-service attack(s) detected with significant impact on SampleCo operations: <ul style="list-style-type: none"> ○ Very successful, difficult to control or counteract ○ Large number of systems compromised ○ Significant loss of confidential data ○ Loss of mission-critical systems or applications ▪ Significant risk of negative financial or public relations impact 	YES	ALERT	ALERT

In the table above, “Routine Update” means the CSIRT Officer or CSIRT Decision Pool will be notified of the incident at the next scheduled routine incident status update, while “Alert” means they will be notified immediately.

Use of the ISS Emergency Response Service

Internet Security Systems, Inc. (ISS) has been engaged to provide Emergency Response Services (ERS) to SampleCo in the event of a computer security incident. In response to SampleCo’s declaration of a security emergency, ISS ERS will respond 24 hours a day, seven days a week with a staff of security experts who can provide SampleCo’s CSIRT with advice and assistance in all phases of incident management and response.

The CSIRT Manager and CSIRT Officer are the only personnel authorized to declare a security emergency under the ISS ERS service. Although ultimately the circumstances surrounding each individual incident will be the deciding factor, ISS ERS will generally be placed on alert for all Severity 4 and Severity 5 incidents as well as the occasional Severity 3 incident.

The CSIRP and Disaster Recovery

While most computer security incidents will not pose a significant threat to SampleCo’s physical infrastructure, there are events that can cause drastic system outages or physical and logical damage to SampleCo computer systems, business applications, web sites, or networks. In

addition, some incidents may cause harm to SampleCo's reputation and integrity. When these events occur, it is necessary to locate the source and type of incident and to work quickly to close off the exposure and minimize the damage caused by the incident. These steps may include communicating incidents to the media, contacting federal or local law enforcement authorities, etc.

In these instances, the computer security incident may be considered a disaster in the context of the SampleCo Disaster Recovery Plan. Recovery from a very severe incident may require the use of SampleCo's contracted disaster recovery facilities until the original facilities can be restored to normal operations. Even if external facilities are not needed, the system recovery plans and procedures maintained by the Disaster Recovery organization may be useful in recovering from the effects of the incident.

To maintain the necessary close ties between the CSIRT and the Disaster Recovery organization, the CSIRT Officer and CSIRT Manager are included on the Disaster Recovery call list, and a representative from Disaster Recovery is included in the CSIRT Decision Pool.

Roles and Responsibilities

The CSIRT Officer, CSIRT Manager, and permanent CSIRT staff are hired and managed by the I/T Security organization. The CSIRT Decision Pool is comprised of senior managers representing the individual I/T organizations and other internal business functions. The CSIRT Response and Recovery Teams are assembled on a per-incident basis, depending on the skill set needed to effectively respond to and recover from the incident. Members will be assigned from the staffs of the various I/T organizations and internal business functions represented in the CSIRT Decision Pool, as well as from the permanent CSIRT Staff.

Team Member Roles and Responsibilities

The CSIRT shall be organized into the following roles and associated responsibilities:

CSIRT Officer

- Activates the CSIRP.
- Activates the CSIRT Decision Pool.
- Provides status and communication to executive management.
- Coordinates with the Disaster Recovery organization when necessary.

Alternate CSIRT Officer

- Takes the place of the CSIRT Officer in the event the CSIRT Officer is unavailable.

CSIRT Manager

- Determines the initial severity of each reported incident.
- Manages response and recovery efforts for all computer security incidents.
- Determines the makeup of the CSIRT Response Team and CSIRT Recovery Team for a particular incident.
- Communicates incident status to the CSIRT Officer regularly until the incident is closed.
- Reviews and approves the incident management plans of business partners, vendors, and external entities.

Alternate CSIRT Manager

- Takes the place of the CSIRT Manager in the event the CSIRT Manager is unavailable.

CSIRT Decision Pool

- Activated by the CSIRT Officer and reports directly to the CSIRT Manager for the duration of the incident.

- Comprised of senior managers representing the individual I/T organizations and other internal business functions. I/T organizations represented include WAN Services, LAN Services, Internet Operations, Mainframe Operations, Midrange Operations, Server Operations, Desktop Operations, and Help Desk. Internal business functions represented include Corporate Security, Legal, Human Resources, Media Relations, and Disaster Recovery.
- Responsible for allocating resources and assigning personnel to serve on the CSIRT Response Team and CSIRT Recovery Team.
- Coordinates efforts with business partners, vendors, and other external entities by working with individuals in similar functional capacities.

WAN Services

- Secure and evaluate system security for external routers, firewalls, and other associated systems.
- Coordinate communications with Internet service providers.

LAN Services

- Secure and evaluate system security for internal routers, firewalls, and other associated systems.

Internet Operations

- Assess impact of incident on the production Internet environment (web servers, e-commerce servers, etc.).
- Coordinate changes to the production Internet environment.

Mainframe Operations

- Assess impact of incident on the production mainframe computer environment.
- Coordinate changes to the production mainframe computer environment.

Midrange Operations

- Assess impact of incident on the production midrange computer environment.
- Coordinate changes to the production midrange computer environment.

Server Operations

- Assess impact of incident on the production application and file server computer environment.
- Coordinate changes to the production application and file server computer environment.

Desktop Operations

- Assess impact of incident on the production desktop computer environment.

- Coordinate changes to the production desktop computer environment.

Help Desk

- Liaison with SampleCo user community.
- Provide computer virus assistance.
- Individual desktop security issues.

Corporate Security

- Determine “pursue vs. protect” priorities (with assistance from Legal).
- Determine importance/security classification of compromised data.
- Conduct necessary employee interviews.
- Physical security.

Legal

- Determine legal ramifications of the incident (and response to it).
- Advise Corporate Security on “pursue vs. protect” question.
- Liaison with law enforcement authorities.
- Review communications to press.

Human Resources

- Advise CSIRT Decision Pool on personnel-related issues.
- Coordinate internal communications to employees.

Media Relations

- Create communications for internal and/or external release.
- Primary focal point for media contact.

Disaster Recovery

- Coordinate business continuity and disaster recovery issues.

CSIRT Response Team

- Members determined on a per-incident basis by the CSIRT Manager, and assigned by the CSIRT Decision Pool.
- Activated once the severity of the incident is determined, and remains active until the incident is closed.
- Determine the scope of the incident and how to prevent it from spreading.
- Determine the exploits/vulnerabilities used by the attacker, and close or block them.

- Assist in evidence collection as dictated by the “pursue vs. protect” decision.
- Make recommendations for remedial actions on affected systems.

CSIRT Recovery Team

- Members determined on a per-incident basis by the CSIRT Manager, and assigned by the CSIRT Decision Pool.
- Activated once the severity of the incident is determined, and remains active until the incident is closed.
- Determine whether affected systems can be restored from backup tapes, or must be reinstalled.
- Reload data on affected systems.
- Restore normal operations.

Team Makeup by Job Title

The following personnel fill CSIRT roles.

CSIRT Officer & Manager

CSIRT Officer

Director, I/T Security

Alternate: Director, Corporate Security

CSIRT Manager

Manager, Internet Security

Alternate: Manager, WAN Security

CSIRT Decision Pool

WAN Services

WAN Security Officer

LAN Services

LAN Security Officer

Internet Operations

Internet Operations Manager

Mainframe Operations

Manager, Mainframe Systems

Midrange Operations

Manager, Midrange Systems

Server Operations

Manager, Application Servers

Desktop Operations

Manager, Desktop Operations

Help Desk

Manager, User Support

Corporate Security

Corporate Security Officer

Legal

Counsel, Internet Law

Human Resources

Manager, Human Resources

Media Relations

Manager, Media Relations

Disaster Recovery

Manager, Disaster Recovery

Response Procedures

This section provides general guidelines for incident response procedures. Detailed response procedures for particular incident types are contained in Appendix A.

Alert Phase

- Potential security incidents may be reported from a variety of sources. Examples include automated intrusion detection systems, firewall log files, user reports to the Help Desk, reports in the popular press, e-mail threats from “hackers,” Human Resources, and Media Relations.
- The security incident is communicated to the CSIRT via the CSIRT Duty Phone/Duty Pager. The CSIRT team member receiving the alert contacts the CSIRT Manager.

Triage Phase

- The CSIRT Manager assembles members of the CSIRT Staff to gather preliminary details about the incident. Based on the information gathered, the CSIRT Manager assigns an initial severity to the incident.
- If the incident is of Severity 3 or greater, the CSIRT Manager alerts the CSIRT Officer.
- If the incident is of Severity 4 or greater, the CSIRT Officer activates the CSIRT Decision Pool. The CSIRT Decision Pool:
 - Evaluates the “pursue vs. protect” decision. This decision must be made before any response is performed, as it affects the techniques and tools that can be used in the response.
 - Allocates resources and personnel to the CSIRT Recovery Team and CSIRT Response Team, based on the CSIRT Manager’s requests and recommendations.
- If the incident is of Severity 3 or greater, the ISS Emergency Response Service may be contacted and/or a formal emergency declared. Authority to make this decision resides with the CSIRT Manager and CSIRT Officer.

Response Phase

- The CSIRT Manager and CSIRT Staff handle incidents of Severity 3 and lower. A CSIRT Response Team will be assembled to handle incidents of Severity 4 and 5.
- The compromised systems are backed up. Depending on the outcome of the “pursue vs. protect” decision, this backup may be performed using specialized forensic imaging equipment, or with standard system backup/imaging tools. The copies are secured in an access-controlled area.

- Audit trails, log files, file system contents, etc. are analyzed to determine the symptoms, cause, and source of the incident.
- Remove the cause of the incident by installing software updates and patches, making configuration changes, removing or disabling insecure software, etc.
- Review all user access to the affected system(s). Remove unneeded access privileges, and change all remaining user passwords.

Recovery Phase

- Locate most recent “clean” backups and all software installation media for the affected system(s).
- Determine whether the affected system(s) can be restored from backup tapes, or if they must be rebuilt from scratch.
- Restore or rebuild affected system(s).
- Test the restored/rebuilt system(s) to ensure they are no longer vulnerable to the attack(s) that caused the incident.
- Test the restored/rebuilt system(s) to ensure they will function correctly when placed back into production.
- Place system(s) back into production.

Maintenance Phase

- Conduct an after-incident review meeting, attended by the CSIRT Officer, CSIRT Manager, CSIRT Staff, and any CSIRT Response and Recovery Teams.
- Provide recommended/suggested configuration and/or procedural changes to the relevant operations groups.
- Provide recommended/suggested policy changes to the relevant policy organizations.
- Update predefined response procedures as necessary.
- Update CSIRP document as necessary.

Appendix A – Preplanned Response Procedures

This section contains preplanned response procedures for common or expected incidents. Where a preplanned response does not exist for the current incident, the procedures for a similar type of incident (e.g., of a different severity) should be used as guidance. After the incident has been closed, a preplanned response for that incident type should be created and included in this section.

Appendix B – Sample Press Release

SAMPLECO'S CUSTOMER DATA SECURE

CUSTOMERS ASSURED OF BUSINESS AS USUAL DESPITE (*INCIDENT/ATTACK*)

NEW YORK, NY (*date*) – SampleCo announced today that despite a (*security incident/external attack/system malfunction which may or may not be local*), its Computer Security Incident Response Team is working to ensure continuity for all of its business processes. A computer system was temporarily disabled (*provide date and time*) as a result of (*give full details: include who/what/where/when/how specifics of situation. Explain what other geographic regions or SampleCo departments may be affected*).

According to (*insert name*), Director of I/T Security, the company's incident response plans and containment procedures have been activated, meaning that customers' information and data have been protected and the (*network/application/server*) involved is being attended to. "SampleCo's primary concern is the privacy of customers', business partners', and employees' information and data," (*name*) said. "We constantly strive to ensure that we continue to deliver the level of service our customers are accustomed to – even in the event of a security incident. Security response procedures have been developed, documented, and rigorously tested to ensure our preparedness for just such a situation."

SampleCo's computer facilities are located in a hardened data center in New York City. The facility was completed in 1997 and is the home of SampleCo's mainframe and midrange computer environments, networks, and application server support for the company's offices around the country. The SampleCo data center employs approximately 500 full-time employees.

(*name*) outlined the response plans that were enacted for this type of situation. "SampleCo has made a considerable investment in incident detection and containment systems, as well as considerable investment in backup computer facilities. We have a staff of dedicated information security specialists who are responsible for ongoing development and testing of the incident response plan. In addition, we have contracted with Internet Security Systems, Inc., a leading provider of security products and services, to take advantage of their knowledge and expertise in managing and responding to computer security incidents." She expected normal computer system operations to be restored by (*date/time*).

Headquartered in Manhattan, SampleCo is one of the world's leading sample companies, and is the market leader in sample sales in the United States. With 1999 revenues of \$567 million, SampleCo currently serves over 10,000 customers in 11 countries throughout Europe, Asia, and the Americas.

Appendix C – CSIRT Contact Information

Contact information for all CSIRT personnel is contained in this section.

Initial notification of an incident should be provided to the CSIRT by calling the CSIRT Duty Phone/Pager.

CSIRT Duty Phone/Pager

The CSIRT Duty Phone telephone number is (999) 999-9999. This telephone number is answered 24 hours a day, 7 days a week.

The CSIRT Duty Pager telephone number is (999) 999-9999. The CSIRT Duty Pager is intended as a backup to the CSIRT Duty Phone.

