2004 E-Crime Watch Survey™

Summary of Findings

Conducted by

CSO
The Resource for Security Executives

Carnegie Mellon
Software Engineering Institute
CERT® Coordination Center

Table of Contents

Purpose & Methodology

The 2004 E-Crime Watch survey was conducted by *CSO* magazine in cooperation with the United States Secret Service & Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center. The research was conducted to unearth e-crime fighting trends and techniques, including best practices and emerging trends.

For the purpose of this survey, the following definitions are used:

> *Electronic crime:* any criminal violation in which electronic media is used in the commission of that crime.
>
> *Intrusion:* a specific incident or event perpetrated via computer that targeted or affected an organization's data, systems, reputation or involved other criminal behavior.
>
> *Insider:* current or former employee or contractor
>
> *Outsider:* non-employee or non-contractor.

The online survey of *CSO* magazine subscribers and members of the U.S. Secret Service's Electronic Crimes Task Forces was conducted from April 15 to April 26, 2004. Results are based on 500 completed surveys. A sample size of 500 at a 95% confidence level has a margin of error of +/- 4.4%.

In addition to the 2004 E-Crime Watch survey team, the following security practitioners served as advisors to the project:

- Michael Assante, Vice President and Chief Security Officer, American Electric Power
- Bill Boni, Vice President and Chief Information Security Officer, Motorola
- Don Masters, Assistant Special Agent in Charge, Los Angeles Field Office, United States Secret Service
- Bob Rose, Senior Managing Director, Bear Sterns
- Dennis Treece, Director of Corporate Security, Massachusetts Port Authority
- James Wellington, Director of Federal Systems, Questerra

Survey results were announced on May 25, 2004. Within the first 30 days of its release, the survey has attracted significant news media coverage from more than 35 outlets, such as CNN, *The Washington Post, USA Today,* and United Press International (UPI). According to a report from PR Newswire (the service with which the news release was distributed to media), the survey was accessed by 517 individuals during the month it was released. In addition to its U.S. appeal, the survey was accessed by nine other countries including Australia, Czech Republic, France, Germany, Ireland, Norway, Philippines, Spain and United Kingdom. As of July 21, 2004, the survey has reached more than six million potential readers worldwide via print publications alone. Additional news media coverage is expected. A listing of news coverage to date is included in the addendum on page 39.

About the Survey Organizers

CERT

The CERT® Coordination Center (CERT/CC) is located at Carnegie Mellon University's Software Engineering Institute in Pittsburgh, Pennsylvania, U.S.A. The Software Engineering Institute is a Department of Defense-sponsored federally funded research and development center. The CERT/CC was established in 1988 to deal with security issues on the Internet. It now partners with and supports the Department of Homeland Security's National Cyber Security Division and its US-CERT to coordinate responses to security compromises; identify trends in intruder activity; identify solutions to security problems; and disseminate information to the broad community. The CERT/CC also conducts R&D to develop solutions to security problems and provides training to help individuals build skills in dealing with cyber-security issues.

CSO *Magazine*

Launched in September 2002, *CSO* magazine provides chief security officers with high-level information, best practices and strategic insight, helping them balance the safety of their enterprise with the pursuit of business opportunity. In its first two years of publication, *CSO* has been embraced by high-level security executives in the government and private sectors and has been recognized by prestigious awards judges for its editorial and design excellence. The magazine and its companion website, www.CSOonline.com, have received more than 50 awards to date, including five Jesse H. Neal National Business Journalism Awards (often referred to as the Pulitzer Prize of publishing) and Grand Neal runner-up honors two years in a row. Most recently, *CSO* was named Magazine of the Year (in the under 80,000 Circulation category) by American Society of Business Publication Editors.

United States Secret Service

The United States Secret Service is mandated by statute and executive order to carry out two significant missions: protection and criminal investigations. The Secret Service protects the President and Vice President, their families, heads of state, and other designated individuals; investigates threats against these protectees; protects the White House, Vice President's Residence, Foreign Missions, and other buildings within Washington, D.C.; and plans and implements security designs for designated National Special Security Events. The Secret Service also investigates violations of laws relating to counterfeiting of obligations and securities of the United States; financial crimes that include, but are not limited to, access device fraud, financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure.

Sourcing & Contact Info

Data from the 2004 E-Crime Watch survey must be sourced as originating from: *CSO* magazine/U.S. Secret Service/CERT Coordination Center.

Media inquiries about the survey may be directed to the following contacts:

CONTACTS:

CSO magazine	CERT Coordination Center	U.S. Secret Service
Susan Watson	Kelly Kimberland	Office of Public Affairs
508.935.4190	412.268.8467	202.406.5708

All other inquires about this report may be directed to:

Carolyn Johnson
Manager, Marketing Research
CXO Media
508.935.4183: phone
508.879.1957: fax
cjohnson@cxo.com: email

Executive Summary

The 2004 E-Crime Watch survey conducted among security and law enforcement executives by *CSO* magazine in cooperation with the United States Secret Service and the Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center, shows a significant number of organizations reporting an increase in electronic crimes (e-crimes) and network, system or data intrusions. Forty-three percent (43%) of respondents report an increase in e-crimes and intrusions versus the previous year and 70% report at least one e-crime or intrusion was committed against their organization. Respondents say that e-crime cost their organizations approximately $666 million in 2003. However, 30% of respondents report their organization experienced no e-crime or intrusions in the same period.

E-Crimes Impact

When asked what types of losses their organizations experienced last year, over half of respondents (56%) report operational losses, 25% state financial loss and 12% declare other types of losses. The average number of individual e-crimes and intrusions is 136. However, a third (30%) of respondents did not experience e-crime or intrusions, while a quarter (25%) experienced fewer than ten. Interestingly, 32% of respondents do not track losses due to e-crime or intrusions. Of those who do track, half say they do not know the total amount of loss. Forty-one percent (41%) of respondents indicate they do not have a formal plan for reporting and responding to e-crimes, demonstrating room for improvement. Slightly more than half (51%) state their organization has a formal process in place to track e-crime attempts. Additionally, respondents indicate a higher degree of familiarity with local and national e-crime laws (39% and 33% respectively), but know little about applicable international laws (8%).

Who are the Criminals?

Nearly a third (30%) of respondents in organizations experiencing e-crimes or intrusions in 2003 do not know whether insiders or outsiders were the cause. Respondents who do know report that an average of 71% of attacks come from outsiders compared to 29% from insiders. Regarding the source of the greatest cyber security threat, hackers were most frequently cited (40%) followed closely by current or former employees or contractors (31%). When it comes to identifying specific types of e-crimes committed against organizations, the survey shows 36% of respondents organizations experienced unauthorized access to information, systems or networks by an insider compared to 27% committed by outsiders. Both sabotage and extortion are committed equally by insiders and outsiders for organizations responding to the survey.

> *"The increase in e-crime over the past year again demonstrates the need for corporate, government and non-governmental organizations to develop coordinated efforts between their IT and security departments to maximize defense and minimize e-crime impact. There is a lot of security spending going on, but not much planning. It's essential for chief security officers and information technology pros to find the most manageable, responsive and cost effective way to stop e-crime from occurring.*
>
> — Bob Bragdon
> Publisher
> *CSO* magazine

Executive Summary (continued)

Monitoring & Reporting

Eighty percent (80%) of respondents report they monitor their computer systems or networks for misuse and abuse by employees or contractors. Ninety-five percent (95%) of respondents say they use some type of employee monitoring (e.g., internet, email, files) to deter e-crime. Thirty-six percent (36%) report using employee monitoring to terminate an employee or contractor for illegal activities. Seventy-two percent (72%) of respondents require internal reporting of misuse or abuse of computer access by employees or contractors. However, just under half (49%) of respondents say intrusions are handled with the help of law enforcement or by taking other legal action.

> *"Many companies still seem unwilling to report e-crime for fear of damaging their reputation," says Larry Johnson, Special Agent in Charge, Criminal Investigative Division, United States Secret Service. "However, as we see with this survey, ignoring the problem or dealing with it quietly is not working. The question is not why can't we stop these criminal acts from happening, but rather, why are we allowing them to take place? The technology and resources are there to effectively fight this. We just need to work smarter to do it."*
>
> — Larry Johnson
> Special Agent in Charge
> Criminal Investigative Division
> United States Secret Service

Best Practices

The most common technologies deployed to combat e-crime are firewalls used by 98% of respondents, followed by physical security systems (94%) and manual patch management (91%). In ranking the effectiveness of various technologies, firewalls are considered the most effective (71%), followed by encryption of critical data in transit (63%) and encryption of critical data in storage (56%). Manual patch management, the third most common technology in use, also holds the dubious distinction of being rated as the single least effective technology (23%). Among policies and procedures, conducting regular security audits is listed as the most effective method (51%), and recording or reviewing employee phone conversations is listed as one of the least effective (26%).

