2005 E-Crime Watch™ Survey

Summary of Findings

Conducted in cooperation by

United States Secret Service

CSO
The Resource for Security Executives

Carnegie Mellon
Software Engineering Institute
CERT® Coordination Center

Table of Contents

Purpose & Methodology

The 2005 E-Crime Watch survey was conducted by *CSO* magazine in cooperation with the U.S. Secret Service and Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center. The research was conducted to unearth electronic crime fighting trends and techniques, including best practices and emerging trends. Respondents' answers are based on the 2004 calendar year. A similar version of this survey was also conducted in 2004 with corresponding answers from the 2003 calendar year. Trending data is provided where relevant.

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

Electronic crime: any criminal violation in which (new in 2005: a computer) or 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 March 3 to March 14, 2005. Results are based on 819 completed surveys, up from the 500 for the 2004 survey. A sample size of 819 at a 95% confidence level has a margin of error of +/- 3.4%.

In addition to the 2005 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, U.S. Secret Service

Survey results were announced on May 3, 2005. Within the first 30 days of its release, this year's survey once again attracted significant news media coverage from more than 20 outlets, including *Investor's Business Daily*, *United Press International* (UPI), *USA Today*, and Washington Times.com. According to a report from PR Newswire (the service with which the news release was distributed to media), the survey was accessed by 758 individuals since its release (i.e., 700 public viewers and 58 journalists). In addition to its U.S. appeal, the survey was accessed by media from twelve other countries including Argentina, Belgium, Canada, Czech Republic, El Salvador, Germany, Ghana, Philippines, South Africa, Spain, Switzerland and United Kingdom. As of July 1, 2005, the survey reached more than three million potential readers worldwide via print publications alone. Additional news media coverage is expected throughout the 2005 calendar year. A listing of news coverage to date is included in the addendum on page 56.

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

Launched in 2002, *CSO* magazine provides chief security officers (CSOs) with analysis and insight on security trends and a keen understanding of how to develop successful strategies to secure all business assets—from people to information and financial value to physical infrastructure. The CSO portfolio includes a companion website (www.CSOonline.com), the CSO Perspectives™ conference and the CSO Executive Council™. The magazine's carefully targeted, controlled circulation of 27,000 security leaders hail from the private and public sectors. The U.S. edition of the magazine and website are the recipients of more than 70 awards to date, including the American Society of Business Publication Editor's Magazine of the Year award as well as eight Jesse H. Neal National Business Journalism Awards and Grand Neal runner-up honors two years in a row. Licensed editions of *CSO* magazine are published around the world, in countries including Australia, France and Sweden. The CSO Perspectives™ conference, the first face-to-face conference designed for CSOs and featuring speakers from the national stage and the CSO community, offers educational and networking opportunities for pre-qualified corporate and government security executives. The CSO Executive Council is a professional organization of CSOs created to advance strategic security practices. *CSO* magazine, CSOonline.com, CSO Perspectives conference and the CSO Executive Council are produced by International Data Group's award-winning business unit: CXO Media Inc.

United States Secret Service Electronic Crimes Task Force (ECTF)

The USA PATRIOT ACT OF 2001 (HR 3162, 107th Congress, First Session, October 26, 2001, Public Law 107-56) ordered the Director of the United States Secret Service to take appropriate actions to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States for the purpose of preventing, detecting and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

The ECTF mission is to establish a strategic alliance of federal, state and local law enforcement agencies, private sector technical experts, prosecutors, academic institutions and private industry in order to confront and suppress technology- based criminal activity that endangers the integrity of the nation's financial payments systems and poses threats against the nation's critical infrastructure. The ECTF model is built on trust and confidentiality without regulators or other outside influences. ECTF law enforcement members develop personal pre-incident relationships with corporate and academic ECTF members and are educated in business concepts such as risk management, return on investment and business continuity plans. As trained first responders to various forms of electronic crimes, ECTF law enforcement members approach incidents with the focus on business designs and information sharing with known corporate and academic individuals. Currently, 15 ECTF models are proving successful in Atlanta, GA; Boston, MA; Charlotte, NC; Chicago, IL; Cleveland, OH; Columbia, SC; Dallas, TX; Houston, TX; Las Vegas, NV; Los Angeles, CA; Miami, FL; New York, NY; Philadelphia, PA; San Francisco, CA; Washington, DC.