CSIRT Officer

The CSIRT Officer is John Smith:

Office telephone:	(999) 999-9999
Home telephone:	(999) 999-9999
Pager:	(999) 999-9999

The alternate CSIRT Officer is Bill Jones:

Office telephone:	(999) 999-9999
Home telephone:	(999) 999-9999
Pager:	(999) 999-9999

CSIRT Manager

The CSIRT Manager is Jane Doe:

Office telephone:	(999) 999-9999
Home telephone:	(999) 999-9999
Pager:	(999) 999-9999

The alternate CSIRT Manager is Mike Smith:

Office telephone:	(999) 999-9999
Home telephone:	(999) 999-9999
Pager:	(999) 999-9999

CSIRT Staff

Bob Jones	NT Security	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Sally Edwards	Unix Security	Office telephone:	(999) 999-9999

		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Mike Martin	E-Commerce Security	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Doug Schultz	Internet Security	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Bill Zimmerman	Anti-Virus	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999

CSIRT Decision Pool

Alice Houser	WAN Services	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Edward Johnson	LAN Services	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Alan Smith	Internet Operations	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Lisa Williams	Mainframe Operations	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
James Watson	Midrange Operations	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Arlene Asquith	Server Operations	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Gregory Watts	Desktop Operations	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Shirley Boyd	Help Desk	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Bob Masters	Corporate Security	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999

Nina Rogers	Legal	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Sandra Burns	Human Resources	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
David James	Media Relations	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999
Mike Adams	Disaster Recovery	Office telephone:	(999) 999-9999
		Home telephone:	(999) 999-9999
		Pager:	(999) 999-9999

ISS Emergency Response Service

The ISS Emergency Response Service is only to be contacted at the direction of the CSIRT Manager or CSIRT Officer.

ISS ERS Contacts

Bob Smith	(999) 999-9999
Ann Jones	(999) 999-9999

ISS ERS Emergency Number

1-800-477-8999



INTERNET
SECURITY
SYSTEMS™

Computer Security Incident Response Planning

Preparing for the Inevitable

Introduction

Computers and computer networks have been part of the corporate landscape for decades. But it's only in the last five years that companies have started to connect these systems and networks to the outside world – suppliers, business partners, and the Internet. Unfortunately, in the hurry to get connected and jump on the e-business bandwagon, computer security is frequently given short shrift, placing corporate assets at risk.

The popular media is filled with accounts of recent Internet security problems, including the denial of service attacks against Yahoo!, eBay, Amazon, CNN, and others, several instances of data theft involving credit cards or personal information, and the "I Love You" virus/worm. Although the press devoted many column-inches and on-air minutes to these stories, they focused primarily on the exciting topic of "the chase" to catch the perpetrators, and generally ignored the more important topics of how frequently computer security incidents occur, how many companies' data is at significant risk, and the potentially devastating impact of computer security incidents on their victims.

The Computer Security Institute, among other industry analysis, reports that computer security incidents are widespread (*2000 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, March 2000). 90% of respondents detected computer security breaches in the previous 12 months, and 70% reported serious security breaches other than the most common ones (viruses, laptop theft, and employee "net abuse"), such as theft of proprietary information, financial fraud, system penetration by outsiders, denial of service attacks, and sabotage of data or networks. The survey also shows that attacks occur frequently, with 35% percent of those acknowledging attacks reporting between two and five incidents in the last year, and 19% reporting ten or more incidents. 71% of the survey's respondents detected instances of unauthorized access by insiders, demonstrating that even companies whose networks are not connected to the Internet are at risk.

The computer security industry offers a variety of solutions to this problem, from firewalls, authentication, and encryption to vulnerability scanning tools and intrusion detection systems. Consulting firms offer a broad range of security services, including security assessments, secure network infrastructure design and deployment, policy development, penetration testing, and so forth. But while all of these products and services have their place, they take time (often months, sometimes years) and money to procure and implement correctly. In the meantime, a company has to live with the security implementation it has – it may not be state-of-the-art, it may not be as strong as it should be, but the systems and networks that depend on it are critical to the company's business, and cannot simply be turned off while waiting for a stronger security solution to be designed and installed.

Given the certainty that attempts will be made to compromise system and network security, and the likelihood that these attempts will succeed, every company, large or small, must be prepared to respond effectively to security incidents when they occur. Even sophisticated, state-of-the-art security systems are not foolproof – thus, regardless of where a company is in the "security spectrum," an organized incident response capability is of the utmost importance.

Incident Response Planning

A Computer Security Incident Response Plan (CSIRP) provides guidance and documentation on computer security incident response handling and communication efforts. The CSIRP is activated whenever a computer security incident occurs, and guides the responses to all incidents whose severity is such that they could affect a company's ability to do business, or undermine its reputation.

The inevitability that (possibly successful) attempts will be made to compromise system and network security dictates that every company, from the largest multinationals to the smallest "dot com" startups, should have a formal CSIRP in place. CSIRP development should be the top security budget priority in any company – more important than security services, and more important than security products. When a security incident occurs, reactions and decisions must be made very quickly (often in a matter of minutes). The company has to be prepared to deal with these incidents as soon as they occur; waiting until a new product arrives or a consulting engagement is completed is not an option.

Establishing a Team

The first step in creating a formal CSIRP is the establishment of a Computer Security Incident Response Team (CSIRT).

The CSIRT Charter

The CSIRT Charter is a document that formally establishes the team, and documents its responsibility to respond to computer security incidents. The CSIRT Charter also delegates the authority to implement necessary actions and decisions during an incident, usually to the CSIRT leader or manager.

Sections of the CSIRT Charter document include:

Mission – Describes the overall goals of the CSIRT; the things it is responsible for. This might include such tasks as responding to all incidents, minimizing their impact, and collecting data and evidence for prosecution.

Scope – Defines the constituency of the CSIRT, i.e., who it serves. Some companies may have a single CSIRT for the entire company, while others may have multiple CSIRTs separated by business unit, geography, or other criteria. This section also describes the team's area of responsibility (e.g., all corporate networks, all networks in a division, all networks connected to the corporate network (such as those of business partners), or some combination thereof).

Organizational Structure – Documents how the CSIRT is organized from a management perspective – how the members of the team are managed, and how the team reports to upper-level management.

Information Flow – Describes how information flows before, during, and after an incident. First, this section describes how a potential security incident is reported to the CSIRT, and provides contact information for doing so. Second, it describes how the CSIRT communicates information about an incident to (a) upper-level management, (b) company employees, and (c) the public.

Services Provided – Documents the specific services the CSIRT provides. This is based on the mission statement (above), and may include services such as incident response, policy development, compliance testing, and user education.

Roles and Responsibilities

A CSIRT usually consists of a manager, a management advisory board, some number of permanent team members, and a larger number of temporary members:

CSIRT Manager/Leader – The CSIRT Manager (or Leader) is responsible for managing the overall response and recovery activities for all security incidents. He or she determines (usually with assistance from others) the severity of each incident, and decides which staff members will perform the actual response and recovery tasks. The CSIRT Manager usually has some degree of budget and decision authority to take necessary actions during an incident.

Management Advisory Board – The management advisory board is made up of senior managers from the company's IT organizations and other internal business functions. IT organizations represented may include Network Services, Internet Operations, Mainframe Operations, Midrange Operations, Server Operations, Desktop Operations, and Help Desk. Other internal business functions represented may include Corporate Security, Legal, Human Resources, Media Relations, and Disaster Recovery. This group makes decisions and budget requests above the level delegated to the CSIRT Manager.

Permanent Team Members – Permanent team members are those IT staff whose primary job responsibility is IT security. Usually, these people report to the CSIRT Manager. They provide the non-response services (such as user education and policy development), and help the CSIRT Manager in the initial response to incidents.

Temporary Team Members – Temporary team members report to the IT organizations and other internal business functions represented on the management advisory board. They are the subject matter experts for the particular systems, applications, and business issues involved in the incident. Temporary team members are usually assigned to an incident by their managers (on the advisory board) at the request of the CSIRT Manager, and serve for the duration of the incident.

Within the CSIRP, it is important to document the specific roles and responsibilities of each of the above groups. Specifically, the following points need to be addressed:

- How much decision and budget authority is delegated to the CSIRT Manager? For example, can he or she authorize overtime? If so, how much? Can he or she authorize disconnecting the company from the Internet altogether? If so, under what conditions?
- What is each group responsible for? Every action to be taken should have an "owner" associated with it, to make sure it gets done. Where necessary, limits should be set and documented (e.g., a server can be taken down for less than an hour without authorization, but longer periods need the approval of someone higher up in the management chain).
- When major decisions need to be made (e.g., disconnect from the Internet, pursue the attacker vs. protect the systems, etc.), what are the criteria for those decisions? Who has the ultimate authority to make the decision?

The roles and responsibilities section of the CSIRP is perhaps the most challenging section to write. On the one hand, it has to be specific in answering the questions posed above, to avoid any ambiguities in interpretation. On the other hand, it has to be general, to avoid getting bogged down in too many details. The best CSIRPs approach this

conflict by being as general as possible, and only getting into specifics when absolutely necessary.

Incident Severity and Declaration

Many security incidents, such as isolated occurrences of computer viruses, are easily handled via well-established procedures (especially in larger companies), and do not justify calling out the entire CSIRT. The CSIRP must describe the criteria used to classify the severity of security incidents, and which severities will result in CSIRP activation.

Incident Severity

Incidents should usually be grouped into a few different severity levels, with broad sets of criteria for each level. For example:

Severity 1 – Small numbers of system probes or scans detected on internal systems; isolated instances of known computer viruses easily handled by anti-virus software.

Severity 2 – Small numbers of system probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable.

Severity 3 – Significant numbers of system probes or scans detected; penetration or denial of service attacks attempted with no impact on operations; widespread instances of known computer viruses easily handled by anti-virus software; isolated instances of a new computer virus not handled by anti-virus software.

Severity 4 – Penetration or denial of service attacks attempted with limited impact on operations; widespread instances of a new computer virus not handled by anti-virus software; some risk of negative financial or public relations impact.

Severity 5 – Successful penetration or denial of service attacks detected with significant impact on operations; significant risk of negative financial or public relations impact.

In this example, incidents of Severity 3, 4, and 5 would result in CSIRP activation, while incidents of Severity 1 and 2 would be handled without CSIRT involvement.

Incident Declaration

When an incident requiring CSIRP activation occurs, a formal incident is declared. The CSIRP should document how such a declaration is made and who is responsible for making it. Generally, incident declaration is a procedure by which the CSIRT Manager notifies upper-level management that an incident is taking place, and then assembles the other members of the CSIRT.

Response Procedures

Response procedures can be described at two levels of detail in the CSIRP. The first level of detail is a set of general guidelines that describes the principal phases of incident response, and what happens during each phase. Every CSIRP should include this level of detail. The second level of detail is a set of step-by-step response procedures, specific to individual incident types (e.g., procedure(s) for handling virus incidents, procedure(s) for handling hacker break-ins, etc.). These procedures will

generally be created over time, and can be added to the CSIRP in appendices as they are developed.

There are five principal phases of incident response, shown below. The general procedures to be followed in each phase should be described in the CSIRP.

Alert Phase

The alert phase is the process of learning about a (potential) security incident, and reporting it to the CSIRT. Alerts may arrive from a variety of sources including: firewalls and intrusion detection systems, anti-virus software, threats received via electronic mail, media reports about a new threat, etc.

The CSIRT is usually notified by providing a "hotline" telephone number, or a duty phone/pager that is reachable 24 hours a day, 7 days a week.

Triage Phase

The triage phase is the process of examining the information available about the incident to determine first if it is a "real" incident, and second, if it is, its severity. The CSIRT Manager usually does this, with assistance from the permanent team members.

If the incident's severity warrants, the CSIRT management advisory board will also be alerted in this phase. The board must do two important things in this phase:

- A decision to "pursue" or "protect" must be made. In other words, does the company want to attempt to catch the perpetrator(s) of the attack for later criminal or civil action, or does it simply want to stop the incident and restore normal operations? This decision must be made *before* response begins, because it influences how the response will happen.
- Resources (personnel and financial) must be allocated to the response and recovery teams at a level appropriate to the severity of the incident.

Response Phase

In the response phase, the CSIRT gathers evidence (audit trails, log files, contents of files, etc.). If the "pursue" option was chosen, this process must be performed in a forensically sound manner so that the evidence will later be admissible in court; the team may need specialized technical assistance and advice from a third party to do this successfully.

Once evidence has been gathered, it is analyzed to determine the cause of the incident, the vulnerability or vulnerabilities being exploited, how to eliminate these vulnerabilities and/or stop the incident, and so forth. An assessment is also made of how far the incident has spread, i.e., which systems are involved, and how badly have they been compromised.

Recovery Phase

The recovery phase begins once the response phase has been completed (there may at times be some overlap). In this phase, the CSIRT restores the systems affected by the incident to normal operation. This may require reloading data from backup tapes, or reinstalling systems from their original distribution media.

Once the affected systems have been restored, they are tested to make sure they are no longer vulnerable to the attack(s) that caused the incident. They are also tested to make sure they will function correctly when placed back into production.

Maintenance Phase

The maintenance phase is also called "lessons learned." In this phase, the entire incident, as well as the response, are reviewed to determine which parts of the CSIRP plan worked correctly, and which parts need improvement. The areas in which improvement is needed are then corrected, and the CSIRP updated accordingly. Other areas that need to be changed (policies, system configurations, etc.) may also be identified during this phase.