> *"The ineffectiveness of manual patching demonstrates the difficulty corporate and individual users have in keeping abreast of the large number of vulnerabilities discovered every month. "In the long-term, we all need to work towards higher quality software, with fewer defects in order to keep our risks at a manageable level."*
>
> — Richard Pethia
> Director of the Software Engineering Institute's (SEI)
> Networked Systems Survivability Program

About Survey Respondents

Job Title

Two-thirds of respondents hold security or IT management-related job titles (32% and 34%, respectively). Twelve percent (12%) hold a law enforcement/ prosecutor title while nine percent (9%) are corporate non-IT managers (see table below).

Job Title ***(base: 500)***	
Security Management-Related (NET)	**32%**
• Director/Manager	17%
• CSO/CISO	11%
• Executive VP/Senior VP/VP	3%
IT Management-Related (NET)	**34%**
• Director/Manager	22%
• CIO/CTO	7%
• Executive VP/Senior VP/VP	5%
Law Enforcement/Prosecutor	**12%**
Corporate Non-IT Management	**9%**
Other	**13%**

Sector

Of the 500 *CSO* magazine and Secret Service Electronic Crimes Task Force (ECTF) members responding, two-thirds (67%) say their organization belongs to the private sector, 24% government and 10% law enforcement.

Length of Employment

Nearly half (47%) of respondents have worked in their current position for five years or longer. One-third (33%) say they've been employed in their current position for between two and five years and 13% for one to two years. Seven percent (7%) are new to their position reporting employment length as one year or less.

Number of Employees

Almost two-thirds (63%) of respondents work in larger-sized companies of over 1,000 employees. Six percent (6%) work in organizations with 100,000 or more employees (see table below).

Number of Employees ***(base: 500)***	
100,000 or more	6%
10,000-99,999	23%
1,000-9,999	34%
500-999	11%
100-499	10%
Under 100	15%
Don't know	<1%

Note: percents may not sum to 100 due to rounding

About Survey Respondents (continued)

Number of Information Security Personnel

The table below breaks out the number of information security personnel employed and outsourced by respondents' organizations:

# Information Security Personnel ***(base: 500)***		
	Employed	Outsourced
500 or more	5%	2%
100-500	7%	2%
50-99	5%	4%
20-49	9%	4%
1-19	57%	26%
None	8%	44%
Don't know	8%	18%

Annual Security Budget

Nearly one-third (30%) of respondents report annual security budgets at their organizations of $1 million or more (see table below for breakout).

Annual Security Budget ***(base: 500)***	
$25 million or more	6%
$10 to $24.9 million	6%
$5 to $9.9 million	4%
$1 to $4.9 million	14%
$500,000 to $999,999	5%
$250,000 to $499,999	7%
$100,000 to $249,999	14%
$50,000 to $99,999	7%
Less then $50,000	16%
Don't Know	22%

Of those providing a dollar figure, sixty percent (60%) say the budget applies to a combination of information and physical/ corporate security spending, 37% say it applies to information security spending only and three percent (3%) say the budget applies to physical/corporate security spending only.

Budget Applies to: ***(base: 391)***	
Information security spending only	37%
Physical or corporate security spending only	3%
Combined security spending	60%

Note: percents may not sum to 100 due to rounding.

About Survey Respondents (continued)

Critical Infrastructure Sector

Eighty-two percent (82%) of survey respondents report that their organization belongs to a critical infrastructure sector (see table below).

Critical Infrastructure Sector ***(base: 500)***	
Government	28%
Information & telecommunications	19%
Banking and finance	15%
Public Health	8%
Transportation	3%
Defense Industrial Base	3%
Food	2%
Energy	2%
Emergency Services	1%
Chemical Industry	1%
Water	<1%
Postal and Shipping	<1%
Not applicable	19%

Primary Industry

Security and law enforcement executives surveyed work in a wide cross-section of industries (see table below).

Primary Industry ***(base: 500)***	
Banking and finance	13%
Information and Telecommunications	12%
Law enforcement/security	11%
Education	10%
Government	10%
Health Care	8%
Electronics/Technology	5%
Military	4%
Services	4%
Insurance	3%
Transportation	2%
Defense Industrial Base	1%
Electric Power	1%
Research & Development	1%
Wholesale	1%
Pharmaceutical	1%
Retail, consumer products	1%
Retail, food and drink	1%
Chemical Industry	1%
Construction/Real Estate	1%
Natural Resources/Mining	1%
Agriculture	<1%
Food	<1%
Gas & Oil	<1%
Water	<1%
Emergency Services	<1%
Other	7%

Note: percents may not sum to 100 due to rounding.

About Survey Respondents (continued)

Involvement – Security or Electronic Crime Related Decisions

Survey respondents are involved in a variety of security or electronic-crime related decisions at their organizations:

- Decisions regarding information security (79%)
- Decisions regarding referral of potential electronic crime to law enforcement (60%)
- Investigations or prosecution of electronic crimes (56%)
- Decisions regarding corporate/physical security (51%)
- Audit reporting concerning fraud or electronic crimes (44%)
- None of the above (4%)

Knowledge Level

Respondents indicate a higher level of familiarity with local and national e-crime laws but know less about international laws surrounding computer crime. Only 13% and 14% of those surveyed report they are not knowledgeable regarding e-crime laws in their state and the United States while 42% are unfamiliar with international laws.

Knowledge Level Regarding Laws Surrounding Computer Crimes *(base: 500)*

	Very or extremely knowledgeable (NET)	Somewhat knowledgeable	Not knowledgeable	Don't know
In your state	39%	46%	13%	2%
In the US	33%	50%	14%	2%
Worldwide	8%	40%	42%	10%

Note: percents may not sum to 100 due to rounding.

Electronic Crimes Impact

Change in Number of Electronic Crimes or Intrusions

Forty-three percent (43%) of security and law enforcement executives responding report that the total number of electronic crimes and network, systems or data intrusions experienced by their organizations increased in 2003 vs. 2002. Twenty-three percent (23%) report no change in the number of e-crimes and intrusions while only six percent (6%) report a decrease. Twenty-eight percent (28%) of respondents don't know whether the total number of electronic crimes and intrusions differed in 2003 compared to 2002.

Number of Electronic Crimes

Thirty-percent (30%) of respondents report that their organizations experienced no electronic crimes or intrusions in 2003. One quarter (25%) report between 1 and 9 incidents while the remaining 45% experienced 10 or more electronic crimes or intrusions last year.

2003 eCrimes/Intrusions ***(base: 485)***	
None	30%
1-9	25%
10-49	20%
50-99	5%
100-249	9%
250 or more	11%

Monetary Losses from Electronic Crimes

Nearly one-third (32%) of respondents say their organizations do not track monetary losses due to electronic crimes. Of those security practitioners that do track losses caused by e-crime, half (50%) are unable to put a price tag on the monetary value.

Monetary value of losses from electronic crimes ***(base: 338)***	
$10 million or more	3%
$1 million to $9.9 million	5%
$500,000 to $999,999	5%
$100,000 to $499,999	11%
Less then $100,000	26%
Don't know	50%

Note: percents may not sum to 100 due to rounding.

Electronic Crime Impact (continued)

Types of Losses

Eighty-three percent (83%) of respondents report their organizations experienced some type of loss in 2003 as a result of electronic crimes. Of that group, over half (56%) report experiencing some type of operational losses, one quarter (25%) financial losses and 12% some other losses. Nearly a third (32%) are unable to pinpoint which type of losses their organizations experienced in 2003.

Types of Electronic Crimes Committed

Among those organizations experiencing attacks in 2003, virus or other malicious code are the most frequent type (77%) followed by denial of service attacks (44%), illegal generation of SPAM email (38%), unauthorized access by insiders (36%) and phishing (31%), i.e., imitating legitimate companies online in an effort to access confidential information.

Types of Electronic Crimes ***(base: 342)***	
Virus or other malicious code	77%
Denial of service attack	44%
Illegal generation of SPAM email	38%
Unauthorized access by an *insider*	36%
Phishing	31%
Unauthorized access by an *outsider*	27%
Fraud	22%
Theft of intellectual property	20%
Theft of other proprietary info	16%
Employee identity theft	12%
Sabotage by an *insider*	11%
Sabotage by an *outsider*	11%
Extortion by an *insider*	3%
Extortion by an *outsider*	3%
Other	11%
Don't know	8%

Consequences of Insider Intrusions

Fifty-nine percent (59%) of security and law enforcement executives responding report some type of adverse impact to their organizations as a result of insider intrusions. Of that group, one-quarter (25%) report that the most adverse consequences from insider intrusions are critical disruptions impacting only their organizations. Forty-one percent (41%) of respondents say that insider intrusions had no impact (see table below).