Sourcing & Contact Information

Data from the 2005 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:

CSO magazine
Lori Piscatelli Scanlon
508.988.6838

CERT Coordination Center
Kelly Kimberland
412.268.8467

U.S. Secret Service
Jonathan Cherry
202.406.5708

All other inquires about this report may be directed to:

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

Executive Summary

"Security practitioners are faced with new e-crimes on a daily basis. Phishing is a perfect example of a crime that entered the market and has just exploded. It's not enough to just track these crimes. Businesses need to be doing a better job of formalizing their reporting procedures so law enforcement can help them combat the attacks, and over the long haul, minimize the threats."

BOB BRADGON
Publisher
CSO magazine

Results from the 2005 E-Crime Watch survey, conducted among security executives and law enforcement personnel, by *CSO* magazine in cooperation with the United States Secret Service and the Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center, reveals the fight against electronic crimes (e-crimes) may be paying off. Thirteen percent (13%) of the 819 survey respondents—more than double the 6% from the 2004 survey—report the total number of e-crimes (and network, system or data intrusions) decreased from the previous year; 35% report an increase in e-crimes and 30% report no change. Almost one third (32%) of respondents experienced fewer than 10 e-crimes (versus the 25% reported in 2004), while the average number of e-crimes per respondent decreased to 86 (significantly less than 136 average reported in the 2004 survey). Respondents report an average loss of $506,670 per organization due to e-crimes and a sum total loss of $150 million.[1]

E-Crimes Impact

While the average number of e-crimes decreased year over year from 2003 to 2004, 68% of respondents report at least one e-crime or intrusion committed against their organization in 2004 and 88% anticipate an increase in e-crime during 2005. More than half (53%) expect monetary losses to increase or remain the same.

When asked what e-crimes were committed against their organizations in 2004, respondents cite virus or other malicious code as most prevalent (82%), with spyware (61%), phishing (57%) and illegal generation of spam email (48%) falling close behind. Phishing, a precursor to fraud and/or identity theft, jumps from 31% in the 2004 survey to 57%, the largest single percent increase of an e-crime year over year.

Of those who experienced e-crimes, more than half of respondents (55%) report operational losses, 28% state financial losses and 12% declare harm to reputation as a result. Interestingly, one third (31%) of respondents do not have a formal process or system in place for tracking e-crime attempts, and 39% do not have a formalized plan outlining policies and procedures for reporting and responding to e-crimes, demonstrating room for improvement.

[1]Monetary loss data not comparable to 2004 figures due to change in question format implemented to collect more precise data.

"What is important for our partners in the private sector to know is that when an intrusion is not reported to law enforcement, that only enables the criminals to continue to do more—and possibly greater—damage elsewhere. The Secret Service philosophy is one of prevention. Together with our private industry partners, we have a proven track record of aggressively investigating and preventing electronic crimes that could adversely affect the businesses and citizens of this country."

LARRY JOHNSON
Special Agent in Charge
Criminal Investigative Division
United States Secret Service

"The respondents rated employee security training education and awareness programs, and regular communication as the most effective strategies for deterring insider threats. These strategies create a culture of security in the organization, where all employees understand that security is a shared responsibility."

DAWN CAPPELLI
Senior Member of the Technical Staff
Software Engineering Institute's
CERT Program
Carnegie Mellon University

Identifying, Monitoring & Reporting

Organizations, in both the public and private sectors, appear to be doing a better job identifying criminals. Only 19% of respondents experiencing e-crimes or intrusions in 2004 do not know whether insiders or outsiders were the cause, down from 30% in last year's survey. Respondents who identify the culprit indicate that 80% of the attacks come from outsiders and 20% from insiders (a drop from 29% in the 2004 survey).