The Advantages of Commercial Incident Response Services

In the last few years, Internet Security Systems and a handful of other companies have begun offering commercial incident response services. These services are usually subscription-based (although some companies will also provide ad-hoc assistance) and include both proactive and reactive components. The proactive components include such items as on-site consulting, policy review and/or development, vulnerability assessments, security advisories, etc. The reactive components usually involve telephone and/or on-site response to customers' security incidents by professionals experienced in computer security incident response disciplines.

When our children enter pre-school or kindergarten, one of the first things we teach them is how to dial 9-1-1 in an emergency. Because it is unlikely that a child can be taught how to properly respond to these emergencies (e.g., a heart attack), it is better to teach them how to quickly summon someone who can. However, even trained professionals (e.g., doctors) recognize that the people who respond to these calls are both better trained and better equipped to handle emergencies, and will therefore make use of 9-1-1 as well, if only to make sure that extra help is available if it is needed.

Commercial incident response services are built around the same thinking. On the one hand, there are numerous companies with little or no in-house IT security expertise. These companies need someone to respond to security incidents for them, because they cannot do it themselves. On the other hand, even large companies, with extensive IT security staffs, recognize the value of having experts on call that "live and breathe" computer security incident response and can offer advice and assistance.

Depth and Breadth of Experience

One of the most valuable components of commercial services is the depth of experience they bring to the table. Every member of the commercial service is experienced in computer security incident response, having responded to dozens, if not hundreds, of actual incidents. A single company's IT staff, on the other hand, has limited experience at best, because it only has an opportunity to respond to incidents affecting that company.

Commercial response teams also bring breadth of experience. Because they respond to incidents at multiple customers, they are exposed to a wider variety of systems, network configurations, and attack methods than a single company's team would be. In many cases, an incident that is new and unheard of to the customer's response team will already be familiar to the commercial response team.

Specialized Skills

Another valuable component of commercial response teams is the set of specialized skills they offer. This includes in-depth experience with a wide variety of operating systems and applications, but also less common skills such as forensics investigation and analysis.

Forensics

A few years ago, most computer security incidents were certainly annoying, and possibly embarrassing, but they caused little if any lasting damage. But as the trend toward e-business continues, this is changing. The CSI survey reports that 74% of respondents reported financial losses because of computer security breaches and misuse last year.

As the potential for actual loss increases, the response to incidents is changing. Where it used to be sufficient to simply make the problem "go away," companies are now becoming much more interested in pursuing legal action (criminal or civil) against the perpetrators.

To pursue such legal action however, evidence is needed, and this evidence must be admissible in a court of law. This means that the evidence must be collected and analyzed in a forensically sound manner, i.e., according to special rules of conduct on the part of the investigators. It is important to note that forensic investigation and analysis is *not* a technical problem, but a legal one. Specialized data-gathering equipment and data-analysis tools are needed to insure that evidence is not inadvertently altered or destroyed. The personnel performing the investigation and analysis must be specially trained to perform their jobs, and, if the case goes to trial, to testify about their actions in court.

Staff Costs

The last, and perhaps the most significant advantage of commercial incident response teams, is one of staff costs. Computer security personnel are in notoriously high demand, making them both expensive to acquire, and difficult to retain.

According to the SANS Institute, security administrators and consultants made average salaries of \$63,598 and \$79,395, respectively (*SANS Security Alert*, SANS Institute, January 2001). Add to this the expense of ongoing training, necessary to keep these employees' skills up-to-date, and the cost goes even higher. The Gartner Group estimates that a small, dedicated, two-person incident response team will cost \$251,000 in first-year capital expenditures, \$324,000 per year in salaries, benefits, and training, and \$100,000 per year in external investigation and forensics services (Source: Gartner Group, October 2000). Justifying the funds to hire a dedicated staff of security personnel is difficult for many large companies, and frequently impossible for smaller ones.

Because the security job market is so volatile, retention is also a problem. Computer security incident response personnel would, on the whole, rather be responding to incidents. If a company does not suffer enough incidents to keep its staff occupied, those people are likely to go elsewhere, where things may be more "exciting."

Advantage

Commercial incident response services can help companies with all of these problems. They offer a pool of highly experienced staff, and make sure that they receive adequate training to keep their skills up to date. Because they can spread the costs over multiple customers, commercial services can offer specialized skills such as forensic investigation and analysis that would be unaffordable to a single company. And, again because they can spread the costs over multiple customers, they can offer their services to customers for little more than the cost of a hiring a single security expert in-house.

Summary

Every company needs to have a Computer Security Incident Response Plan in place, regardless of where the company is in the "security spectrum." Security incidents won't wait for new security software to be installed, or security consulting engagements to be completed. A company has to be prepared to defend what it has, and respond to security incidents as they occur.

Commercial security incident response services can help companies develop their CSIRPs, not only with consulting to build the plan itself, but also by providing response team personnel. A company can augment its own security staff, whatever its size and experience, with a commercial service to provide additional expertise and specialized skills. This partnership approach results in the best protection at the lowest cost.

About Internet Security Systems (ISS)

Internet Security Systems, Inc. (ISS) (Nasdaq: ISSX) is the leading global provider of security management solutions for the Internet. By combining best of breed products, security management services, aggressive research and development, and comprehensive educational and consulting services, ISS is the trusted security advisor for thousands of organizations around the world looking to protect their mission critical information and networks.

Copyright © 2001 Internet Security Systems, Inc. All rights reserved. Internet Security Systems is a trademark of Internet Security Systems, Inc. All other trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications are subject to change without notice.

AMERICAN CORPORATE COUNSEL ASSOCIATION
October 22, 2002, 2:30 PM

⋮

SECURING YOUR ASSETS IN A CONNECTED WORLD
(PRESENTED BY ACCA'S E-COMMERCE COMMITTEE)

⋮

SOURCES OF LEGAL DUTIES FOR DATA PROTECTION, SECURITY
MONITORING & VENDOR DUE DILIGENCE¹

⋮

WILLIAM H. MOHR
Former Assistant General Counsel
Datek Online Holdings Corp.
wmohr@nyc.rr.com

- I Risk Awareness in a Connected World**
- II. Promises that are Hard to Keep.**
- III. Gramm-Leach-Bliley Act (“GLB”) Compliance for Financial Firms.**
 - A. What is Personally Identifiable Information (“PII”)?**
 - 1. The Statute**
 - 2. The SEC Regulation**
 - 3. The Sum and Substance of PII**
 - 4. SEC Resources on GLB.**
 - B. GLB Privacy & Security Compliance Notes for Broker-Dealers:**
 - C. GLB Standards for Safekeeping Customer Information**
 - 1. Summary of GLB Regulations**
 - 2. FTC Financial Data Safeguards Rulemaking**
 - 3. Bank Interagency Guidelines for Customer Information**
 - D. GLB Compliance Inspection & Examination Issues**
 - E. GLB Litigation Issues**
- IV. Health Insurance Portability and Accountability Act**
- V. Duty of Care & Tort Liability**
 - A. Negligence**
 - B. Best Practice Guides**
 - 1. Federal Security Guidelines**
 - 2. National Institute of Standards and Technology**
- VI. State Legal Authorities**
 - A. Right of Privacy Statutes and Constitutional Provisions**
 - C. State Information Security Provisions**
- VII. International Legal Authorities**
 - A. Organization for Economic Cooperation and Development**
 - B. European Union & Members**
 - C. Additional Resources**

¹ This paper is current as of its submission date of August 30, 2002.

I. Risk Awareness in a Connected World

Any firm that has sensitive data, whether or not an “e-commerce” firm, must consider the risks that now arise from anonymous, transnational computer hackers, “script kiddies,” and economic guerrillas. Since our venue is Washington, there is no better illustration of the perils of the inter-connected world than the government itself—starting at the Pentagon. This summer the Washington Post ran a page one story that 34 military sites had been found where network security was easily compromised (lack of firewalls and password protections or easily cracked passwords), including Army computers at Fort Hood, Texas; NASA's Ames Research Center in Northern California and Navy facilities in Maryland and Virginia.²

The scope of the threat is also evident from testimony on Capitol Hill that Defense Department networks experienced 23,662 “incidents” in 2000, most of which were “routine” probes and scans by automated hacking tools, but 413 were determined to be “malicious” and on 215 occasions attackers pierced unclassified data. Further, the Defense Department expert emphasized that the “threat continues to improve.”³ In sum, if the Defense Department is unable to secure all of its networks despite its resources and the evident classified nature of its assets, the prospects for secure civilian systems appears unpromising.

Nonetheless, financial service providers are obliged by law to “establish appropriate standards...to **insure** the security and confidentiality of customer records and information.”⁴ Similar requirements will soon be promulgated for firms that obtain or maintain electronic health care information. Additional firms are eagerly taking upon themselves similar obligations by the promises that they make via privacy policies to the public. Thus the aggregate web security exposure of business (i) to the public for the potential loss or unauthorized access to stored personal information, (ii) from reputational injury and (iii) for remediation costs if a data loss occurs appears incalculable.

The materials that follow (i) provide references to the basic source documents on the legal requirements for web security measures and (ii) examine the issue in detail in the context of financial service providers—an arena that is now under a legal mandate to maintain information safeguards.

II. Promises that are Hard to Keep

Our Privacy Policy

Maintaining the security and confidentiality of information we maintain

² Sleuths Invade Military PCs With Ease, Robert O'Harrow, Jr., *Washington Post*, August 16, 2002; Page A01, <http://www.washingtonpost.com/wp-dyn/articles/A24191-2002Aug15.html>. The discoveries were made by a start-up, San Diego IT consultancy. Within hours of the article a search warrant was executed on the firm for illegally entering the government computers. Consultants Invaded Federal Computers, Robert O'Harrow Jr., *Washington Post*, August 21, 2002; Page E03, <http://www.washingtonpost.com/wp-dyn/articles/A42019-2002Aug20.html>.

³ Statement of Major General James D. Bryan, U.S. Army Commander, Joint Task Force Computer Network Operations U.S. Cincspace and Vice Director, Defense Information Systems Agency before the Military Readiness Subcommittee of the Armed Services Committee, of the United States House of Representatives, hearing on Vulnerabilities of Department of Defense Networks, May 17, 2001; <http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-05-17bryan.html>

⁴ Gramm Leach Bliley Act, Public Law 106-102 (November 12, 1999), Section 501(b).

about our customers is a top priority for us at _____. We carefully manage Customer Information within _____ in order to give you better service, greater convenience, and additional benefits consistent with the nature of your overall business with us. Hence we maintain personal data with appropriate and high-level physical, electronic, and managerial safeguards to insure the security and confidentiality of the data against foreseeable risks. Security is designed to prevent unauthorized use, access, disclosure, destruction and change of data.

This exemplar of a Privacy Policy typifies the approach of many firms that approached the issue from the marketing perspective. Such firms, consequently, have made promises that will be difficult to keep. Such documents represents the primary source of liability to customers for the unauthorized disclosure of personally identifiable information.

Such promises are enforceable by the Federal Trade Commission, State Attorney Generals, local government public advocates and individual consumers by virtue of the FTC Act and parallel statutes at the state and local level. Additional consideration must be given to the potential applicability of state statutes and constitutional provisions that may grant a right of action for the invasion of personal privacy (*see* Section VI *infra*). The following enforcement proceedings are the leading cases:

_ **Microsoft Corporation** on August 8, 2002 settled FTC charges alleging false data security and privacy promises concerning its "Passport Single Sign-In, Passport 'Wallet,' and Kids Passport." Microsoft agreed to (i) maintain a comprehensive security program, (ii) submit to the FTC biennial third-party inspections of its practices over the next 20 years, and (iii) cease misrepresenting its data services and products. The FTC did not charge that any data was compromised or unlawfully accessed. *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises; "Passport Single Sign-In, Passport 'Wallet,' and Kids Passport Named in Complaint Allegations*, August 8, 2002, <http://www.ftc.gov/opa/2002/08/microsoft.htm>, The Consent Order requires Microsoft to now comply with the FTC's rule applicable to certain financial firms that come under the FTC's jurisdiction (*see* Section III-C-2 *infra*). <http://www.ftc.gov/os/2002/08/microsoftagree.pdf>.

_ **Ziff Davis Media Inc.** on August 28, 2002 reached a settlement with the New York, California and Vermont Attorneys General regarding a November 2001 incident in which records of 12,000 subscribers were rendered accessible, some of whom became victims of identity fraud. The states invoked deceptive business practice statutes premised upon Ziff's privacy pledge of "reasonable security precautions." Ziff agreed to pay \$500 each to 50 persons whose credit card data was accessed, \$100,000 to the states, augment security practices and supply reports to the AGs. <http://www.wired.com/news/business/0,1367,54817,00.html>

_ **Eli Lilly & Co.** On January 18, 2002 Lilly settled via an administrative consent an FTC proceeding that was commenced after an untrained Lilly employee dispatched a group e-mail to all customers that were receiving Prozac by mail, thus revealing the email addresses of 669 customers. Lilly agreed to institute procedures to heighten information security and to identify reasonably foreseeable internal and external risks to the

security, confidentiality, and integrity of personal information, <http://www.ftc.gov/opa/2002/01/elililly.htm> .

Consent Order <http://www.ftc.gov/os/2002/01/lillyagree.pdf>

_ **FTC v. Toysmart.com**, No. 00-11341-RGS (D. MA filed July 10, 2000). Toysmart's privacy policy pledge not to share customer information but its bankruptcy forced it to weigh the sale of its customer list. The FTC obtained consent relief after maintaining that a departure by a firm from its stated privacy policy is a deceptive business practice actionable as a violation of §5(a) of the FTC Act. <http://www.ftc.gov/opa/2000/07/toysmart2.htm> (July 21, 2000).