Most Adverse Consequence From Insider Intrusion ***(base: 500)***	
Critical disruption to organization only	25%
Harm to organization's reputation	15%
Critical system disruption affecting customers & business partners	7%
Loss of current or future revenue	7%
Loss of customers	3%
Critical system disruption, affecting the larger critical infrastructure	2%
Personal Injury	<1%
No impact	41%

Note: percents may not sum to 100 due to rounding.

Who Are The Criminals?

Outsiders vs. Insiders

Nearly one-third (30%) of security and law enforcement executives in organizations experiencing electronic crimes or intrusions last year don't know if the attacks originated from outsiders or from insiders. Sixty-four percent (64%) report that one or more attacks are known or suspected to have come from outsiders compared to forty-one percent (41%) from insiders (see table below).

Source of Electronic Crimes ***(base: 342)***		
Number	Outsiders	Insiders
None	7%	30%
1-9	32%	22%
10-49	14%	11%
50-99	4%	4%
100-249	6%	2%
250 or more	8%	2%
Don't know	30%	30%

Groups Posing Greatest Cyber Security Threat

Forty-percent (40%) of respondents say hackers posed the greatest cyber security threat to their organizations in 2003. Insiders rank second with twenty-eight percent (28%) citing current or former employees and 4% current or former service providers, contractors or consultants. One in five respondents (20%) are unsure which group posed the greatest threat.

Greatest Cyber Security Threat in 2003 ***(base: 500)***	
Hackers	40%
Current employees	22%
Former employees	6%
Current service providers/contractors/consultants	3%
Customers	2%
Foreign entities	2%
Competitors	2%
Terrorists	1%
Former service providers/contractors/consultants	1%
Suppliers/Business Partners or Information Brokers	<1%
Don't know	20%

Note: percents may not sum to 100 due to rounding.

Who Are The Criminals? (continued)

Sources of Insider Intrusions in 2003

Current employees not employed in management positions are most frequently cited as a source of insider intrusions in 2003 (73%) followed by current employees in positions within management (38%). See table below.

Sources of insider intrusions in 2003 *(base: 140)*	
Current employees not in management positions at the time of the intrusion	73%
Current employees in management positions at the time of the intrusion	38%
Current contractors/temporary employees at the time of the intrusion	33%
Former employees previously employed in non-management positions	31%
Former contractors/temporary employees	15%
Former employees previously employed in management positions	14%
Don't know/Not sure	9%

Note: percents may not sum to 100 due to rounding.

Monitoring

Formal Tracking Process

- Over half (51%) of respondents say their organization has a formal process or system in place for tracking e-crime attempts. Thirty-seven percent (37%) say their organization does not have a formal process or system in place for tracking e-crime attempts while twelve percent (12%) don't know.

Monitoring for Misuse & Abuse

- Eighty-percent (80%) of security and law enforcement executives say their organizations monitor systems and networks for misuse or abuse by employees or contractors. Of that group, two-thirds (67%) say their organizations monitor both systems and networks, 8% networks only and 5% systems only. Thirteen percent (13%) report that their organizations do not monitor systems or networks for insider misuse or abuse while 6% are unsure.

Discovery of Electronic Crimes

- Nearly one-half (48%) of respondents report that some percentage of e-crimes against their organizations were uncovered accidentally, as opposed to as a result of systems and/or policies in place. Over one-quarter (27%) aren't sure what percent of e-crimes were discovered by an accident (see table below).

Percent of e-Crimes Discovered Accidentally ***(base: 500)***	
Zero	25%
Less then 10%	17%
10-24%	9%
25-49%	7%
50-74%	7%
75-99%	3%
100%	5%
Don't know	27%

Note: percents may not sum to 100 due to rounding.

Responding & Reporting

Formal Plan for Responding & Reporting

- One-half of respondents (50%) report that their organizations have formalized plans outlining policies and procedures for reporting and responding to e-crimes while nearly one quarter (23%) say they are planning to implement a formalized plan in the next year. Seventeen-percent (17%) say there are no plans to implement any type of formalized plan for reporting and responding to e-crimes while ten percent (10%) aren't sure.

Use of Incident Response Team

- Two-thirds (67%) of security and law enforcement executives responding say their organization has an incident response team. Of this group, members of the MIS, IS, IT, computer or networking team are the most commonly represented (83%) followed by information security (74%), senior management (60%), physical or corporate security (54%) and legal/contracts (45%). Twenty-seven percent (27%) of respondents' organizations do not have an incident response team while six percent (6%) don't know.

Incident Response Team Representation *(Base: 337)*	
MIS, IT, IS, computer or networking	83%
Information security	74%
Senior management	60%
Physical or corporate security	54%
Legal or contracts	45%
Human resources	38%
Public relations	28%
Accounting, finance or purchasing	16%
Executive committee	14%
General administration	9%
Manufacturing, production or operations	7%
Board of directors	5%
Other	10%
Don't know	6%

Internal Reporting of Misuse or Abuse

- Nearly three quarters (72%) of respondents' organizations require internal reporting of misuse or abuse of computer access by employees or contractors. Eighteen percent (18%) do not make reporting mandatory while 10% don't know.

Note: percents may not sum to 100 due to rounding.

Record Keeping

Eighty-percent (80%) of respondents say their organization keeps records on or otherwise keeps track of network, data and systems intrusions. Of that group, one in five (22%) say their organization holds on to records for a year or less, sixteen percent (16%) for 1-2 years, sixteen percent (16%) for 2- 5 years and fourteen percent (14%) keep records for 5 years or longer. Nearly one-third (32%) of security practitioners at organizations keeping track of intrusions don't know how far back records are kept.

Responding to Insider Intrusions

Respondents reporting insider intrusions at their organizations report that an average of 72% of insider intrusions were handled internally without involving legal action or law enforcement. On average, 18% of insider intrusions were handled internally with some type of legal action while only 13% were handled with law enforcement assistance. On average, two percent (2%) of insider intrusions were handled externally through some civil action.

Reasons Insider Intrusions Not Referred for Legal Action

Over half (58%) of security practitioners reporting insider intrusions at their organizations report that these incidents were not referred for legal action because of insufficient damage levels. Over one-third (36%) cite lack of evidence or information to prosecute as the reason for not pursuing while twenty-seven percent (27%) cite concerns about negative publicity.

Reasons Insider Intrusions Not Referred for Legal Action *(Base: 140)*	
Damage level insufficient to warrant prosecution	58%
Lack of evidence/not enough information to prosecute	36%
Concerns about negative publicity	27%
Concerns that competitors would use incident to their advantage	11%
Prior negative response from law enforcement	7%
Unaware that we could report these crimes	1%
Other	16%
Don't know	7%

.

Note: percents may not sum to 100 due to rounding.

Best Practices - Technologies

Technologies Installed

Firewalls are used by nearly all of respondents' organizations (98%) followed by physical security systems (94%), manual patch management (91%), encryption of critical data in transit & role-based access control tied at 85% (see table below)

Technologies Installed ***(base: 500)***	
Firewalls	98%
Physical security systems (electronic access control systems, badging systems, CCTV, etc.)	94%
Manual patch management	91%
Encryption of critical data in transit	85%
Role-based access control	85%
Intrusion detection systems monitored by person	81%
Information assurance technologies (that track access & use of corporate data)	76%
Automated patch management	74%
Intrusion detection systems monitored by automated systems w/ built-in alarms	74%
Encryption of critical data in storage	71%
Anti-Fraud technologies working with ERP/account payable/billing systems	63%
Two factor authentication (using biometrics, smart cards, etc.)	56%
Wireless monitoring	54%
Keystroke monitoring of individual users	39%

Note: percents may not sum to 100 due to rounding.

Best Practices – Technologies (continued)

Technologies Effectiveness

In ranking the effectiveness of various technologies, firewalls are considered the most effective (71%), followed by encryption of critical data in transit (63%) and encryption of critical data in storage and two factor authentication (tied at 56%). Manual patch management, the third most common technology in use, also holds the dubious distinction of being rated as the single least effective technology. .The table below provides a complete breakout. Note that the top 5 rankings for each column are provided (in parenthesis).

Technologies Effectiveness *(percents based on those with technology in use)*	**Very or Extremely Effective**	**Somewhat Effective**	**Not Effective**	**Don't know**
Firewalls	71%(1)	22%	2%	4%
Encryption of critical data in transit	63%(2)	19%	5%	13%
Two factor authentication	56%(3-tie)	16%	8%	20%(4)
Encryption of critical data in storage	56%(3-tie)	21%	6%	17%(5)
Intrusion detection systems monitored by automated systems w/ built-in alarms	51%(4)	28%	8%	13%
Physical security systems	48%(5)	39%(1)	9%	4%
Intrusion detection systems monitored by person	45%	34%(4)	11%	10%
Role-based access control	44%	35%(3-tie)	9%	12%
Automated patch management	39%	32%(5)	14%(4)	16%
Information assurance technologies	35%	35%(3-tie)	13%(5)	16%
Anti-Fraud technologies working with ERP/account payable/billing systems	33%	30%	7%	30%(2)
Wireless monitoring	26%	31%	20%(2)	23%(3)
Manual patch management	26%	37%(2)	23%(1)	14%
Keystroke monitoring of individual users	24%	27%	16%(3)	33%(1)

Note: percents may not sum to 100 due to rounding.