Eighty percent (80%) of respondents report their organizations monitor their computer systems or networks for misuse and abuse by employees or contractors. Sixty-nine percent (69%) require internal reporting of misuse or abuse of computer access by employees or contractors. However, there is still an opportunity to progress in reporting e-crimes to outside officials. Among organizations experiencing e-crimes, the majority of respondents (78%) report that one or more cases were handled internally without involving legal action or law enforcement. The top three reasons stated for not referring an intrusion for legal action are: damage level insufficient to warrant prosecution (59%), lack of evidence/not enough information to prosecute (50%) and concerns about negative publicity (15%). However, only 31% of respondents consider themselves extremely or very knowledgeable in understanding U.S. laws about computer crimes; only 7% consider themselves knowledgeable about international laws.

Effective Practices

The top technologies used to combat e-crime are firewalls and automated virus scanning used by 99% of respondents, followed by physical security systems (94%), spyware/adware detection software (93%), intrusion detection systems (91%) and manual patch management (90%). For the second year in a row, manual patch management, a common strategy in use, is rated by respondents as the single least effective technology (26%). Among the most effective technologies, the use of firewalls is listed as most effective at 68%, followed by automated virus scanning (66%), encryption (58%), two-factor authentication (56%) and intrusion detection systems (50%). Moreover, the top five security policies and procedures in use by respondents to prevent or reduce an e-crime are: account/password management policies (74%), formal inappropriate use policy (71%), employee education and awareness programs (67%), monitoring of internet connections (65%) and corporate security policy (62%).

About Survey Respondents

Respondent Base Composition

As with the 2004 survey, this year's respondent base comprises two sample groups of security and law enforcement practitioners: 1. *CSO* magazine subscribers and 2. U.S. Secret Service Electronic Crimes Task Force (ECTF) members. The table below shows the number of respondents from each group. One goal successfully implemented in 2005 was to increase the number of completed surveys from both respondent groups.

Composition of Respondent Base	2005 (base: 819)	2004 (base: 500)
CSO Magazine Subscribers	460	345
Electronic Crimes Task Force (ECFT) Members	359	155

Job Title

Fifty-eight percent (58%) of respondents hold an IT management title, down from nearly two-thirds (66%) in the 2004 survey. Those respondents reporting a non-IT management title increased slightly from 8% to 11% in 2005. The percent of survey participants holding a law enforcement title also increased from 12% to 17% in this year's survey (see table below).

Which of the following best describes your job title?	2005 (base: 819)	2004 (base: 500)
IT Management (NET)	58%	66%
IS/IT/networking	29%	34%
Security	29%	32%
Non-IT Management (NET)	11%	8%
Law Enforcement	17%	12%
Other (staff, consultant)	14%	13%

Sector

Among those responding, sixty-two percent (62%) say their organization belongs to the private sector, down from 67% in 2004. Participation by respondents in the law enforcement/prosecutor sector increased to 14% from 10% last year (see table below).

In which category does your organization fall?	2005 (base: 819)	2004 (base: 500)
Private Sector	62%	67%
Government	23%	24%
Law Enforcement/Prosecutor	14%	10%

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

Electronic Crimes Task Force (ECTF)/ Electronic Crimes Working Group (ECWG) Membership

One-third (33%) of respondents currently belong to a U.S. Secret Service Electronic Crimes Task Force (ECTF) or Electronic Crimes Working Group (ECWG).

Are you, your organization or another individual at your organization currently a member of a U.S. Secret Service Electronic Crimes Task Force (ECTF) or Working Group (ECWG)?	2005 (base: 819)
Yes	33%
No	52%
Don't know/not sure	15%

Among those respondents belonging to an ECTF or ECWG, specific groups represented are as follows:

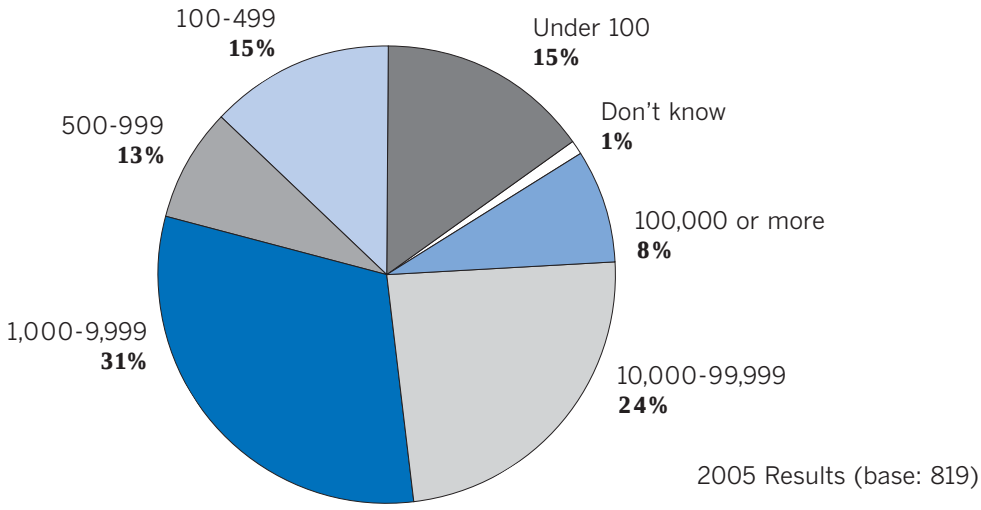
To which of the following Electronic Crimes Task Force (ECTF) or Working Group (ECWG) do you belong to?	2005 (base: 267)
San Francisco	18%
Chicago	13%
New York	13%
Los Angeles	11%
Boston	6%
Charlotte	6%
Dallas	6%
Washington DC	6%
Birmingham	5%
Cleveland	5%
Las Vegas	4%
Miami	3%
Orlando	3%
Oklahoma City Tulsa	2%
Philadelphia	1%
Houston	<1%
Minneapolis	<1%

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

Number of Employees

Respondent breakout by number of employees remained consistent from 2004 to 2005 with 63% of respondents employed by large organizations (1,000+ employees), 21% in mid-sized organizations (100-999 employees) and 15% employed by small organizations of less than 100 employees (see table below).

What is the total number of employees in your entire organization (please include all plants, divisions, branches, parents and subsidiaries worldwide)?



Annual Security Budget

The following table breaks out annual security budgets at respondents' organizations by IT security, corporate/physical security and converged security spending (see definitions below).

What was your organization's approximate annual budget for information and corporate/physical security products, systems, services and/or staff in 2004?	IT Security Spending* (base: 819)	Corporate/ Physical Security Spending* (base: 819)	Converged Security Spending* (base: 819)
Over $100 Million	4%	3%	2%
$10 Million -$99.9 Million	5%	7%	5%
$1 Million -$9.9 Million	15%	12%	12%
$500,000 -$999,999	4%	4%	4%
$250,000 -$499,999	5%	5%	4%
$100,000 -$249,999	10%	7%	6%
$50,000 -$99,999	9%	8%	7%
Less than $50,000	18%	18%	18%
Don't know	30%	36%	42%

*Definitions:
IT security spending (spending on hardware, software, services, staff for the specific use of protecting the organization's electronic assets ONLY, i.e., firewalls, anti-virus, intrusion prevention systems, content filtering, etc.)

Corporate/Physical security spending (spending on hardware, software, services, staff for the specific use of protecting the organization's physical assets ONLY, i.e., CCTV systems, locks, guard services, etc.)

Converged security spending (spending on hardware, software, services, staff for the specific use of protecting the organization's electronic AND physical assets, i.e., access control systems that control access to both physical and IT assets, etc.)

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

Critical Infrastructure Sector

Eighty percent (80%) of survey respondents report that their organizations belong to a critical infrastructure sector, consistent with the 2004 survey (see table below).

Please indicate the critical infrastructure sector to which your organization belongs:	2005 (base: 819)	2004 (base: 500)
Government	25%	28%
Information & Telecommunications	18%	19%
Banking & Finance	14%	15%
Public Health	5%	8%
Defense Industrial Base	4%	3%
Emergency Services	4%	1%
Transportation	3%	3%
Energy	2%	2%
Food	2%	2%
Chemical Industry & Hazardous Materials	1%	1%
Postal & Shipping	1%	<1%
Agriculture	<1%	N/A
Water	<1%	<1%
Not applicable	20%	19%

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

Primary Industry

Survey respondents work in a wide cross-section of industries (see table below). The percentage of respondents who work in the law enforcement/security industry increased to 15% from 11% in 2004.