III. Gramm-Leach-Bliley Act ("GLB") Compliance for Financial Firms

The GLB Act requires that the respective administering regulators "shall establish appropriate standards...relating to administrative, technical, and physical safeguards-- (1) to **insure** the security and confidentiality of customer records and information..." (Act §501(b)).⁵ Fortunately, regulators have not acted to make financial institutions "insurers" of the security and confidentiality of customer data. However, the competitive market place that firms operate in requires that they operate with the utmost attention to security matters.

A. What is Personally Identifiable Information ("PII")?

1. The Statute: GLB bars a financial institution from disclosing "*nonpublic personal information to a nonaffiliated third party*," 15 USC §6802(b). This term is then defined in §6809, (§509 of the Act), as follows:

(4) Nonpublic personal information.--

(A) The term "nonpublic personal information" means personally identifiable financial information--

(i) provided by a consumer to a financial institution;

(ii) resulting from any transaction with the consumer or any service performed for the consumer; or

(iii) otherwise obtained by the financial institution.

2. The SEC Regulation: SEC Regulation S-P, 17 CFR §248.3(u)(1)⁶ (Definitions), frames a definition of "*Personally identifiable financial information*" that both inserts "*financial*" and expands upon the "*otherwise obtained*" language as follows:

(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

⁵ Whether disgruntled customers will be able to maintain private actions to enforce this language or the regulations issued pursuant to the GLB Act is examined in section III-E of this outline.

⁶ While this outline focuses on the SEC privacy regulation, the rule was the product of coordinated drafting and enactment process with federal banking regulators.

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

The Regulation then goes on to provide several examples that utilize the “*about a customer*” portion of the definition:

(D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;

(E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on a loan or servicing a loan;

(F) Any information you collect through an Internet "cookie" (an information collecting device from a web server); and

(G) Information from a consumer report.

The SEC Regulation then gives some examples of information that is not “personally identifiable financial information,” namely:

(A) A list of names and addresses of customers of an entity that is not a financial institution; or [The telephone book or prospect lists are not PII.]

(B) Information that does not identify a consumer, such as *aggregate* information or *blind data* that does not contain personal identifiers such as account numbers, names, or addresses.

3. The Sum and Substance of PII

_ Ignore the inclusion of “financial” in the SEC definition. The SEC Release makes clear that information is “financial” if a BD collects it—it’s not a limiting term at all.

_ The safest approach is to assume that all information about a customer is PII.

_ The insertion of “cookies” was an expansion by the SEC of the final rule from the draft published for comment. Although “cookies” uniquely identify a machine, not a person, the best practice is to disclose that a web site may collect data via a cookie. Not all cookies are the same and “web bugs” or “web beacons,” in the better view are *not* cookies at all. A common trap for many privacy disclosures is a too specific description of “cookies” that may exclude other tracking technology techniques.⁷

⁷ Plaintiffs have generally failed in attempts to curb cookies by asserting an array of federal statutes. *In Re Pharmatrak, Inc. Privacy Litigation*, 2002 U.S. Lexis 15293 (D. MA); *Chance v. Avenue A, Inc.* 165 F.Supp. 2d (WD WA 2001); *In Re DoubleClick, Inc. Privacy Litigation*, 154 F.Supp. 2d 487 (SDNY 2001)(third party cookie); *but see, In Re Intuit Privacy Litigation*, 138 F.Supp. 2d (CD CA 2001) (first party cookie). Disclosures made by firms employing cookies, web bugs and web beacons are also a principal focus of litigation. DoubleClick on August 26, 2002 reached a [settlement](#) (PDF) pact with the

4. SEC Resources on GLB

_ Final Rule: Privacy of Consumer Financial Information (Regulation S-P), June 22, 2000; 17 CFR PART 248; Release Nos. 34-42974, IC-24543, IA-1883; File No. S7-6-00; <http://www.sec.gov/rules/final/34-42974.htm>.

_ Division of Investment Management FAQs: Electronic Filing for Investment Advisers on IARD: Staff Responses to Questions About Regulation S-P, April 9, 2001; <http://www.sec.gov/divisions/investment/iard/faqregsp.shtml>.

_ Office of Compliance Inspections and Examinations ("OCIE"): Examinations of Broker-Dealers ("BDs") Offering Online Trading: Summary of Findings and Recommendations, January 25, 2001 (Part V; Security); <http://www.sec.gov/news/studies/online.htm>.

_ Final Rule: Definition of Terms in and Specific Exemptions for Banks, Savings Associations, and Savings Banks Under Sections 3(a)(4) and 3(a)(5) of the Securities Exchange Act of 1934, May 11, 2001; Release No. 34-44291; File No.: S7-12-01; <http://www.sec.gov/rules/final/34-44291.pdf>.

_ SIA Letter to David L. Aaron, Under Secretary for International Trade, Re: International Safe Harbor Privacy Principles, May 14, 2001; http://www.sia.com/privacy/html/privacy_safe_harbor_principles.html.

_ Investment Counsel Association of America, Investment Advisers Strategies for Compliance with Regulation S-P (prepared by Dechert law firm), April 2001, 40 pages, <http://www.icaa.org/public/privacy.pdf>.

B. GLB Privacy & Security Compliance Notes for Broker-Dealers

_ **Applicability:** The SEC's Regulation S-P, enacted by the SEC to implement Title V of GLB, is applicable to: (i) all entities that meet the definition of a broker under §3(a)(4) of the Securities Exchange Act (15 U.S.C. §78c(a)(4)) whether or not they are actually registered as a broker; (ii) any investment adviser ("IA") registered with the SEC under the Investment Advisers Act of 1940; and (iii) investment companies. 17 CFR §248.3(b), (q), (5) and (w). Since IAs with less than \$25 million are registered by the states where they have their principal office, and not the SEC, they are subject to the rules that were enacted by the FTC.

New York Attorney General and 9 other states regarding its use of cookies and web beacons. DoubleClick agreed to (i) provide a limited "cookie viewer" that will permit consumers to see the profile categories maintained by DCLK from its data harvesting web surfers, (ii) require DCLK to monitor sites using its services to correctly disclose its data collection practices, (iii) effect certain changes in its privacy policies and (iv) conduct 3 outside reviews of its policies over the next 4 years. In May 2002 DCLK settled private lawsuits relating to its privacy practices and agreed to pay attorneys fees of \$1.8 million. http://www.oag.state.ny.us/press/2002/aug/aug26a_02.html

_ Notices to former Customers: Firms that do not engage in sharing information with unpermitted third parties are not required to make an initial notice or afford an opt-out notice to former customers. Conversely, if there will be non-exempt data sharing, the notice and opt-out opportunity must be afforded.

_ Defining Customers: A “customer relationship” is defined to mean a continuing relationship through which a firm provides a product or service, §248.3(k)(1). The SEC advises that an annual notice need not be presented to an account that is inactive under a firm’s policies consistently applied. The same result applies where the firm has not communicated with the customer about the relationship for a period of 12 consecutive months, other than to provide annual privacy notices or promotional material. Not every circumstance is resolved by the regulation. Some examples include:

- There may be persons who have applied for an account but not funded an account and hence have not received any product or service.
- There may be others who transacted but now have no balance.

_ Electronic Delivery in the Account Opening Process. For the consumer who conducts transactions electronically the SEC rejected mere posting, however conspicuous, on a web site. Rather, firms must post the notice on the web site and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining a financial product or service, §248.9(b)(1)(iii). By contrast, mailing to the last known address of the unwired customer suffices, §248.9(b)(1)(ii).

_ Joint Notices are permissible. A firm may provide a joint notice for it and one or more affiliates or other financial institutions, as long as the notice is accurate with respect to all institutions, §248.9(f). The adopting release states that: “a clearing broker could provide a joint notice with an introducing broker for which it clears transactions on a fully disclosed basis, or a fund complex could provide a joint notice for all the funds in the complex. We emphasize that the notice must be accurate for each institution that uses the notice, and must identify each institution by name.” Similarly, a firm could send a joint notice for itself and an independent firm used as a custodian for IRAs.

_ Record keeping requirements. SEC Regulation S-P’s requirement of security “policies and procedures” requires a writing as NASD Rule 3010(b) requires that firms maintain written supervisory procedures to comply with applicable laws and regulations. Further, records concerning the delivery to consumers of privacy notices and opt-outs notices must be maintained in accordance with the record keeping requirements of 17 CFR 240.17a-4 (broker-dealers); 270.31a-2 (funds); 275.204-2 (registered advisers). Adopting Release, n.143.

Service Providers. Section 502(e) of the Act creates an important exception from the requirement of providing an opt-out notice about data-sharing with third parties engaged for “maintaining or servicing” the customer’s account.⁸

Regulation S-P carries forward this exemption by providing that the privacy notice may exclude from the categories of affiliates and non-affiliated third parties to whom information is disclosed those persons who fall within 17 CFR §§ 248.14 and 248.15, *see* 17 CFR §248.6(a)(3). The applicable §248.14(a), which is entitled “*Exceptions for processing or servicing transactions at consumer’s request,*” provides that the notice and opt-out provisions do not apply to data sharing “necessary to effect, administer, or enforce a transaction.” The “necessary to effect...” provision is further defined by §248.14(b)(2) as a “usual, **appropriate, or acceptable** method: (i) To carry out the transaction or the product or service business of which the transaction is a part, and record, **service or maintain** the customer’s account in the ordinary course of providing the financial service or financial product...”

Additional requirements of the service provider exception are that an initial privacy notice be given at the point of customer acquisition and that the firm enter “into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which you disclosed the information,” §248.13(a)(1)(ii).

C. GLB Standards for Safekeeping Customer Information

1. Summary of GLB Regulations

The statutory goals of GLB §501(b) are to:

- ◇ insure the security and confidentiality of customer information;
- ◇ protect against anticipated threats/hazards; and
- ◇ protect against unauthorized access.

Federal Bank regulators have promulgated detailed regulations addressing the security and confidentiality protections that banks must adhere to in safeguarding customer information, Bank Interagency Guidelines Establishing, 66 FR 8615 (February 1, 2001). Although these regulations are not explicitly applicable to broker-dealers—or even to broker-dealer affiliates of banks—they are recognized as standards or “best practices” against which other firms may well be evaluated.

⁸ GLB Section 502(e) provides:

- e) General Exceptions.--Subsections (a) [Notice] and (b) [Opt-out] shall not prohibit the disclosure of nonpublic personal information--
 - (1) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with--
 - (A) servicing or processing a financial product or service requested or authorized by the consumer;
 - (B) maintaining or servicing the consumer's account with the financial institution, or with another entity...

Although the SEC coordinated with the federal bank Interagency group in the drafting of the initial template of privacy notice and opt-out provisions that the GLB Act ordained for all financial institutions, the SEC did not participate in the framing of the new data security rules, has not proposed its own rules and does not intend to issue rules on this subject. In enacting Regulation S-P the SEC merely restated the text of GLB §501(b) substituting BDs, investment advisers and investment companies as actors in place of the statute's command of agency action and substituting "policies and procedures" by the firms in lieu of agency standards, §248.30. The NASD in Notice To Members 00-66 has indicated that it will not enact further rules. <http://www.nasdr.com/pdf-text/0066ntm.txt>

The Federal Trade Commission, which has jurisdiction of a variety of financial service firms, steered a middle course—its Security Standards are more fully considered than the SEC but far less prescriptive than those of the Bank Interagency Guidelines. The sections that follow examine the FTC approach and the detailed requirements for banks. As noted above, the FTC has been applying its Rule to non-financial firms via enforcement proceedings.

2. FTC Financial Data Safeguards Rulemaking

On August 31, 2000 the FTC sought comment, pursuant to GLB section 501(b), on developing an "administrative, technical, and physical information Safeguards Rule for the financial institutions under its jurisdiction, see GLB section 505(a)(7), <http://www.ftc.gov/os/2000/05/65fr33645.pdf> . The FTC invited comment on whether it should pursue an approach similar to the detailed guidelines of the federal banking regulators or that of the SEC that merely rested the 501(b) statutory objectives.

The Securities Industry Association ("SIA") submitted an October 21, 2000 comment letter in which it urged that the FTC follow the SEC approach and accord flexibility in implementation of the Act and eschew detailed requirements. http://www.sia.com/gramm_leach_bliley/html/privacy_provisions_-_comment_1.html.

Indeed, the SIA distinguished the bank regulators actions from that of the SEC due to the direction in the Act that the banking agencies issue standards pursuant to section 39(a) of the Federal Deposit Insurance Act, which authorizes prescriptive rules for internal controls, information systems and internal audit systems. No similar GLB directive exists in GLB for the SEC and the FTC.

On May 23, 2002 the FTC published *Standard for Safeguarding Customer Information* for certain financial firms under the GLB Act jurisdiction of the FTC, 67 FR 36484, 16 CFR Part 314. The rules become effective on May 23, 2003⁹, except that for contracts with unaffiliated vendors entered into prior to June 24, 2002 the compliance date is May 23, 2004 even if the contract does not include a requirement that the service provider maintain appropriate safeguards for customer

⁹ 16 CFR §315.5(a).

information, 16 CFR §315.5(b). The FTC's mandatory five elements for an information security plan are specified in §314.4:

(a) **Designate an employee** or employees to coordinate your information security program.