Best Practices – Policies & Procedures

Security Policy

The majority (96%) of security and law enforcement executives surveyed have a security policy in place at their organizations. Of that group, half (48%) say their organization only updates the policy on an as needed basis and one-quarter (24%) update the policy annually (see table below).

Frequency of Security Policy Updates ***(base: 480)***	
As needed	48%
Annually	24%
Every 6 months	7%
Monthly	2%
Other	3%
Don't know	16%

Written Inappropriate Use Policy

- Eight out of 10 respondents' organizations (82%) have some type of written inappropriate use security policy in place governing use of networks, data, and systems while 7% have a policy pending. Seven percent (7%) of respondents say their organizations do not have an inappropriate use policy.

- Of those security and law enforcement executives with inappropriate use policies in place, over one-half (55%) require employees to review their organization's written inappropriate use policy when hired. Over ten percent (12%) say their organizations do not require employees to review the inappropriate use policy (see table below).

Frequency of Inappropriate Use Policy Review ***(base: 410)***	
Upon employment	55%
Annually	28%
Periodically	13%
Not required	12%
Upon accessing data	11%
Every 6 months	1%
Don't know	3%

- Hardcopy distribution (57%) is the most frequently cited means for distribution followed by email (48%) and posting the inappropriate use policy online (44%). See table below for more information.

Inappropriate Use Policy Distribution ***(base: 410)***	
Hardcopy distribution	57%
Electronic Mail	48%
Web reference	44%
Direct communications from managers	35%
Training materials	32%
Training classes	27%
Other	5%
Don't know	4%

Note: percents may not sum to 100 due to rounding.

Best Practices – Policies & Procedures (continued)

Policies & Procedures in Place

The top 5 policies or procedures in place at respondents' organizations are written inappropriate use policies (94%), requiring sign-off on acceptable use policies (90%), monitoring Internet connections (90%), mandatory reporting of insider misuse or abuse (89%) and employee education and awareness programs (89%).

Policies & Procedures in Place ***(base: 500)***	
Written inappropriate use policy	94%
Monitor Internet connections	90%
Require employees/contractors to sign acceptable use policies	90%
Education and awareness programs	89%
Mandatory internal reporting of insider misuse/abuse	89%
Conduct regular security audits	88%
Corporate security policy	88%
New employee security training	88%
Periodic risk assessments	88%
Employee/contractor background examinations	87%
Regular security communication from management	86%
Periodic systems penetration testing	85%
Use of an incident response team	78%
Employee monitoring	77%
Include security in contract negotiations with vendors/suppliers	75%
Storage & review of computer files	69%
Storage & review of e-mail	69%
Hired a Chief Security Officer (CSO)/ Chief Information Security Officer (CISO)	54%
Use of "white hat" hackers	54%
Government security clearances	52%
Storage & review of voice mail	48%
Record or review employee phone conversations	41%
Polygraph examinations	31%

Note: percents may not sum to 100 due to rounding.

Best Practices – Policies & Procedures (continued)

Effectiveness of Policies & Procedures

The top 5 policies & procedures considered most effective in preventing or reducing e-crime at respondents' organizations are: conducting regular security audits (51%), hiring a CSO or CISO (49%), periodic systems penetration testing (48%), monitoring internet connections (46%) and periodic risk assessments (45%). Recording or reviewing employee phone conversations is the least effective policy or procedure in place (26%) followed by storage & review of voice mail (25%). See table below. Note that the top 5 rankings for each column are provided (in parenthesis).

Effectiveness of Policies & Procedures ***(percents based on those with policy or procedure in place)***	**Very or Extremely Effective**	**Somewhat Effective**	**Not Effective**	**Don't know**
Conduct regular security audits	51%(1)	32%	8%	9%
Hired a Chief Security Officer (CSO) or Chief Information Security Officer (CISO)	49%(2)	23%	8%	19%(5-tie)
Periodic systems penetration testing	48%(3)	30%	6%	16%
Monitor Internet connections	46%(4)	35%	11%	8%
Periodic risk assessments	45%(5)	36%	9%	10%
Use of an incident response team	44%	36%	7%	13%
Government security clearances	43%	27%	12%	19%(5-tie)
Corporate security policy	42%	39%	11%	7%
Mandatory internal reporting of insider misuse/abuse	40%	35%	16%	8%
Employee education & awareness programs	40%	43%(3)	13%	4%
Employee/contractor background examinations	40%	37%	10%	12%
Include security in contract negotiations with vendors/ suppliers	39%	31%	11%	19%(5-tie)
Written "inappropriate use" policy	38%	40%	17%(5-tie)	4%
Regular security communication from management	37%	40%	17%(5-tie)	5%
New employee security training	36%	44%(2)	15%	6%
Require employees/ contractors to sign acceptable use policies	34%	41%(5)	18%(4-tie)	6%
Use of "white hat" hackers	31%	32%	9%	28%(4)
Employee monitoring	28%	45%(1)	15%	12%
Storage & review of computer files	25%	38%	19%(3-tie)	18%
Storage & review of e-mail	24%	42%(4)	18%(4-tie)	16%
Polygraph examinations	20%	26%	19%(3-tie)	35%(2)
Storage & review of voice mail	15%	30%	25%(2)	30%(3)
Record or review employee phone conversations	12%	27%	26%(1)	36%(1)

Single Most Effective Security Policy/Practice

Survey respondents were asked to briefly describe in one or two sentences the single most effective security policy or practice in place at their organizations for preventing electronic crime. Their comments have been categorized and provided verbatim in an addendum beginning on page 26.

Note: percents may not sum to 100 due to rounding.

Best Practices – Policies & Procedures (continued)

Policies & Procedures Impact

Respondents were asked, in their opinion, whether or not any of the policies and procedures in place at their organizations have directly led to the deterrence, detection, termination or prosecution of an alleged criminal. In terms of deterrence, corporate security policies and new employee security training tie as the most frequently cited deterrents to e-crime. Conducting regular security audits leads in the detection area with nearly half (46%) of those employing that procedure saying it directly contributed to detecting e-criminals. The written inappropriate use policy is credited most often (32%) as directly leading to termination among those respondents whose organizations employ that procedure. The table below provides a complete breakout. Note that the table is sorted by the first column, deterrence. The top 5 rankings for all other columns are provided in parenthesis.

Impact *(percents among those respondents with policy/procedure in place)*	**Deterrence**	**Detection**	**Termination**	**Prosecution**	**None**	**Don't know**
New employee security training	61%(1-tie)	9%	4%	<1%	14%	22%
Corporate security policy	61%(1-tie)	21%	16%	7%(2)	11%	19%
Employee education & awareness programs	60%(2)	19%	12%	4%(5-tie)	12%	18%
Regular security communication from management	58%(3)	10%	4%	1%	14%	23%
Require employees/contractors to sign acceptable use policies	55%(4-tie)	11%	14%	4%(5-tie)	11%	25%
Written inappropriate use policy	55%(4-tie)	15%	32%(1)	5%(4-tie)	8%	16%
Include security in contract negotiations with vendors/suppliers	51%(5)	16%	5%	2%	15%	26%
Hired CSO or CISO	45%	25%	11%	8%(1-tie)	19%(3-tie)	30%
Mandatory internal reporting of insider misuse/abuse	44%	24%	20%(5)	3%	12%	24%
Employee/contractor background examinations	43%	24%	10%	2%	14%	28%
Monitor Internet connections	41%	41%(3)	25%(3)	5%(4-tie)	12%	18%
Conduct regular security audits	40%	46%(1)	10%	2%	11%	21%
Periodic risk assessments	37%	38%(4)	3%	<1%	15%	23%
Storage/review of e-mail	36%	30%	22%(4)	5%(4-tie)	16%(5-tie)	25%
Employee monitoring	36%	32%	27%(2)	8%(1-tie)	16%(5-tie)	22%
Government security clearances	34%	16%	4%	2%	19%(3-tie)	37%(4)
Storage/review computer files	32%	36%(5)	18%	6%(3)	16%(5-tie)	25%
Use of incident response team	29%	35%	11%	8%(1-tie)	18%(4)	25%
Periodic systems penetration testing	29%	42%(2)	3%	<1%	16%(5-tie)	25%
Storage & review of voice mail	24%	17%	5%	2%	23%(2-tie)	38%(3)
Use of "white hat" hackers	23%	34%	2%	1%	16%(5-tie)	36%(5)
Record/review employee phone conversations	20%	19%	8%	3%	23%(2-tie)	42%(2)
Polygraph examinations	18%	14%	3%	3%	25%(1)	46%(1)

Note: percents may not sum to 100 due to rounding.