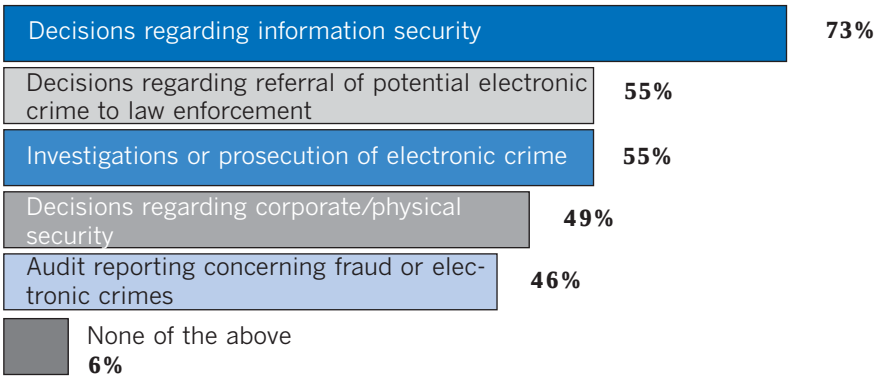
Which of the following best describes your organization's primary industry?	2005 (base: 819)	2004 (base: 500)
Law Enforcement/Security (non-emergency services)	15%	11%
Information & Telecommunications	12%	12%
Banking & Finance	11%	13%
Government	8%	10%
Education	7%	10%
Electronics/Technology	5%	5%
Health Care	5%	8%
Military	4%	4%
Services	4%	4%
Insurance	3%	3%
Retail, Consumer Products	3%	1%
Defense Industrial Base	2%	1%
Emergency Services	2%	<1%
Research/Development	2%	1%
Transportation	2%	2%
Agriculture	1%	<1%
Chemical	1%	1%
Construction/Real Estate	1%	1%
Electric Power	1%	1%
Food	1%	<1%
Gas & Oil	1%	<1%
Pharmaceutical	1%	1%
Postal & Shipping	1%	0%
Retail, Food/Drink	1%	1%
Wholesale	1%	1%
Hazardous Materials	<1%	N/A
Natural Resources/Mining	<1%	1%
Water	<1%	<1%
Other	9%	7%

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

Involvement—Security or Electronic Crime Related Decisions

Survey respondents are involved in a variety of security or electronic crime related decisions at their organizations (see table below). Nearly three-quarters (73%) of respondents are involved in decisions regarding information security, down from 79% in 2004. The percentage of respondents involved in decisions regarding the referral of potential electronic crime to law enforcement increased to 60%, from 55% in last year's survey.

Are you personally involved in any of the following at your organization?



2005 Results (base: 819)

Knowledge Level

Respondents indicate a higher level of familiarity with local and national electronic crime laws but know less about international laws surrounding computer crime. Only 11% and 12% (respectively) of those surveyed report they are not knowledgeable regarding electronic crime laws in their state and the United States, while 46% consider themselves not knowledgeable about international laws.

How knowledgeable do you consider yourself in understanding laws surrounding computer crimes? (base: 819)	Extremely Knowledgeable	Very Knowledgeable	Somewhat Knowledgeable	Not Knowledgeable	Don't Know
In your state	10%	27%	50%	11%	2%
In the U.S.	6%	25%	55%	12%	2%
Worldwide	2%	5%	40%	46%	7%

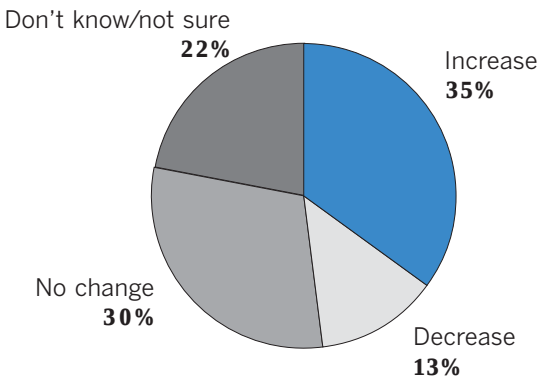
NOTE: percents may not sum to 100 due to rounding.