(b) **Identify reasonably foreseeable internal and external risks** to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information **safeguards to control the risks** you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) **Oversee service providers**, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) **Evaluate and adjust** your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

3. **Bank Interagency Guidelines for Customer Information**

_ **Overview of Requirements for an Information Security Program.** The central elements of an information security program are:

- Assess Risk.
- Manage and Control Risk.
- Oversee Service Provider Arrangements.
- Obtain program approval by the Board of Directors.
- Implement the Standards by 7/1/01.
- Continuously monitor and adjust the program.
- Report regularly to the Board.

_ **Standards for Safekeeping Customer Information:**

- Banks must implement a comprehensive, written information **security program** that includes the following **elements**: (i) administrative, (ii) technical and (iii) physical safeguards appropriate to the nature and scope of its activities.
- **Risk Assessment** has the following required elements:
 - ◊ identify reasonably foreseeable threats, both internal and external;
 - ◊ assess the likelihood and potential damage from these threats; and
 - ◊ evaluate the policies & systems in place to control the risks.
- The **Risk Management** program must consist of the following elements:
 - ◊ Program must be commensurate with the nature of the firm's business and consider the following design elements:
 - ‡ system access controls;
 - ‡ physical access restrictions;
 - ‡ encryption;
 - ‡ segregation of duties (dual control procedures);
 - ‡ intrusion monitoring;
 - ‡ mitigation measures for environmental hazards and technology failures;
 - ‡ scripted response scenarios for event scenarios; and
 - ‡ security review procedures of system changes.
 - ◊ Train staff to accomplish the security plan.
 - ◊ Regularly test the systems, procedures and controls.
- The **Oversight of Vendor** Arrangements requires:
 - ◊ Exercising Due Diligence in vendor selection.
 - ◊ Contractually requiring vendors to meet the firm's security measures.
 - ◊ Monitoring vendors via periodic reviews of "audits, summaries of test results, or other equivalent evaluations."

These regulatory requirements must be reflected in agreements entered into with vendors after 3/5/01. Vendor relationships established by contracts entered into prior to this date have until 7/1/03 to come into compliance.

The adopting release also indicates that the bank regulators are not insisting upon on-site inspections by firms. Further, of the three types of information that banks might require and review, the regulators express the highest credence to AICPA Statements of Auditing Standards ("SAS") 70 reports. SAS 70's, the release states, "may enable an institution to assess whether its service provider has information security measures that are consistent with representations made to the institution during the service provider selection process."

- Management must **continuously adjust** the security program (section III-E of the release). Several examples are enumerated of circumstances warranting

further inquiry, including (i) changes in technology generally or a firm's own systems; (ii) internal or external threats; and (iii) changing business arrangements, e.g., mergers and acquisitions, outsourcing arrangements.

In the broker-dealer context, NASD Rule 3010 may be a vehicle for regulators to assert that a firm must have a documented, supervisory program and that the firm verify compliance by periodic inspection procedures.

- The Board **oversight function** includes approval of the initial plan and monitoring of management's continuing responsibilities. 12 CFR §30.3, Appendix B, III-A and III-F. The enacting release justifies Board involvement on the basis that data security is "critical to the safety and soundness of the institution." 66 FR at 8620. "Day-to-day monitoring...is a management responsibility," but the "lines of authority and responsibility for development, implementation, and administration...need to be well defined and clearly articulated." *Id.*

A report to the Board must occur at least annually and address the following elements:

- ◇ status of the program and compliance with the guidelines;
- ◇ risk assessment;
- ◇ risk management and control decisions;
- ◇ results of testing;
- ◇ security breaches or violations and management's responses; and
- ◇ recommendations for program changes. 66 FR at 8634.

In holding company structures the bank regulators agree that it is appropriate for the parent organization to articulate the security program. However, each subsidiary "must conduct an **independent review** to ensure that the program is suitable" and in compliance with the requirement's of the subsidiary's primary regulator. *Id.*

A high level of intrusive, regulatory scrutiny of data security measures emerges in these provisions and in the remarks of the accompanying release. It is even more evident in several elements that were proposed but withdrawn from the final regulation, namely, (i) a requirement to designate a "Corporate Information Security Officer"—though a footnote observes that 12 CFR §208.61(b) already requires such a designation; (ii) a mandate for specific types of tests; (iii) a mandate that firms use third party auditors or evaluators; and (iv) a management prescription that it must:

- ◇ evaluate the consequences for the security program of changes in IS and business arrangements;
- ◇ document compliance with the guidelines; and
- ◇ keep the board informed of the "overall status" of the security program. 66 FR 8621-7.

- Banks were required to implement their security programs must by the effective date of the GLB provisions of July 1, 2001.

D. GLB Compliance Inspection & Examination Issues

_ Representatives of the SEC, the NASD and NASAA (the association of state securities regulators) have indicated that they will engage in Inspections & Examinations to determine compliance with the requirements of Title V of GLB. To date there have been no publicly announced enforcement actions stemming from violations of GLB privacy or security provisions.

_ Likely areas to be probed by regulators are:

- ◇ Comparison of firm notices with their actual practices.
- ◇ Review of written supervisory procedures to determine if the practices described in the notices are supported by effective supervisory procedures.
- ◇ Determine if appropriate training has been given to firm employees.
- ◇ Determine if appropriate supervisors have been designated to carry out the operational elements of GLB, especially in the areas of network security, marketing arrangements and data access controls.
- ◇ Compare vendor contracts with firm notices.
- ◇ Assess industry reliance on the transmission of PII via unencrypted email to customers. The SEC's Office of Compliance and Inspections ("OCIE") previewed this issue in its report of January 25, 2001 on online brokers.
- ◇ Determine industry practices in the area of vulnerability assessments. Here OCIE will be seeking to better understand both potential threats and readiness of firms to meet these threats.

_ OCIE's January 25, 2001 Online Report addressed security measures and made recommendations for online brokers. OCIE's major findings and recommendations in the Report are:

- ◇ **Email:** Only about one third of the online firms examined used some form of email encryption and 20% had written policies on employees sending confidential information in unsecured email or warned firms about sending such information via email.

While the report implicitly criticizes sending personal information to customers in unencrypted email, the SEC's Division of Market Regulation has not required that monthly statements, trade confirmations or notices be disseminated via secure email. There are vendor solutions that enable the delivery of these documents in a secure manner.

- ◇ The Report urges that there be both better communication with customers about the insecurity of email and adoption of written, internal policies.

- ◇ **Firewalls:** The majority of firms were found to have multiple levels of firewalls and about one-third periodically employed outside consultants to

their security vulnerabilities. The SEC urges firms to consider hiring such outside consultants.

◇ **Passwords:** The SEC criticizes policies that result in non-secure passwords, the resetting of passwords or the changing of forgotten/lost passwords.

◇ **Session Cookies:** The SEC criticizes the use of session cookies that permit a user to log in with their password only once without forcing reauthentication after a period of nonuse. The risk is that another person with access to the computer could thereby access the account.

E. GLB Litigation Issues

_ **Private Rights of Action:** Title V of the GLB Act does not expressly provide a private right of action. The provisions of Title V appear to rely primarily on agency rulemaking and enforcement (§§ 522 and 525) supplemented by criminal penalties for certain conduct involving obtaining customer information by false pretenses (§§ 521 and 523).

_ The reliance upon agency enforcement and the absence of “rights creating language” appears to compel a determination that no private right of action arises under Title V of the GLB Act. *Alexander v. Sandoval*, 2001 U.S. Lexis 3367 (April 24, 2001) (Scalia, 5-4), *citing*, *California v. Sierra Club*, 451 U.S. 287, 294, 68 L. Ed. 2d 101, 101 S. Ct. 1775 (1981)(“ Statutes that focus on the person regulated rather than the individuals protected create no implication of an intent to confer rights on a particular class of persons.”).

_ The GLB Act alone, however, does not conclude the matter of whether private actions may ensue. Any firm subject to and in compliance with Title V will have delivered to its customers a detailed notice of its practices which requires renotification and an opt-out opportunity before any disclosure “other than as described in the...notice,” §248.8(a). The FTC and state AGs have demonstrated that a departure from these policies will be redressed as a deceptive business practice under Section 5 of the FTC Act and in state counterparts.

_ *Individual Reference Services Group, Inc. v. FTC*, 2001 U.S. Dist. Lexis 5732 (DC April 30, 2001) sustained the FTC, FDIC, OCC, OTS and NCUA privacy regulations in a suit attacking them as unconstitutional and arbitrary and capricious. The SEC was not named as a party.

IV. Health Insurance Portability and Accountability Act¹⁰ (“HIPAA”)

HIPAA applies to the health care industry and authorizes the Department of Health and Human Services (“HHS”) to issue regulations concerning the physical and electronic security of personally identifiable health information obtained by firms.

¹⁰ Public Law 104-191, August 21, 1966; *see* Part C, Title XI, §§1171-79.

HHS has completed the issuance of privacy rules.¹¹ HIPAA's proposed final Security Rule is expected to be issued in the fall of 2002. HHS has stated that the Security Rule will apply only to the maintenance and transmission of electronic forms of identifiable health information. The Security Rule as proposed sets forth administrative, physical and electronic safeguards for protected health information.¹² When proposed four years ago the Security Rule was to become effective two years after enactment (three years for small health care providers).

V. Duty of Care & Tort Liability

A. Negligence

_Breach of Fiduciary Duty. Where a relationship of trust and confidence exists the law imposes a duty of care. The Department of Interior's failure to safeguard and secure Indian trust funds within its care has produced the most compelling series of decisions detailing the IT failures,¹³ the consequent embargoing of Interior from the Internet¹⁴ and the agency's efforts under the watchful scrutiny of a Special Master, the Indian plaintiffs and the Court to restore Interior's connection to the wired environment.¹⁵

_Duty of Care, Foreseeability. The elements for negligence claims are: (i) a duty of care is owed, which may arise from a special relationship, (ii) a breach of the duty and (iii) injury proximately caused by the breach of the duty. Relationships of bailment and of common carriers may be sufficiently analogous to persuade courts that a duty arises for businesses that obtain and maintain electronic information files. Even in the absence of any special relationship every person

¹¹ Standards for Individually Identifiable Health Information, 65 FR 82461 (December 28, 2000) and 67 FR 53182 (August 14, 2002)(effective April 14, 2003, except for certain small plans that will have an additional year to comply);

¹² Security and Electronic Signature Standards, 63 FR 43242 (August 12, 1998); proposed 45 CFR §162.

¹³ *Cobell v. Norton*, 2001 Lexis 20453 (D DC)(200 page Report of Special Master filed December 6, 2001) citing *Ripley v. Denver U.S. Nat'l Bank*, 273 F. Supp. 718, 735 (D. Col. 1967)("It is generally agreed that a trustee owes a duty to his beneficiaries to exercise such care and skill as a man of ordinary prudence would exercise in safeguarding and preserving his own property."); Rest. 2d Trusts § 173 (Comment c)(trustee should preserve records in a manner that provides trust beneficiaries access "to such information as is reasonably necessary to enable [them] to enforce [their] rights under the trusts or to prevent or redress a breach of trust."); 205 F.R.D. 52, U.S. Dist. Lexis 422 (January 15, 2002)(adopting Report of Special Master).

¹⁴The Court entered a temporary restraining order on December 5, 2001 requiring that all IT systems that contain Indian trust data be disconnected from the Internet together with all PCs that may access systems that contain trust data. *Cobell v. Norton*, 184 F.Supp. 2d 1, U. Dist. Lexis 1710 (February 5, 2002)(2d Status report of Special Master describes December 5, 2001 TRO and December 17, 2001 Order regarding process for re-establishing Internet services to Dept. of Interior).

¹⁵*Cobell v. Norton*, 2001 U.S. Dist. Lexis 20907 (December 17, 2001); 206 F.R.D. 27; 2001 U.S. Dist. Lexis 12591 (Court Monitor appointed) (April 16, 2001); 2002 U.S. Dist. Lexis 5291 (March 29, 2002)(sanctions against defendants' for protective order motion); 201 F. Supp. 2d 145; 2002 U.S. Dist. Lexis 9720 (May 17, 2002) (slipshod and haphazard way in which the Interior Department continues to carry out its solemn trust responsibilities).

owes a duty of ordinary care to every other person to prevent any foreseeable injury from occurring to such other person. The want of care and appropriate skill in operating a business that maintains consumers' health data or credit card numbers leads to clearly foreseeable potential injury claims.

_ **Strict Liability in Tort.** Products of inherent dangerousness to the user may give rise to strict liability. *Restatement (Second) of Torts* §402A. Product liability claims have been asserted against America Online for damages caused to computers and data from AOL's online access software Version 5.0.¹⁶

_ **Invasion of Privacy.** Unauthorized disclosure of private information may be actionable as a common law invasion of privacy.¹⁷ Hence, a victim of identity theft might assert that the failure to employ adequately trained employees and systems to safeguard personal data led foreseeably to a customer's injury.

B. Best Practice Guides

The touchstone for these tort issues is that a failure to observe generally recognized standards applicable to any given area of endeavor is evidence from which one can infer that a non-compliant firm has failed to exercise reasonable prudence.¹⁸ If management knows that important aspects of its operations are not compliant with industry-wide "best practices," and that material adverse consequences will follow for its customers, whether from a data integrity, unauthorized account access or potential identity theft event, due to a breach of data security, the failure to have warned of this non-compliance may constitute a basis for liability.¹⁹

While awareness of a material gap between a company's practices and "best practices" may initially seem to be a significant proof hurdle, the pervasiveness of self-assessment management models and continuous process improvement disciplines virtually ensures that every enterprise has staff that is aware of the relevant best practices and how their enterprise compares.²⁰ Further, consultants retained by firms confronting IS challenges frequently invoke applicable "best practice" yardsticks in critiquing the circumstances that they find.