Electronic Crime Most Proud of Preventing/Solving

Security and law enforcement executives surveyed were asked to briefly describe the electronic crime attempt or occurrence that they are most proud of preventing or solving. Respondents provided a wealth of comments, many relating to the virus and hacker categories. These comments help illustrate the potential damage caused by electronic crime, both from an organizational and a personal standpoint.

A complete list of verbatim comments is provided in the addendum (see page 33).

Note: percents may not sum to 100 due to rounding.

Addendum

Verbatim Comments - Single Most Effective Security Policy/Practice

When asked to briefly describe (1-2 sentences) the *single most effective* security policy or practice in place at their organizations for stopping e-crime, security and law enforcement executives responding provided the following responses:

Authentication/Passwords

- Two factor authentication.
- Enforcing tighter access controls on confidential data.
- Implementation of a network account subscription process that requires proof identity and persons signature as agreement to abide by security policies.
- Requiring employee ID and password prior to access to confidential systems.
- Requiring secure passwords.
- Strict user access controls.
- Strong passwords are required to access corporate data at any level.
- The most effective security policy is the use of strong passwords along with a great firewall and IDS application.
- Theft of service is our primary problem. Since we deal with general public, these thefts are reported by customers to us and we are reactive as opposed to proactive. Sales and marketing strategies limit the ability to screen prospective callers beyond verification that billing mechanisms (credit card, debit card, check account, person accounts set up as direct bill) are legit and billable.
- We ensure all employees and system users have minimal security clearance. We require an Entrance National Agency Check (ETNAC) of all employees and most require additional checks.

Conduct Regular Security Audits/Period Risk Assessments/System Testing

- 24-7-365 automated auditing and patch management.
- Auditing and review, without a review process, policies are just words on a piece of paper.
- Auditing Security Policy.
- Auto update of security patches to commonly used software.
- Consistent review of network traffic.
- Assessment Committee.
- Daily review of firewall logs Internet connection of during nonbusiness hours.
- Frequency of comprehensive security reviews and penetration testing, plus patch management.
- Frequent testing of access and resources for vulnerabilities has limited the amount of incidents within our systems.
- Annual reviews.
- I think our rolling audit program, hitting each plant annually with simultaneous IT and financial audits, prevents a lot of potential problems. It is tied with the management bonus program.
- Instituting audits and security reviews of all applications prevented considerable problems from happening at all.
- Manual review of currently operating servers including checks for 'unauthorized' files.
- Penetration testing and program validation.
- The AUP in conjunction with annual principal review with staff and students.

Written "Inappropriate use" Policy

- A comprehensive security policy is drafted and pending.
- Because this is a small federal agency, security policies are well known and discussed often.
- Classification policy.
- In our law enforcement organization we are not necessarily subject to fraud or loss of profits. We do have a written policy in place that is supposed to prevent misuse of email, Internet, and confidential information sharing with unauthorized persons.

- Inappropriate use - revised when I was hired. CEO just signed off on ww distribution of Corporate InfoSec Policy - distributed (date removed to protect respondent identity).
- Inappropriate use (4 mentions).
- Institution of appropriate use policy and gaining backing of management.
- Published use policy that says if you sign it you agree to it and it is grounds for dismissal on first offense.
- The employee handbook describes in detail the inappropriate use policy for network and systems.
- Written computer and network protocol in employee handbook.
- Written policy.

Monitor Internet Connections/Firewall/Anti-virus/Patches

- A series of firewalls and encryption of data; segregation of gateways.
- A single tightly controlled Cisco PIX firewall.
- All emails are scanned for attachments. All attachments are scanned for viruses and the emails placed on a secure server.
- An effective IDS, firewall and spam filter.
- Anti-virus software for scanning email.
- Automated patch management.
- Automated security monitoring and intrusion detection.
- Automatic security monitoring and firewall Black Box.
- Ban on outside Web mail reduces virus infection tremendously.
- Boarder/Firewall protection at Internet gateway.
- Building security and limited access to servers - good firewalls.
- Clamped down firewall policies.
- Firewall.
- Constant monitoring of industry and security bulletins and notices regarding current attacks and schemes.
- Constant monitoring of the system.
- DMZ-design firewall keeps sniffers that are placed behind it from broadcasting, so the 'need' for academic freedom which allows a lot of leeway and contamination of the system does not infringe on the need for a secure system.
- Monitoring of systems and networks for unusual activity.
- Examination of data flows to org, and encryption of sensitive data in transit, based on examination of the data.
- Financial and ERP systems firewalled from rest of university.
- Firewalls - no generic sign-on/password.
- Firewall and Internet access log reviews.
- Firewall, system hardening.
- Firewalls.
- Firewalls and security policies
- Firewalls for intrusion and keeping the gates to a minimum
- Firewalls in place with monitoring by IT
- Firewalls, IDS system
- Firewalls active on all PCs in the network seem to help stop worm transfer on LAN by network shares
- Firewalls, SPAM monitors, use of Linux vs. Windows for servers, use of non-Microsoft
- General awareness, monitoring
- Good firewall, Norton Internet Security - tracking and preventing hackers
- Heavy reliance on firewalls - internal communications regarding spam mail alert employees that crimes can be committed by outsiders.
- Highly trained policy enforcement team monitors external reports of inappropriate activity and takes appropriate steps to halt ongoing activity and prevent future occurrence.
- Host based firewalls, network-based firewall, employee training

- Host-based intrusion detection is the most useful all-around. It highlights intrusions and attempted intrusions.
- Implementation of Cisco Systems Secure PIX 525 firewall and a suite of Symantec Corporate Edition Anti-Virus software
- Internet monitoring of Web browsing and email
- Internet monitoring software combined with inappropriate use written policy.
- Intrusion detection
- Intrusion detection monitoring
- Intrusion detection systems and firewalls
- Intrusion detection/Prevention
- IT monitoring equipment
- Least privilege, users, systems, networks are only allowed access to the data, functions, networks that are required to perform their function.
- Monitor Internet and email usage
- Monitoring access to systems and Internet, having written policy most effective - need to better communicate the policy.
- Monitoring and patching of CERT security vulnerabilities
- Monitoring and sign-ins
- Monitoring application usage
- Monitoring irregular activities
- Monitoring network applications and inbound / outbound traffic
- Monitoring of Internet and email
- Monitoring of network and systems
- Monitoring of suspected individual
- Monitoring systems, access and use
- Monitoring workstations and written policy
- Monitoring, education and awareness
- Monitoring/Audit
- Multidimension process -- hardware, software and policies -- for example we use 2 independent software products for anti-virus at the gateway level, plus a product workstation security, we use firewalls to control internal traffic as well as connections to the Internet, along with subnetting.
- Network controls, firewalls, and intrusion detection systems and personnel who monitor these areas seem to perform above expectations.
- Network defense-in-depth using firewalls and packet filtering routers
- Network firewall
- Network monitoring
- Network monitoring policy deters users from certain activities knowing that their are being monitored.
- Network monitoring, enforcing policies
- Outside - firewalls, multiple complex passwords
- Placement of firewalls and anti-virus software
- Restricting access and monitoring those with access
- Restricting access to know entities is the most effective deterrent.
- Surveillance
- System monitored by HQ.
- The implementation of firewalls and anti-virus products
- The use of firewalls
- There are two equally critically important: Updated anti-virus software and updated patches. With these two practices working effectively, any organization can prevent 90% of all attacks from being effective.
- Unannounced, periodic monitoring of network and systems activity
- Use of firewalls and network monitoring

- User awareness that monitoring and existence of Computer Incident Response Team has been most effective up to this point.
- Very tightly regulated firewall and email processes
- Virus protection software has been the single most effective security device in this organization.
- VPN Firewall appliance and Zone Alarm Personal Firewall for all Company PCs at home
- Currently looking into Zone Labs Integrity.
- We have implemented a secure perimeter using firewall, anti-virus, and content filtering hardware and software. This has stopped many attacks successfully.
- We have placed very effective virus and other monitoring on our network as well as put tough firewalls in place.
- We have the most up-to-date firewall and network protection programs in place.