The lesson of "best practices" is that standards must be universal. If this is an unflattering comparison, then the decision to deploy systems or retain vendors that have not been adequately assessed will potentially constitute recklessness.

¹⁶ See *In Re AOL Version 5.0 Software Litigation*, 168 F. Supp. 2d 1359, 2001 U.S. Dist. Lexis 6595 (S.D. FL)(dismissing claims under the Computer Fraud and Abuse Act, 18 U.S.C. §1030, and abstaining on state liability claims). In a related proceeding, *AOL v. St. Paul Mercury Ins. Co.*, 207 F. Supp. 2d 459, 2002 U.S. Dist. Lexis 11346 (E.D. VA), AOL's commercial general liability policy was found not to cover damage to intangible (data) property.

¹⁷ See, *Restatement (Second) of Torts* §652D (1976); *Coverstone v. Davies*, 38 Cal. 2d 315, 322 (1952); *Forsher v. Bugliosi*, 26 Cal. 3d 792, 808 (1980).

¹⁸ *Restatement (Second) of Torts* §§ 295A (Custom), 299 (Want of Competence) & 299A (Undertaking in Performance or Trade)

¹⁹ Moreover, these facts may also support both consumer fraud actions, see Section II.

²⁰ See James Cortado, *Best Practices in Information Technology* (1998).

Although no overarching institutional paradigm has yet been framed for e-commerce or technology-dependent firms, numerous formulations of "best practices" exist for both quality management practices and for software development processes. The GLB and HIPAA inspired Safeguard Rules may become judicial sources in measuring negligence. Other federal and state statutes applicable to the government's management of its information systems are, together with the body of standards that they create, similar candidates.

1. Federal Security Guidelines

_ The Government Information Security Reform Act ("GISRA"), P.L. 106-398, Title X, Subtitle G, 44 U.S.C. §§3531-5, October 30, 2000, requires federal agencies, *inter alia*, to: (i) implement efforts to secure electronic information, (ii) thoroughly assess their security management practices, (iii) maintain procedures for detecting, reporting and responding to security incidents, (iv) annual self-assessment of security programs, technology, processes and personnel, and (v) reporting of findings of significant deficiencies. Amendments to GISRA are being considered that would require agencies to implement best practices.

_ The Clinger-Cohen Act of 1996, (formerly known as the Information Technology Management Reform Act), 40 U.S.C. §1401 et seq., directs executive agencies to establish the position of Chief Information Officers and places responsibility on the CIO for "providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency technology architecture for the executive agency; and promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency."

_ The Computer Security Act of 1987, 40 U.S.C. §1441 et seq., P.L. 100-235, (amended by the Clinger-Cohen Act), requires the government to promulgate standards for computer security, train relevant employees in computer security and establish plans for the security and privacy of computer information. In relevant part, the Act requires that "each federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use or operation of each system within or under the supervision of that agency," and "establish a plan for the security and privacy of each federal computer system . . . that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information c o n t a i n e d i n s u c h s y s t e m . "

_ The Office of Management and Budget Circular A-130, *Management of Federal Information Resources* (Nov. 28, 2000) and Appendix III to Circular A-130, establishes policies for the management of Federal information resources. Circular A-130 directs agencies to "plan in an integrated manner for managing information throughout its life cycle" and requires that agencies "ensure that information is protected commensurate with the risk and magnitude of the harm that would

result from the loss, misuse, or unauthorized access to or modification of such information,” and that agencies “must make security's role explicit in information technology investments and capital programming.” The Circular also sets out specific guidelines for agencies to ensure the security of information systems.

_ Office of Management and Budget Circular A-123, *Management Accountability and Control* (June 21, 1995), “provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls.”

_ The Office of Management and Budget Circular A-127, *Financial Management Systems* (July 23, 1993), prescribes “policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems.”

_ OMB Bulletin No. 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information* (July 9, 1990), whose purpose is to provide guidance to Federal agencies on computer security planning activities required by the Computer Security Act of 1987. This Bulletin supersedes OMB Bulletin No. 88-16, “Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information” (July 6, 1988).”

_ Memorandum for the Heads of Departments and Agencies from Office of Management and Budget (February 28, 2000) directs agencies to plan for IT Security needs, by making “security's role explicit in information technology investments and capital programming.”

_ National Security Telecommunications and Information Systems Security Committee Publication 1000, *National Information Assurance Certification and Accreditation Process* (April 2000), establishes a “standard national process, set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system or site.”

2. National Institute of Standards and Technology ("NIST")

Finally, executive agencies, receive best practice guidance via pronouncements by NIST and the Federal Information Processing Standards (FIPS).²¹ These Guides

²¹ Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions. For general information see, <http://www.itl.nist.gov/fipspubs/geninfo.htm>.

include:

_ NIST Special Publication 800-10, *Keeping Your Site Comfortably Secure: an Introduction to Internet Firewalls* (Feb. 1995), provides a basic understanding of how firewalls work and the steps necessary for implementing firewalls. *Id.* at ix.

_ NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* (Sept. 1996), provides a baseline that organizations can use to establish and review their IT security programs. *Id.* at 1.

_ NIST Special Publication 800-12, *Introduction to Computer Security* (Oct. 1995). This NIST Handbook provides assistance in securing computer-based resources (including hardware, software, and data) by explaining important concepts, cost considerations, and interrelationships of security controls. It illustrates the benefits of security controls, the major techniques or approaches for each control, and important related considerations.

_ NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role and Performance Based Model* (April 1998), provides a framework for IT Security Training that is both “appropriate for today's distributed computing environment and [flexible] for extension to accommodate future technologies and the risk management decisions.” *Id.* at 4.

_ NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems* (Dec. 1998), details what should be done to enhance or measure an existing computer security program or to aid in the development of a new program. *Id.* at 2.

_ NIST Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)* (June 2001), presents a list of “system-level security principles to be considered in the design, development, and operation of an information system.” *Id.* at 1.

_ NIST Special Publication 800-31, *Intrusion Detection Systems* (Aug. 2001), is a primer on intrusion detection, how to select and configure intrusion detection systems for their specific systems and network environments, how to manage the output of intrusion detection systems, and how to integrate intrusion detection functions with the rest of the organizational security infrastructure. *Id.* at 5;

_ FIPS Publication 31, *Guidelines for ADP [Automatic Data Processing] Physical Security and Risk Management* (June 1974), which provides a handbook for use by “organizations in structuring physical security and risk management programs for their ADP facilities.” *Id.* at 1.

_ FIPS Publication 73, *Guidelines for Security of Computer Applications* (June 1980), describes “methods and techniques that can reduce the hazards associated with computer applications.” *Id.* at 1.

_ FIPS Publication 83, *Guideline on User Authentication Techniques for Computer*

Network Access Control (Sept. 1980), provides guidance in the “selection and implementation of techniques for authenticating the users of remote terminals in order to safeguard against unauthorized access to computers and computer networks.” *FIPS Publications*, <http://www.itl.nist.gov/fipspubs/by-num.htm>.

_ FIPS Publication 87, *Guidelines for ADP Contingency Planning* (March 1981), describes for organizational and data processing management the relevant considerations when developing a contingency plan for an ADP facility. *Id.* at 1.

_ FIPS Publication 102, *Guidelines for Computer Security Certification and Accreditation* (Sept. 1983), describes how to establish and carry out certification and accreditation programs for computer security. *Id.* at 1.

_ FIPS Publication 112, *Password Usage* (May 1985), establishes the basic criteria for the design, implementation and use of a password system as an access control technique. <http://www.itl.nist.gov/fipspubs/fip112.htm>.

_ FIPS Publication 191, *Guidelines for the Analysis of Local Area Network Security* (Nov. 1994), discusses threats and vulnerabilities and addresses security mechanisms for Local Area Networks. <http://www.itl.nist.gov/fipspubs/fip191.htm>.

VI. State Legal Authorities

A. Right of Privacy Statutes and Constitutional Provisions

State constitutional provisions, case law and statutes are a potential source of privacy rights that may be invoked by customers of a firm whose information may have been accessed without their consent. California, for example, is one of a number of states that has enacted protections relating to health records. These include mandating that: (i) off-site back-up storage of electronic records exists and (ii) electronic records are unalterable. A good source that collects the myriad (and growing) array of state privacy protections is <http://www.epic.org/privacy/consumer/states.html>.

B. State Information Security Provisions

The increasing incidence of identity theft and dramatic events such as Eli Lilly's negligent disclosure of Prozac patients has heightened public awareness of the harm that can arise from lapses in information security protections. A product of such attention will be, unless pre-empted by national legislation, state statutes attempting to dictate the rules of cyberspace. An example of such a bill is California Senate Bill 1386 that was awaiting Senate concurrence in Assembly amendments on August 28, 2002.²² The Bill defines a breach of the security of a system and requires, unless law enforcement requests otherwise, that anyone whose unencrypted personal information has been acquired receive the “most expedient” notification of the breach. Customers are further afforded a right of action for damages and injunctive relief. The law would be applicable to any

²² See http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_1386&sess=CUR&house=S.

person doing business in California. The law is proposed to become effective on July 1, 2003.

VII. International Legal Authorities

A. Organization for Economic Cooperation and Development (OECD)

The OECD Council adopted and released on July 25, 2002 *Towards a Culture of Security*, its Guidelines for the Security of Information Systems and Networks, www.oecd.org/sti/security-privacy. The Guidelines represent the consensus views of all 30 OECD member countries and support the OECD's larger goal of promoting economic growth, trade, and development. Although the Guidelines are voluntary, they represent a consensus among OECD governments resulting from discussions that also involved representatives of the information technology industry and consumer advocates. OECD members, industry, and other participants will draw on the Guidelines in establishing policies, measures and training programs for online security.

The Guidelines encourage governments in other countries to adopt a similar approach, and ask businesses to factor security into the design and use of their systems and networks and provide security information and updates to users. The Guidelines urge all individual users to be aware and responsible and take preventive measures to lessen the security risks inherent in an interconnected world. These Guidelines replace the Guidelines for the Security of Information Systems that the OECD issued in 1992.

The Guidelines consist of nine principles that aim to increase public awareness, education, information sharing, and training that can lead to a better understanding of online security and the adoption of best practices. The nine principles of the newly announced Security Guidelines include:

- *Awareness* Participants should be aware of the need for security information system and networks and what they can do to enhance security.
- *Responsibility*. Participants are responsible for the security of information systems and networks.
- *Response*. Participants should act in a timely and cooperative manner to prevent, detect, and respond to security incidents.
- *Ethics*. Participants should respect the legitimate interests of others and recognize that their action or inaction may harm others.
- *Democracy*. The security of information systems and networks should be compatible with essential values of a democratic society.
- *Risk Assessment*. Participants should conduct risk assessments to identify threats and vulnerabilities to their information systems.
- *Security Design and Implementation*. Participants should incorporate security as an essential element of information systems and networks.
- *Security Management*. Participants should adopt a comprehensive approach to security management.

- *Reassessment.* Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, measures, and practices.

B. European Union & Members

_ European Union Data Protection Main Page:

http://europa.eu.int/comm/internal_market/en/dataprot/

_ Council of Europe Data Protection Main Page:

http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/

C. Additional Resources

_ International Organization for Standardization: ISO 17799. This is a comprehensive standard outlining best practices for system access control, maintenance and development, physical security, compliance, personnel security, computer and operations management and security policy. <http://www.iso17799software.com/>. The Geneva-based ISO has also promulgated a series of five widely recognized standards, the ISO 9000 series, pertinent to software development, acquisition and the minimum requirements for a quality assurance.

_ Canada: Personal Information Protection and Electronic Documents Act (April 13, 2000) http://www.privcom.gc.ca/legislation/02_06_01_e.asp .

_ Links to International Data Protection Agencies and Authorities:

<http://www.privacyexchange.org/gpd/sites/dpcsites.html>

_ Data Privacy in Latin America:
<http://www.ulpiano.com/dataprotectionenglish.html>

_ Australian Office of the federal Privacy Commissioner,
<http://www.privacy.gov.au/>; Data Security Requirements,
<http://www.privacy.gov.au/publications/dnppg.html#7>

TABLE OF RESOURCES: BEST PRACTICES FOR NETWORK SECURITY

⋮

WILLIAM H. MOHR
Former Assistant General Counsel
Datek Online Holdings Corp.
wmohr@nyc.rr.com

9-02	[Announced Schedule] US Critical Infrastructure Protection Board to release national plan to bolster information security.
8-28-02	Ziff Davis Media reached a settlement with the New York Attorney General (NYAG), the CAAG and the VTAG regarding a November 2001 incident in which records of 12,000 subscribers were rendered accessible, some of whom became victims of identity fraud. The states invoked deceptive business practice statutes based upon Ziff's privacy pledge of "reasonable security precautions." Ziff must pay \$500 each to 50 persons whose credit card data was accessed, augment security practices and supply reports to the AGs. http://www.wired.com/news/business/0,1367,54817,00.html
8-26-02	DoubleClick settlement (PDF) pact with the NYAG and 9 other state addresses its use of cookies and web beacons. DCLK agreed to (i) provide a limited "cookie viewer" that will permit consumers to see the profile categories maintained by DCLK from its data harvesting web surfers, (ii) require DCLK to monitor sites using its services to correctly disclose its data collection practices, (iii) effect certain changes in its privacy policies and (iv) conduct 3 outside reviews of its policies over the next 4 years. In May 2002 DCLK settled private lawsuits relating to its privacy practices and agreed to pay attorneys fees of \$1.8 million. http://www.oag.state.ny.us/press/2002/aug/aug26a_02.html

8-22-02	<p>FBI Raids Firm After Hacking Claim, AP, August 22, 2002. Hours after the claims of weak Defense Department security made by a web security firm were reported in a front-page article in The <u>Washington Post</u>, the FBI began searching the firm's offices. "Regardless of the stated intent, unauthorized entry into Army computer systems is a federal offense," said Marc Raimondi, spokesman for the Army Criminal Investigation Command in Virginia. "If there is an intrusion and we are notified or we detect it, then we launch a criminal investigation into the act."</p> <p>http://www.washingtonpost.com/wp-dyn/articles/A50628-2002Aug22.html</p>
8-16-02	<p>Sleuths Invade Military PCs With Ease, Robert O'Harrow, Jr., <u>Washington Post</u>, Friday, August 16, 2002; Page A01. ForensicTec, a San Diego web security firm, said it identified 34 military sites where they said network security was easily compromised, including Army computers at Fort Hood, Texas; NASA's Ames Research Center in Northern California and Navy facilities in Maryland and Virginia.</p>
8-9-02	<p>Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed GAO-02-918T July 9, 2002 Accessible Text. Potential benefits for this division include more efficient, effective, and coordinated programs; better control of funding through a single appropriation for the new department and through establishing budget priorities for transferred functions based on their homeland security mission; and the consolidation of points of contact for federal agencies, state and local government, and the private sector in coordinating activities to protect the homeland. Finally, the new department will also face challenges, such as developing a national critical infrastructure protection strategy, improving analytical and warning capabilities, improving information sharing on threats and vulnerabilities, and addressing pervasive weaknesses in federal information security.</p>
8-8-02	<p>Microsoft Settles FTC Charges Alleging False Security and Privacy Promises concerning its "Passport Single Sign-In, Passport 'Wallet,' and Kids Passport. MSFT agreed to (i) maintain a comprehensive security program, (ii) submit to the FTC biennial third-party inspections of its practices over the next 20 years, and (iii) cease misrepresenting its data services and products. The FTC did not charge that any data was compromised or unlawfully accessed.</p> <p>http://www.ftc.gov/opa/2002/08/microsoft.htm, FTC Consent Order (PDF)</p> <p>http://www.ftc.gov/os/2002/08/microsoftagree.pdf</p>
8-2-02	<p>Hewlett Packard threatened a lawsuit against a small security consulting firm on the basis of provisions of the Digital Millennium Copyright Act, 17 USC §1201, and the Computer Fraud and Abuse Act, 18 USC § 1030(c)(3) and (4), for posting a buffer overflow exploit of Tru64 UNIX. http://www.wired.com/news/print/0,1294,54297,00.html</p>

7-25-02	The Organization for Economic Cooperation and Development (OECD) Council adopted and released on July 25, 2002 <i>Towards a Culture of Security</i> , its Guidelines for the Security of Information Systems and Networks, www.oecd.org/sti/security-privacy . The Guidelines represent the consensus views of all 30 OECD member countries and support the OECD's larger goal of promoting economic growth, trade, and development. Although the Guidelines are voluntary, they represent a consensus among OECD governments resulting from discussions that also involved representatives of the information technology industry and consumer advocates.
6-26-02	IT Experts Say Government Not Ready for Cyber Attack, Ellen McCarthy, <i>Washington Post</i> , June 26, 2002. Released in conjunction with this week's E-Gov conference in DC, a Business Software Alliance sponsored survey of IT staff found that, "almost half of information technology workers who participated in the survey think a major cyber-attack in the United States is likely to occur in the next 12 months. And nearly three-quarters think there is a gap between the likelihood of a major cyber-attack in the United States and the government's ability to defend itself." "Two-thirds of companies are not reporting cyber-attacks and breaches. It breaks the trust model," said William Conner of Entrust Inc. "Until we understand where we're at, it's going to be difficult to get the sense of urgency we need." http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A47680-2002Jun26&notFound=true http://www.bsa.org/usa/press/newsreleases//2002-06-25.1175.phtml
6-18-02	Internet Security Systems discloses security hole in Apache web software, open source code used in 60% of all web servers. Incident reveals that CERT, based at Carnegie Mellon and partially funded by the Defense Dept., does not share information with the National Infrastructure Protection Center (NIPC) within the FBI.
6-18-02	The President transmitted draft legislation to Congress for the creation of a Department of Homeland Security to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recovery from attacks that do occur. As proposed, functions of the Homeland Security Department's Information Analysis and Infrastructure Protection Division would include (1) receiving and analyzing law enforcement information, intelligence, and other information to detect and identify potential threats; (2) assessing the vulnerabilities of the key resources and critical infrastructures; (3) developing a comprehensive national plan for securing these resources and infrastructures; and (4) taking necessary measures to protect these resources and infrastructures, in coordination with other executive agencies, state and local governments, and the private sector. To create this division, six federal organizations that currently play a pivotal role in the protection of national critical infrastructures would be transferred to the new department.
5-23-02	67 FR 36484. FTC publishes Standard for Safeguarding Customer Information for certain financial firms under the GLB Act jurisdiction of the FTC, 16 CFR Part 314.

5-8-02	HR 4678 introduced by House Energy and Commerce Commerce, Trade and Consumer Protection Subcommittee Chairman Cliff Stearns, R-Fla. Section 105 of the Bill requires firms that collect data to maintain security programs and to effect remedial actions within a reasonable period of time upon notice from CERT or the federal government of a security matter.
2-02	President Bush proposes an additional \$4 billion in security spending in his 2003 budget request. Much of that funding is earmarked for electronic security measures.
1-14-02	US Comptroller of the Currency, OCC Bulletin 2002-2, Guidance on ACH transactions involving the Internet. Bulletin calls attention to the warranties made in ACH transactions by originating institutions under NACHA rules and the need for security measures to control risk and detect fraudulent transactions.
1-7-02	Computer Science and Telecommunications Board, <i>Cybersecurity Today and Tomorrow: Pay Now or Pay Later</i> , National Academy Press, Washington, DC, www.cstb.org
1-10-02	<u>NYLJ</u> , Ira M. Golub & Edward S. Kornreich (Proskauer Rose), <i>Grappling With New Health Privacy Rules</i> , concludes that “it is generally anticipated that the new HIPAA privacy protections will be considered by many courts to create a new standard of reasonable prudent practice in the care of individually identifiable health data. Accordingly, it is predicable that in the years to come HIPAA standards will serve as the basis for state law actions seeking damages for the breach of an individual’ right to the confidentiality of his or her medical information.”
12-20-01	Microsoft Issue Windows XP Fix, AP Wire, MSFT “acknowledged that the risk to consumers was unprecedented because the glitches allow hackers to size control of all Windows XP operating system software without requiring a computer user to do anything more except connect to the Internet.” The holes were discovered by reformed 21-year-old hacker, Marc Maiffret who has advised WH, FBI and testified before Congress. The exploit of the “universal plug and play” feature allows in MSFT’s words, “the first network based remote compromise” of a Windows desktop system.
12-11-01	SW, High Anxiety: Information Technology Assn. Of Am. (ITAA) Poll Finds Almost Three of Four Americans Concerned About Cyber Security.
12-10-01	Network Interoperability Consultative Committee (“NICC”) to the Office of Telecommunications (“OfTel”), Draft Guidelines on the Essential Require-ments for Network Security and Integrity, www.oftel.gov.uk/publications/ind_guidelines/esre1201.htm
12-5-01	CNET, US Approves Stronger Encryption Standard, NIST (of Commerce) adopted the Advanced Encryption Standard (AES) to replace DES (56K 1977) and triple-DES. AES supports 128-bit, 192-bit and 256-bit keys and is based on the Rijndael (rhine doll) encryption formula.

12-4-01	CERT suffered another denial of service attack today; one suffered in May made the site unreachable for several days.
11-28-01	House passes HR 1259, Computer Security Enhancement Act of 2001, enhances NIST's role in establishing voluntary interoperability standards for PKI systems http://thomas.loc.gov/cgi-bin/query/D?c107:3:/temp/~c107RT9ivx::
11-15-01 Hearing	House Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce CYBER SECURITY: PRIVATE-SECTOR EFFORTS ADDRESSING CYBER THREATS
Statement	for the SIA of C. Warren Axelrod, Ph.D. (Pershing's Head of InfoSec), Board of Managers, FS/ISAC LLC (Financial Services Information Sharing and Analysis Center, <i>see</i> 5-98 entry). Deterrence has been low and the population of potential attackers is increasing rapidly; the greatest counter-force is information sharing. FOIA and AT issues need to be resolved to foster sharing of info with gov't. Pass the Critical Infrastructure Information Security Act of 2001, S1456 (Kyl-Bennett), http://thomas.loc.gov/cgi-bin/query/D?c107:1:/temp/~c107WHJKAj:: The Critical Infrastructure Assurance Office (CIAO) has coordinated the drafting of sector plans including one for the Banking/Finance sector. These plans should become the basis for a national strategy for homeland security. The building of a separate, highly secure network must be considered. GovNet to be first. http://www.sia.com/testimony/html/axelrod_testimony_11-15-01.html
11-14-01	Reuters, ICANN Warned on Web Vulnerability, Researchers at an ICANN conf. Are worried that a an attack on the 13 root servers that direct computers to domain names or the 10 top-level domain servers was capable of bringing down the Internet. Registrars are another weak link; tampering could make it difficult to prove ownership of a domain. "The Internet is relatively fragile," said a participant.
11-9-01	AP, Gov't Networks Get an 'F', Agencies must report security efforts to OMB and GAO regularly hacks other agency computers. Failing agencies included Justice, Defense, Commerce, Transportation, Treasury, Energy, HHS and Interior; FEMA managed a D. The House Gov't Reform Comte headed by Stephen Horn announced the findings at a hearing today; a similar hearing on the topic was held earlier in the year.
11-9-01	AP, Cambridge students became the 2 nd group to crack IBM's DES standard s/w for bank ATMs. They published their on the Internet after IBM did not engage after attempts going back to April. The brute-force key attack was cut from 70 years to one day by attacking 16,384 keys at the same time. http://www.admin.cam.ac.uk/news/pr/2001110901.html]

11-5-01	Report of <i>Legal Times</i> Forum, <i>Securing E-Commerce</i> : Peter Swire (GWU) there's a proposed trespasser exception bill that would allow firms to invite FBI in to surveil trespassers on firm's system but current law lacks protection (suppression rule) for other communications intercepted; WorldCom counsel urged what and how long logs are maintained, intrusion detection capability, employee monitoring capability, and components of data security.
10-16-01	Executive Order on Critical Infrastructure Protection, No. 13231, http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html
10-01	President Bush establishes a federal Critical Infrastructure Protection Board, naming Clinton appointee Richard Clarke his special adviser for cyberspace security. The board is charged with making sure that state and local governments and non-governmental organizations are doing their respective parts to maintain effective warning systems and share information they receive about threats and attacks.
9-26-01	GAO Issues report on Infrastructure Protection finds that "significant pervasive weaknesses" in federal government security systems continue to put critical operations and assets at risk. http://www.gao.gov/new.items/d011168t.pdf
8-24-01	NYT, Carl Kaplan, Can Hacking Victims Be Legally Liable? Reports on two papers: (1) by Stanford Law's Margaret Jane Radin, " <i>Distributed Denial of Service Attacks: Who Pays?</i> " (commissioned by Mazu Networks of Cambridge, MA), concludes that there is a significant risk of liability of websites to customers from a DDOSA and of ISPs to attacked websites. Radin called the vulnerability of firms "staggering." She cited a Yankee Group estimate of \$1.2B in damages to DDOSAs and that the Computer Security Institute[http://www.gocsi.com] of SF survey found 1/3 rd had experienced a DDOSA. BD disclaimers might be found to be oppressive or lack proper consent. The ISPs are most vulnerable because they lack contractual disclaimers and may be found negligent if "preventive measures are reasonably effective and affordable." ISPs are in the "best position to take system-wide precautions, she said." http://www.mazunetworks.com/radin-toc.html (2) Alan Charles and Frank R. Volpe, " <i>Liability for Computer Glitches and Online Security Lapses</i> ," was published by the BNA Electronic Commerce Law Report, vol. 6, No. 31 (8-8-01) and urges that the implementation of aggressive security measures is necessary to stave off liability. www.sidley.com/cyberlaw/features/liability.asp
6-3-01	NYT, John Markoff & John Schwartz, Expert Says Windows XP Aids Vandals

4-26-01	<u>NYT</u> , Jennifer Lee, Punching Holes in Internet Walls
4-24-01	OCC Alert 2001-4, Network Security Vulnerabilities, advises banks and their service providers to review recent NIPC advisories on hacking of e-commerce sites and exploitation of “vulnerabilities in commercially available hardware and software.”
3-8-01	NIPC Advisory 01-003, <i>E-Commerce Vulnerabilities Update</i> , www.nipe.gov
2-1-01	66 FR 8616, Interagency Guidelines Establishing Standards for Safeguarding Customer Information
2-15-01	OCC Bulletin 2001-8: Guidelines Establishing Standards for Safeguarding Customer Information
12-28-00	HHS, Standards for Privacy of Individually Identifiable Health Information, 65 FR 82461.
12-1-00	NIPC Advisory 00-60, <i>E-Commerce Vulnerabilities</i> .
11-28-00	National Institute of Standards and Technology (“NIST”), Computer Security Division, Systems and Network Security Group, <i>Federal Information Technology Security Assessment Framework</i> , provides guidance for “consistent and effective measurement of their security status for a given asset...controls are documented, implemented, tested and reviewed, and incorporated into a cyclical review/improvement program.”
11-28-00	OCC Advisory Letter 2000-12, FFIEC Guidance on Risk Management of Out-sourced Technology Services
9-27-00	<u>WSJE</u> , Stacy Foster, <i>E*Trade Fixes Flaw That Left Accounts Open to Hackers—No Customer Data Appear to Have Been Compromised</i> . Bugtraq disclosed the flaw in the way ET stored account names and passwords in cookies, calling it “incredibly bone-headed” as it only took 30 minutes to unscramble the encoding mechanism.
8-31-00	FTC Notice for Comment, Administrative, Technical and Physical Information Safeguards Rule (pursuant to GLB § 501(b)).
— Comment	National Association of Consumer Agency Administrators (NACCA) Advocates minimum standards actionable by FTC/states as UFTP. www.ftc.gov/os/comments/glbcommentextension/nacca.htm
6-26-00	65 FR 39472, Notice for Comment, Interagency Guidelines Establishing Standards for Safeguarding Customer Information.