Employee Monitoring

- Ability to track employee activity
- Advise employees that we monitor their use.
- Centralized logging and monitoring has been critical to both recognizing and tracking eCrime against the organization.
- Constant monitoring and communication with employees as to what is acceptable and not acceptable usage of system.
- Constant monitoring of employee behavior/attitudes/contentment.
- Employee integrity and practices are critical.
- Employee notification that use of enterprise resources will be monitored.
- Employees are the number one risk and the best policy is to keep them happy with the company.
- Internet usage monitoring and the threat of email review.
- Letting employees know their computer use/misuse can be monitored.
- Limit Internet access. Close all ports except those needed.
- Limiting access to resources and keeping computer features to a minimum to do the work needed.
- Regular notice to employees of 'no presumption of privacy' anywhere on our network or in our offices - when we catch someone in violation, we publish a 'generic' account of the crime or intrusion and the punishment (termination, suspension, etc.) widely within the organization.
- Sign on notification of privacy matters. Effectively, there is no assumption of individual privacy. Equipment and its content are owned by the company.

Corporate Security Policy

- Acceptable use policy (4 mentions).
- Acceptable use policy and mandatory security education and awareness programs.
- Acceptable use policy and security awareness.
- Acceptable use policy enforcement via Internet and email monitoring.
- Acceptable use policy for computers, email, and Internet.
- Acceptable use policy must be accepted every time a user logs into their PC.
- Acceptable use policy with sanctions.
- Acceptable use, awareness training and sign oath.
- Establishing acceptable use policy with the right to monitor employee's computer activities.
- Implementation of security policies and oversight through a state statute .
- Information policy requiring acknowledgement before data access.
- Introducing of network and system security standards policies and procedures.
- IR Policy for the use and protection of information resources and acceptable use policy.
- ISO 17799 security-based policies.
- It is unacceptable to use information assets to actively engage in creating, procuring, or transmitting any materials that are in violation of the company's policies or local laws.
- IT security policy.

Single Most Effective Security Policy/Practice (continued)

- Applying the 80/20 rule, 80% of systems will be desktops (which today have the power and reach servers did just a few years ago) operated by nonsystem nontechnical people, representing a new dimension in social engineering.
- Network usage policy.
- New appropriate use policy.
- One of our longest standing policies is the prohibition against downloading or installing any unauthorized executable files, whether directly from the Internet or from an email attachment. Although email filtering has prevented much of this, employee awareness training has made this policy successful.
- Opsec practices in place.
- Our cyber security program is in its infancy. Our most effective policy is our inappropriate use policy and our URL filtering policy and application.
- Our most effective policy/practice to date has been the e detection, location, and reporting of P2P Downloader's. Behind that has been the implementation of the Cisco IDS system for the network.
- Policy concerning the use of unauthorized software, with spyware and viruses.
- Procedures for handling HIPAA PHI inside and in contacting outside partners.
- Published use policy that says if you sign it you agree to it and it's grounds for dismissal on first offense.
- The acceptable use policy.
- The largest use of resources policy questions that face universities to date is that of DMCA and file sharing. We must maintain an open and free environment, all the time adhering to all copyright laws.
- The threat of termination and/or prosecution for violating any part of the corporate security policy.
- Use of code of conduct and internal security.
- We don't think we can ever stop e-crime or even prevent it from happening. However, in all our investigations, the 'Code of Conduct' and 'Appropriate Use policy' are the two most effective tools used for internal incidents. Our application and adherence to these documents form our practice which helps in decision-making process in all cases.
- We have a policy on the use of electronic systems and information.

Employee Education & Awareness Programs/New Employee Security Training/Awareness

- Awareness training (2 mentions).
- Adequate training and refresher training on how to detect and report suspected e-crimes in a timely manner.
- Awareness.
- Awareness, white-hat social engineering, tiger team.
- Being aware - making individuals responsible for their systems.
- Communicating the policies to all our employees.
- Constant training and monitoring as well response team efforts and continued education.
- Educated employees.
- Education (6 mentions)
- Education and awareness training.
- Education is the number one key followed by strict enforcement of policies/guidelines.
- Education of employees on IS monitoring capabilities.
- Employee awareness (3 mentions).
- Employee awareness and practices.
- Employee awareness education.
- Employee education (3 mentions).
- Employees are tested yearly pertaining to security policies.
- Ensure employees understand their role in stopping e-crime. Ensure management understands their role in supporting the employee efforts to stop e-crime.
- Good awareness training and published policy on Web.
- Having our employees being our eyes/ears is the best deterrent.
- Having the right employees, doing the right thing and creating a balance between the two.

Single Most Effective Security Policy/Practice (continued)

- I believe awareness and recognition of an event is the best practice we have in use today at our firm.
- I give employees advice on protecting their home computers, and in turn ask for their assistance in protecting office computers.
- Intro information assurance briefing for new employees, regular information assurance training, use of new work monitoring and incident response teams.
- Knowledge - the educated end-user is the single most effective counter to cyber-threats.
- Knowledge awareness prevention.
- Make the computer users accept their responsibility.
- Mandatory yearly refresher security training.
- Ongoing security awareness training to inform employees of various threats to information assets.
- Education of work force on the issues of security.
- Employee awareness combined with inappropriate use policy - deterrence is stronger than physical barriers.
- Posting of security breach by an individual in the elevators.
- Probably the information protection training - it's mandatory on an annual basis - it raised awareness and led many people to bring to our attention attempts at obtaining information fraudulently.
- Regular security awareness training covering current events.
- Repeated / continual employee education.
- Require employees to obtain CISSP certification.
- Security awareness.
- Security awareness education coupled with a robust internal IT security team and processes.
- Strong awareness program at all levels: executives, managers, employees, suppliers.
- The most important factor is that the people on the network know that there ‘is’ a way to detect activity that is out of normal ranges..
- The security awareness brochure with reporting reference that is distributed to all employees.
- The single most effective security policy is education..
- Training and communication.
- Training end users (social engineering) and spam filtering as well as firewalls.
- Training of current employees.
- Training on procedures to avoid most email attacks has dramatically cut the time spent on email sorting.
- User training, and continued enforcement.
- We use training, audits and IDS.
- Web-based policy training and sign-off.

Require Employees/Contractors to Sign Acceptable Use Policies

- Confidentiality agreement for the protection of patient healthcare information.
- General security policy statement signed by employees during the hiring process getting law enforcement offices involved.
- Sign oath.
- Signed Network and Computer Usage Policies and proper instruction on its interpretation.
- Signing of statement saying you understand the security of computers and their use.
- User use policy signed by each user.

Employee and/or Contractor Background Examinations/Government Security Clearances

- Background checks and a professional environment along with security practices that support the business process are key to stopping e-crime.
- Backing checking contractor candidates followed by background checking candidates for employment.
- Employee background checks.
- Employee background security checks.
- Enforcement of established policy to the point of firing employee for inappropriate conduct.
- Pre-hire and pre-termination screening of employees.

Corporate Security/Hired a Chief Security Officer (CSO) or
Chief Information Security Officer (CISO)/Security Team

- Computer incident response team, appropriate policy.
- Computer security incident response procedures.
- Coordinated Incident Response teams to quickly respond to worm and virus attack.s
- Corporate security and IT security associate working in conjunction with Corporate Loss Assessment Committee.
- Creation of CERT team.
- Facility (building) security that reduces the risk to communications networks, control systems and maintenance functions.
- Implementing and information protection program that is well supported by top management.
- Incident Response Team.
- Our security incident response processes.
- Security standards and electronic usage guidelines.
- Small, dedicated team combined with mild security measures.
- Systems security as it outlines the security measures for bringing up systems and access controls to be in place.
- Systems security task force weekly meetings to identify potential issues and takes steps to resolve them.
- Technicians that continuously watch the network or operational anomalies.
- The ability to proactively scan for and remove connected systems from our network for failure to comply with our policies.
- The system architecture provides multiple security layers.

No major system in place

- Common sense.
- We are a small enough organization that reviews of 'suspicious activities' leads to immediate action, with no red tape in the way of a solution..
- We do not compartmentalize, do not use ACLs or any other firewall beyond the external perimeter. We rely on mostly luck since security products and services cost more than what they protect/detect.
- When in doubt, don't do it.

Corporate Ethics

- Corporate ethics- we're all cops or support personnel.
- Maintain confidentiality, integrity, and availability.

Include Security In Contract With Vendors/Suppliers

- Termination of employees or contractors for inappropriate or criminal use.
- The policy governing network access by vendors, business partners, and road warriors- same standard .for everyone and it eliminates presentations done on a vendor machine in our facilities.

Can't Disclose Information
1 response

Not applicable
8 total responses

None
11 total responses

Verbatim Comments - Electronic Crime Most Proud of Preventing or Solving

When asked to briefly describe (1-2 sentences) the electronic crime attempt or occurrence that they are most proud of preventing or solving, security and law enforcement executives provided the following responses:

Use of 3rd Party to Help Prevent/Solve eCrime

- 3rd-party external network analysis
- Collaboration between Internal Audit and IT to determine and prove the creation of false documents
- IDS catching foreign intrusions
- One of our sites was defaced regularly. Support contractor was directed to implement basic configuration standards to prevent attacks. This eventually resulted in the consolidation of the security detection and control functions to one organization group.
- We have a computer information systems security class that is currently NSA approved.
- We used these students to track down the last problem.