5-15-00	Final Report of FTC Advisory Committee on Online Access and Security recommends that the process elements of security programs should be specified (e.g., risk assessment, planning and implementation, internal reviews, training, reassessment) but that the substantive elements be flexible and measured by an "appropriateness under the circumstances" test. In consideration of Enforcement Alternatives, §4.1, ACOAS selected reliance on existing enforcement options based upon the posting upon a site of its security procedures and thence FTC, state and PROA arising from false statements. Third-party audit or assurance issuance was a second option. http://www.ftc.gov/acoas/papers/finalreport.htm
5-15-00	OCC Bulletin 2000-14, Infrastructure Threats – Intrusion Risks
2-00	A spate of crippling distributed denial of service (DDOS) attacks bring down several of the world's largest and most popular e-commerce sites, costing the companies millions in lost revenue. The attacks trigger a string of congressional hearings and legislative proposals aimed at closing security holes and intensifying the hunt for cyber vandals.
1-7-00	Publication of National Infrastructure Protection Plan laying out two broad goals: the establishment of the U.S. government as a model of information security, and the development of a public-private partnership to defend our national infrastructures. http://www.epic.org/security/CIP/WH_pr_1_7_00.html
11-12-99	Gramm-Leach-Bliley Act, P.L 106-102, becomes laws. Title V requires financial companies (e.g., banks, credit card issuers and brokers) to disclose privacy and security practices annually and at the point of establishing a customer relationship.
7-99	President Clinton signs the Year 2000 Readiness and Responsibility Act, which limits the legal liability of companies that make good faith efforts to fix their systems in advance of the date rollover. The law says companies being sued for technological failures may raise a Y2K defense if they can prove they took adequate steps to prepare their systems for the switch.
8-24-98	OCC Bulletin 98-38, Technology Risk Management: PC Banking
5-98	President Clinton appoints Richard Clarke National Coordinator for Critical Infrastructure Protection Security and Counter-terrorism. Clarke is charged with overseeing policies and programs relating to electronic security. Clarke repeatedly warns that the United States could face an "electronic Pearl Harbor" if it fails to beef up its cyber-defenses.
5-98	Presidential Decision Directive No. 63 on Critical Infrastructure Protection encourages gov't-industry cooperation via industry ISACs (Info. Sharing and Analysis Centers). Treasury is the designated partner for the banking/finance sector



4-98	U.S. Senate leaders empanel a special committee on Y2K readiness. Chaired by Utah Republican Robert Bennett, the committee keeps close tabs on businesses and government efforts to ready their systems for the date rollover. Although the committee is set to disband a few months after the date change, Bennett pushes to morph the panel into a permanent cybersecurity body following the date change. While the committee does disband, its efforts lay the groundwork for many later congressional cybersecurity efforts.
2-98	President Clinton appoints former Deputy Budget Director John Koskinen to chair his Year 2000 Conversion Council. The council centralizes executive branch efforts to ready government agencies for the date rollover. The council also becomes a template for later executive branch efforts to centralize oversight of cybersecurity threats.
7-15-96	President Clinton signs Executive Order establishing the President's Commission on Critical Infrastructure Protection and the Infrastructure Protection Task Force ("IPTF") within the Department of Justice, chaired by the FBI, to undertake interim coordinating mission. http://www.epic.org/security/infowar/eo_cip.html
7-96	Rep. Stephen Horn (R-Calif.) publishes his first quarterly Year 2000 readiness "report card," giving many agencies failing grades. Following the millennial date rollover, Horn issues similar report cards grading agencies on their cybersecurity readiness. In both cases, the grades, particularly the poor ones, spark greater scrutiny of federal information technology officials.
1991	Justice Dept. establishes computer crime and intellectual property section. Scott Charney heads the unit from 1991 until 1999. He is now the head of security for Microsoft.

COMPUTER CRIMES: An Overview of the Statutes and the Reporting Mechanisms

Joel Michael Schwarz
Department of Justice
Computer Crime and Intellectual Property Section
Criminal Division
(202) 353-4253 / Joel.Schwarz@usdoj.gov
<http://www.cybercrime.gov>

Today's goals

Discuss computer crime statutes that apply to:

-  Intruders in your system (ex. hackers, exceeding access authorization)
-  Employee misuse of your system (ex. stealing trade secrets, downloading child pornography, etc.)

Reporting computer crime and cooperating with law enforcement

1.

“There’s an intruder in my system!”

The Frantic Call from the Head of IT Security Management

“The head of your IT Security Management received an anonymous call this morning from someone claiming to have broken into your system, copied 500 customer account numbers and passwords, and uploaded a virus to cover his tracks. He is now threatening to post the account numbers and passwords on the Internet, as well as the backdoor that he used to get into your system, unless you give him \$500,000.” Subsequent investigation confirms this story

What Laws Could He Have Broken? Major network crimes (18 USC)

- Confidentiality: 1030(a)(2)
- + Fraud: 1030(a)(4) and 1343
- Damage (data or systems): 1030(a)(5)
- Password trafficking: 1030(a)(6), 1029
- Extortion: 1030(a)(7), 871 et seq.
- Attempt: 1030(b) covers all of 1030(a)

Obtains Information From Your System: 1030(a)(2)

- Intentionally accessing computer w/o or in excess of authorization
- And thereby obtaining information
 - (A) in a financial record or a credit report
 - (B) from a federal agency or
 - (C) from a "protected computer" if conduct involved an interstate communication
- Even if merely reading/browsing the info.
 - United States v. Czubinski, 106 F.3d 1069 (1997)

“Protected Computer”

- Key term #1: “Protected computer”
[defined in 1030(e)(2)]
 - (A) exclusively for use by financial institution or U.S. Govt. (or non-exclusive use, but conduct affects that use)
 - (B) used in “Interstate or foreign commerce or communication” (even computer located outside U.S. that is used in a manner that affects commerce)

Punishment for violating 1030(a)(2)

- Misdemeanor if no aggravating factors (and no previous offense)
- 5 year felony if:
 - for commercial gain
 - committed in furtherance of a criminal or tortious purpose
 - or value of information > \$5,000

Fraud: 1030(a)(4)

- Prohibits knowingly and with intent to defraud:
 - accessing a protected computer (without, or in excess of, authorization), and because of such conduct:
 - furthers the intended fraud (must have another action in addition to the access itself – ex. copying information which he will ransom); and
 - obtains anything of value
 - Object of fraud and thing of value obtained cannot be only the use of the computer itself, when that use is less than \$5000 in a one year period.
- Up to five year felony (unless previous offense)

Damaging Computers

Intentionally: 1030(a)(5)(A)(i)

- Prohibits knowingly causing the transmission of a “program, information, code, or command” and as a result of such conduct, intentionally causing “damage” (without authorization) to a “protected computer”
- Applies to insiders or outsiders
- Applies to viruses, even w/o “access”
- Up to ten year felony (unless previous offense)

“Damage” to a Protected Computer

- Key term #2: “Damage”
 - Defined as “any impairment to the integrity or availability of data, a program, a system, or information” causing:
 - a loss of at least \$5,000 within the period of a year; or
 - modification or impairment of medical records/data; or
 - physical injury to a person; or
 - threatening public health or safety; or
 - damaging system used in admin of justice, national security, or national defense

“Loss” includes cost of:

responding to offense, conducting damage assessment, restoring the data/program/system/information, and revenue lost/consequential damages suffered due to interruption of service

Damaging Computers: 1030(a)(5)(A)(ii)

- Prohibits intentionally accessing a protected computer without authorization and “recklessly” causing damage
- Applies only to outsiders
- Up to five year felony (unless previous offense)

Damaging Computers: 1030(a)(5)(A)(iii)

- Prohibits intentionally accessing a protected computer without authorization and as a result, causing damage [i.e. negligently causing damage]
- Applies only to outsiders
- Up to one year (unless previous offense)

Might Have A Violation Of 1030(a)(7) Threats to Damage a Computer

- Prohibits transmitting a threat to cause damage to a protected computer w/intent to extort any thing of value
- Up to 5 year felony (unless previous offenses)
- Query: Is threatening to post an unauthorized backdoor into your system a threat to "cause damage to a protected computer"?
- Consider – you might at least have: 18 USC 875(d) - Extortionate threats to injure the property of another

Civil Restitution – 18 USC 1030(g)

Civil restitution if:

- (i) loss of at least \$5000 during a 1 year period (if civil action is based only upon loss under this section - limited to economic damages);
- (ii) modification or impairment of medical exam, diagnosis, treatment or care (potential or actual)
- (iii) physical injury
- (iv) threat to public health or safety
- (v) damage affecting government computer system (relating to admin of justice, national security or defense)

You can also seek injunctive/equitable relief

2.

“What the @\$#%*& has my employee been doing on my system!”

The Frantic Call from the Head of IT Services

- “An employee traded in his laptop for a newer model. As the service technician was going through the laptop’s hard-drive, he found the source code for the new operating system you just released to compete with Unix and Windows. Since this employee works in human resources, there is no reason for the employee to have this sensitive information. The technician also found E-mails from the employee soliciting bids for this information from other companies.”

What Law Might Apply?

Theft of trade secrets: 18 USC 1832

- Defendant stole, or w/o authorization of owner, obtained, copied, destroyed, or conveyed information
- Defendant knew information was proprietary
- Information was a trade secret
- Defendant intended to convert the trade secret to economic benefit of someone besides the owner
- Defendant knew or intended that the owner of the trade secret would be injured
- Trade secret was related to a product that was produced for or placed in interstate or foreign commerce

Other statutes that an employee might infract (mostly 18 USC):

- Threats: 844(e), 875
- Harassment: 47 USC 223(a)(1)(C, E)
- Kiddie porn: 2252A
- Counterfeiting: 470-514
- Criminal copyright: 2319, 17 USC 506(a)
- Criminal trademark: 2320
- Economic espionage: 1831

If it looks like criminal activity, consider getting law enforcement involved

- **Statistics Suggest Victim Reporting is a Big Problem**

In the 2002 CSI/FBI survey, only 34% of the respondents who experienced computer intrusions reported to law enforcement.

Concerns about reporting: Myths and Realities

- **Concerns:**
 - Don't know who to call
 - Don't know whether law enforcement will be competent
 - Don't want to lose control of system
 - Don't think prosecutors will take the crime seriously
 - Don't want to challenge hackers

Who to call?

Number of Law Enforcement Agencies Prepared to Respond

- Plan (and meet) in advance
 - FBI's Infragard program
 - National Infrastructure Protection Center
Hotline: 202-323-3205 (888-585-9078)
 - NIPC Website: www.nipc.gov
 - E-Mail: nipc.watch@fbi.gov
 - CCIPS Website: www.cybercrime.gov
 - <http://www.cybercrime.gov/reporting.htm>
 - List of contact sources and numbers for reporting
cybercrime

Concerns about competency

- Law Enforcement won't understand intrusions.

Tremendous Increase in Law Enforcement's Ability to respond

- Lot of money and training poured into problem
- FBI: 17+ "Computer Crime Squads" in key cities around country
 - Well trained agents
- Agent with computer crime responsibilities in every FBI office
- Increasing Attention by Secret Service, Military, Postal Service, Customs, Agency IGs
- 11 CHIPS Units established in US Attorney's Offices around the U.S.
- Not all the way there, but getting better

Concern about Conduct of Investigation

- Will law enforcement agents seize critical data, and perhaps entire computers, and seriously jeopardize the normal operations of the company?
- Will the company totally lose control of the matter?

Law Enforcement's Sensitivity to Victim Entities

- Law Enforcement doesn't seize victim's computers
- Victims don't lose control; most investigations require intimate cooperation with the victim's system operator for technical operations.
- Victim consulted closely
- Often – interests are aligned
 - In order to secure systems after an attack a company will need to analyze systems and their logs to find holes
 - Law enforcement forensics will aid this process

Concern that Hackers will target Companies that Report

- Reputation for being a risk-free mark
- Must resist being a community of fear
- Even if don't report, look for means to share information
 - Infragard
 - Information Sharing and Analysis Center (ISACs)
 - CERT