Prevention of Hackers

- A college student hacked into our system and re-arranged some images and some text. He was eventually caught by tracing the IP address and prosecuted.
- Attempt to hack into our CC data.
- Attempt to launch a DOS on our web servers
- Attempts to hack the network by outside contractors, who were unable to do it.
- Attempts to penetrate our customer information database
- Breakup of widespread hacks that lead to DDOS attacks.
- Computer Incident Response Team (CIRT) worked as an effective team in multiple recoveries from malicious virus attacks initiated by outside hackers.
- Currently employee was detected hacking into CEO's email account. Resulted in termination.
- Discovering that a student was trying to use the account of a regular employee who was on vacation.
- Hacker intrusion
- Hacks into financial institutions to obtain credit card information
- Hijacking.
- Identification of internal hacker
- Internal hacking detection
- Massive abuse of compromised ('zombie') machines on other networks by one of our customers
- Multitude of worm and virus attacks on network numbering over 65,000
- Our best triumph in protection has been the detection and location of an outside hacker who had gained access to some of our systems.
- Preventing employee from hacking into the system
- Preventing hackers
- Previous employee attempting to gain access to HR system
- Solved a hacker incident working in cooperation with local FBI agents as crime involved breaking into an EDI payment database.
- Solved a student hack against a university
- Terminated employee using hacker software from network
- The constant hack attempts on our Web servers
- Tracking down a hacker and sending him an aerial photo of his neighborhood.
- Tracking off-shore hackers resulting in their arrest
- Upon recovering from a major hacker attack, when we turned on our outside connections, we were hit by hackers at the rate of 5 - 10 per second and nobody got through.
- We are most proud of solving and catching a break-in, before the control of a server was completely lost.
- We had received reports of a system attempting to hack into our network and traced it back to a military device in Quantico, VA. The device's security had apparently been breached, and we were able to alert the military installation's NOC of its problem before any further systems were impacted.

- We have traced several hackers back to their home sites and systems, and let them know that they have been identified by us.
- 'White Hat' team from other agency tried an unannounced hack to our system and did not get through.

Prevention of Virus Attacks

- A combination of user education campaigns and a layered anti-virus design resulted in zero virus/worm exposures to our company over the last 12 months. (Microsoft-based company)
- A pop-up covered the entire screen of the monitor with a black background, and offered to clear the screen if the employee would 'click here to clear it'. The employee recognized that we could not determine what would happen if he 'clicked here' to clear the screen, and he avoided the issue by shutting down and rebooting the system.
- A virus got into the network via an outside contractor and was quickly quarantined to a small segment of the network and then eradicated with no disruption to operations.
- Agency does a good job of preventing email virus and worms. Use purchased software (and updates) to fix patches - (automated system) are very effective.
- Any occurrence of intrusion that is found and subsequently thwarted is a success and we have accomplished just that.
- Being able to control the spread of viruses
- Being able to stop a worm attack in mid-stream and keep the disruptions to users to a low level
- Code Red - my team successfully identified it and set in place methods to combat and contain.
- DDoS
- DDoS attack that affected several of my computers was stopped by implementing a filter system in advance at the company of our ISP.
- Detection of a virus over a weekend period, allowing the response team to purge network and continue operations with little or no loss of data
- Discovering a mass-mailing worm on an unattached PC by watching IP traffic patterns
- The problem was discovered within minutes and removed before it could wreak havoc beyond this location.
- Fast quarantining of virus attacks that manage to get through
- Getting a call while on vacation 2 weeks before Blaster hit because the network was slow. Made the call to block all Windows SMB ports, which as an ISP was a major decision. Turned out to be a hardware problem, but the blocks were left in place and the only Blaster infections on a huge network were through dial-up and laptops infected while connected to other LANs.
- Good virus detection across network has kept network stable during nationwide attacks
- Have kept the major worms and viruses from infecting our systems
- I consider the virus hit in October the big one. I was on board only weeks when it hit and it allowed the organization to change its mode of handling viruses as well as bring all servers up to par.
- Identified the onset of Code Red back in 2001 due to the honey pots and NIDs solutions we built in house. We identified suspicious traffic and reported the information we were spared from Nimda, Code Red, Slammer, Blaster, etc., due to the combination of our proactive patching and 24/7/365 security configuration auditing as our real time NIDs devices.
- Identifying and preventing a brand new virus from spreading very far
- Intrusion of Malware/viruses into network
- Learning to cloak myself better to keep away Trojan horse and worm hackers.
- Malware infections that brought down other government agencies
- Management at home PC violated with 100+ viri, worms, Trojans, and two unknown hosted P2P Web sites. PC restored, information gathered and turned over to ISP for information. Hack originated in Germany.
- Preventing Trojan's from penetrating our networks.
- Preventing virus attacks through Business Partner connection, responsive patch management process
- Significantly reducing virus incidents by employing both automated updating of virus protection software and instituting a patch program to keep systems up to date.

- Social engineering attempts, virus/Trojan/Malware detection
- Student installed a backdoor Trojan on one of our computer lab systems. Our network virus software picked up on it.
- The IT Help Desk staff were able to quickly isolate the few infected machines when the 'Beagle' virus hit, removed them from the network, and repaired them. This was complicated by the almost simultaneous release of the 'Netsky' virus, which was also stopped from spreading beyond only a few machines (out of 1,100).
- The recent rash of Novarg, MiMail, MyDoom, Netsky viruses was detected at its inception by our organization. We helped establish solid definitions to defend against those initial outbreaks.
- Tracking a former employee spamming to infect network with virus. Law enforcement was no help, so I did detection myself and effectively protected front and back doors
- Until Blaster last year, our network/PC security group had our firewalls so well locked down and our AV and patches so up to date that no major instances of a virus had occurred. Blaster/Welchia did get us due to short timeframe, but the group's overall record is still excellent.
- Virus attacks (2 mentions)
- Virus attacks; Internet intrusions
- Virus designed to bring entire system down
- Virus detection and hacker detection systems we have recently put in place have been very effective in stopping attempts at intruding into our system
- Virus infections that were stopped by intrusion prevention
- Virus prevention is the main object of our security prevention.
- Viruses, DoS, inappropriate Internet access
- W32/Mydoom virus (and all its variants) prevention
- We haven't been infected with any of the viruses that have come out lately and our systems completely blocked them all.
- We prevented Slammer and Blaster from impacting us at all with a proactive program of patching, filtering, and response.
- Where the latest attack of the Blaster/Nachi worm dramatically impacted many companies, our established policies, anti-virus technologies and user awareness relegated these attacks as harmless. Less than .1% of the computers in the organization were impacted.

Prevention of "Denial of Service" Attacks

- A denial of service attack
- A denial of service attack that was preventing our customers from accessing their email
- Primarily denial of service attacks on a 'routine' basis
- Putting in more powerful hardware and software to stop denial of service attacks.

Intrusion Prevention

- A doctor at a client site loaded a file-sharing program to the Internet Information server and it mapped the entire network to the internet.
- An individual placed a Wireless Access Point on our network, inside our firewall.
- Daily attempts from outsides to gain access to our systems - hundreds daily
- Deployed a new intrusion prevention system that functions very well. System has incident logging only for investigative purposes.
- Existing compromise of Web facing system
- Firewall
- Firewall probing that was discovered from within the organization
- Foiling SMTP Relay from Central and South American IP addresses.
- Implementation of firewall rules for outbound traffic was most useful in illustrating nefarious activities on the network.
- Intrusion detection having firewalls and sniffers in place
- Intrusion detection systems and firewalls

- Preventing wireless access to core network files
- Removing a dial-up modem from an old development Web server that people were using as a remote gateway into the network
- Several attacks against a hardened Web server
- Systems resistant to outside penetration despite frequent attempts

Efforts with Law Enforcement

- A former employee of a law firm accessed numerous user accounts and downloaded confidential files. Am also proud of helping stalking victims obtain restraining orders from those that harass them online.
- A leak of proprietary information, solved and the perpetrator prosecuted.
- Security working with local law enforcement identified, arrested, and prosecuted this terminated employee.
- An IT employee who was arrested for an unrelated offense and hacked into the system with two others - all arrested, charged and convicted.
- Attempt by an employee to engage in sexual activity with a minor across state lines.
- Basic network attacks
- Capture of theft of customer identity
- Case involving the distribution of child porno - local business set up as ISP - the business was 90 percent child porn sites. Federal prosecution of this case
- Check fraud involving an employee - our computer forensic investigation provided the evidence with which to arrest and indict the individual.
- Child exploitation in which the child was sexually assaulted
- Child Pornography
- Defacing of the state's homepage - perpetrator was found by law enforcement with help from our staff.
- Each occurrence holds an equal amount of pride and relief.
- Embezzlement discovered within payroll management
- Employee access to child pornography detected, investigated and referred to law enforcement, led to termination and prosecution.
- Employee altering records to move money into personal account
- Grand theft by use of stolen credit card used to make purchases on Internet sites
- Halting inappropriate use by employee
- Inappropriate access of data on the part of a first line manager
- Inappropriate access to unauthorized web site material
- Inappropriate use of corporate technologies
- Multinational smuggling ring
- Operating of illegal foreign futures exchange over Internet to US customers.
- Phishing, mishandled hardware devices containing confidential information
- Phising scam to a member that would have caused them to lose their identity along with life savings
- Pornography
- Prevented loss of proprietary data.
- Purposeful losing employee data by office manager
- Release of privileged information
- Several child porn cases
- Solved restored and reported on malicious data destruction by an associate
- Stolen proprietary information (software code)
- Successful investigation of two employees in a network operations center (NOC) downloading customer data for personal use - two-month investigation revealed system weaknesses and protected reputation of company. Employees fired, not prosecuted.
- Theft of mission-critical data
- Transferring company information to outside sources
- Unauthorized access to private information

- USSS Lenny Rose case
- We were able to aid local authorities in apprehending an abusive parent/child pornographer who assumed our network gave him anonymity.
- We were able to shut down two phishing schemes within two to three hours.
- We were an early victim of phishing scams - by contacting the local secret service ASAP was able to get the offending Web site shut down.

Internal Threats

- An employee using outside email cover threatened the life of an upper manager. IT/Corp.
- An overseas employee sent threatening e-mail to our CIO.
- Identifying the system and user that a kid was sending threatening emails to a teacher
- Intercepting and monitoring of harassing email to staff member that had the potential to lead to physical injury to staff member

Prevention Through Network Monitoring

- By monitoring our network for intrusions we were able to find and investigate DoS zombie systems before they were involved in malicious activity.
- Detection of potential sharing of proprietary trade secret information
- Ensure that we have excellent 7/24 monitoring of our network boarder that's accepting traffic from the Internet and/or third-party business partners
- External attacks
- File transfer by unauthorized persons
- Limiting access to unauthorized sites
- Prevention of theft of intellectual property and software resources - anticipating behavior of employee we incapacitated his ability to extract or access information before any damage could occur.
- Purchase of computer components and assembly into finished PCs, then selling - caught by monitoring of electronic mail system.
- Showing employees how easily their actions are audited and tracked
- Theft of time - keeping employees from surfing the Web for hours during the work day.
- Uncovered open proxy
- Using Internet auditing software found file sharing and stopped immediately.
- We track, monitor, and sometimes block Internet traffic to sights/areas not deemed appropriate and/or relevant to our daily operations.
- We used a 3rd-party vendor to do a check for rogue wireless access points. We found a contractor who had set one up in violation to policy. He is now removed from the account.
- When a user attempted to set up an unauthorized Web page and was detected by our monitoring activities.

Password Policy

- By just the use of password to access the network, no one can login our network without our permission.
- Determining that an information leak probably comes from violating our sharing password policy. Since it was not investigated thoroughly, evidence remains circumstantial - but it's a pretty strong indication.
- Password breaking attempt

Prevention of Identity Theft/Fraud

- Computer hardware fraud case where ringleader was sentenced to Federal Prison
- Computer method identity theft/fraud
- Design theft
- Fraud attempts by contractors

- Fraud occurring because of network loopholes allowing access without authentication
- Fraud using our IT systems
- Identity theft (2 mentions)
- Identity theft cases
- Internal data theft
- Routinely we catch credit card thieves because of our tracking ability and those people wind up caught by law enforcement for more major crimes, including theft, rape, murder and drug.
- Trade secret theft
- Uncovered credit card data theft numerous times from different locations
- Very ironically, a local retired law enforcement officer was a victim of ID theft, from a transaction on the auction company e-bay. A potential victim from London, England, contacted our agency and we were able to prevent a fraud from being committed.
- We had a major assault last summer of people calling into the company misrepresenting themselves as officers from our parent company requesting names, telephone numbers, earnings reports, budgets, etc. Due to the raised awareness, people informed the information security office and we were able to prevent the loss of information.

Increased Company Awareness

- I am most proud of getting the Company (Executive Management) to recognize that laws apply to private companies that provide consumer financing - GLBA. Dept., Budget and staff went from 0 to 8 (including myself) and budget to 8 million.
- Identification of published vulnerabilities that directly affect my organization. Patch deployment is made simpler with that knowledge.
- Modifying historical corporate view that programmers had authority to modify security values and filters.

All Incidents

- All of them
- All terminations resulting from inappropriate access to protected healthcare information
- Each occurrence holds an equal amount of pride and relief.
- Most of them - this survey did not examine attempts vs. successful intrusions. 1 million vs. 5
- Nothing stands out - ongoing

Not Pleased With Current System/Nothing Stands Out

- Not that proud of where we are in IT security practices.
- Unfortunately most of it has been clean up and discovery after the fact not prevention. Not much can be done once former employee has fled the country.

N/A

27 total responses

Don't Know

5 total responses

No Occurrences of eCrime

26 total responses

Cannot Disclose Information

7 total responses

Summary of News Coverage Through 7/21/04

PRINT (Total Reach = 6,141,503)
- Washington Post, 5/25/04: In Brief
- Kansas City Star, 5/25/04: On the Net
- Investor's Business Daily, 5/26/04: Online Crime Cost $666 Mil in '03
- USA Today, 6/15/04: Snapshot: Electronic Attacks on Firms
- Sacramento Bee, 6/22/04: Electronic Attacks on Firms
- USA Today, 7/8/04: Snapshot: Companies Hit by More Cybercrime
- CSO Magazine, 7/04: Top 10 Most Effective Cybercrime Policies

RADIO
- KGO-AM Radio (ABC, San Francisco), 5/25/04: KGO Radio News -Larry Johnson Interview
- KNX-AM Radio (CBS, Los Angeles), 5/25/04: KNX 1070 NewsRadio-Bob Bragdon Interview
- KYW-AM (NBC, Philadelphia), 5/25/04: Newsradio

TELEVISION
- CNN Headline News, 5/25/04, 1:15pm ET: Bob Bragdon Interviewed by Renay San Miguel

WIRE
- United Press International, 6/14/2004: Web-savvy Phishers Net Surfers

ONLINE
- WashingtonPost.com, 5/25/04, Study: Online Crime Costs Rising
- National Journal's Technology Daily, 5/25/04, Executives See Rise In E-Crimes
- Ukranian Computer Crime Research Center, 5/25/04, Computer Crime Costs
- KSL-TV, 5/25/04: Corporate Execs Shift Their Focus To Outside Cyberthreats
- Government Technology, 5/25/04: 2004 E-Crime Watch Survey
- Security Focus.com, 5/25/04: Study: Online Crime Costs Rising
- BizReport.com, 5/25/04: Study: Online Crime Costs Rising
- ECommerceTimes.com, 5/25/04: Study: Online Crime Costs Rising
- Black Enterprise Magazine, 5/25/04: Study: Online Crime Costs Rising
- CNN Money, 5/25/04: Study: Online Crime Costs Rising
- Kiplinger.com, 5/25/04: Study: Online Crime Costs Rising
- ITtoolbox Online, 5/26/04: Study: Online Crime Costs Rising
- Daily Business Journal Online, 5/26/04: E-Crime On the Increase
- Kansas City Infozine, 5/27/04: Online Attacks on Corporate & Government Networks
- WashingtonPost.com, 6/1/04: Online Crime on the Rise
- Yahoo! News, 6/11/04: Hack Attacks Drop, Cybercops Say
- ComputerWeekly.com, 6/11/04: Hack Attacks Down on Last Year, Says Survey
- MacCentral.com, 6/11/04: CSI, FBI survey Finds Hack Attacks Down Again
- PCWorld.com, 6/11/04: Hack Attacks Drop, Cybercops Say
- TechWorld.com, 6/11/04: Hack Attacks Down Again, Says FBI
- USA Today.com, 6/15/04: Snapshot: Ways Companies Watch Workers
- ITtoolbox Online, 6/15/04: Web-savvy Phishers Net Surfers
- CRM News, 6/15/04: Web-savvy Phishers Net Surfers
- Chemical Week, 6/23/04: Break-In Losses Decline Again
- ContinuityCentral.com, 6/30/04: 2004 E-Crime Watch Survey
- IOMA.com -Security Director's Report, 8/1/04, SdR News Briefs

NEWSLETTERS
- Washington Post E-Newsletter, 5/26/04: Online Crime on the Rise
- Continuity Guide, 6/9/04: Financial Institutions Report Twice As Many Cyber Attacks