Electronic Crimes Impact

Change in Number of Electronic Crimes or Intrusions

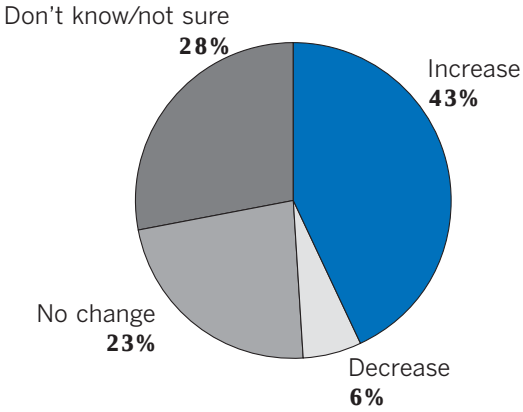
Thirty-five percent (35%) of respondents report that the total number of electronic crimes or intrusions experienced by their organizations increased in 2004 compared to 2003. This number is down from the 43% reporting an increase in the previous survey. Thirteen percent (13%) of respondents say the number of electronic crimes or intrusions decreased from the previous year compared to only 6% in the 2004 survey. Nearly one-third (30%) of respondents report no change in the number of electronic crimes or intrusions up from 23% last year.

Did the total number of electronic crimes and network, system or data intrusions experienced by your organization increase, decrease or remain the same in 2004 compared to 2003?



2005 Results (base: 819)

Did the total number of electronic crimes and network, system or data intrusions experienced by your organization increase, decrease or remain the same in 2003 compared to 2002?



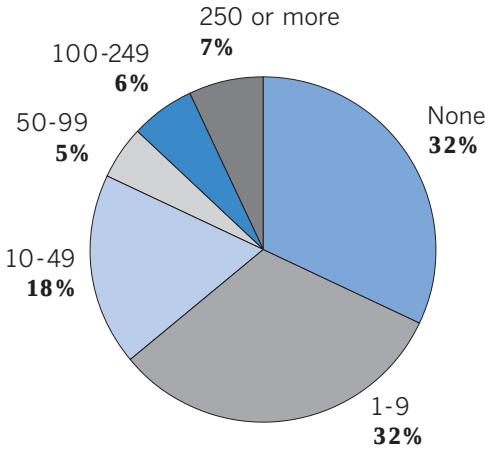
2004 Results (base: 500)

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

Number of Electronic Crimes

Sixty-eight percent (68%) of respondents report that their organizations experienced at least one electronic crime or intrusion (consistent with last year's 70%). The percentage of respondents reporting zero electronic crimes or intrusions also remained constant year over year at nearly one-third (32% and 30%, respectively). The average number of electronic crimes or intrusions at respondents' organizations fell significantly to 86 from 136 in last year's survey.

Please estimate the total number of electronic crimes or network, system or data intrusions experienced by your organization in 2004. Note that each crime should only be counted once, for example any worm or virus that could be classified as an electronic crime should only be counted as a single attack, not once per infected machine (type-in).



Mean 86
Median 3

2005 Results (base: 819)

Monetary Losses from Electronic Crimes

Nearly two-thirds (62%) of respondents are unable to estimate the total monetary value of losses caused by electronic crimes or system intrusions. Of those providing an estimate, 19% said zero while 12% estimated losses at under $100,000.*

Please estimate the total monetary value of losses your organization sustained due to electronic crimes or system intrusions in 2004 (type-in)	2005 (base=777)
$10 million or more	1%
$1 million -$9.9 million	2%
$500,000 -$999,999	1%
$100,000 -$499,999	4%
$1-$99,999	12%
Zero	19%
Mean	$506,670
Median	$0
Sum	$150,000,000
Don't know/not sure	62%

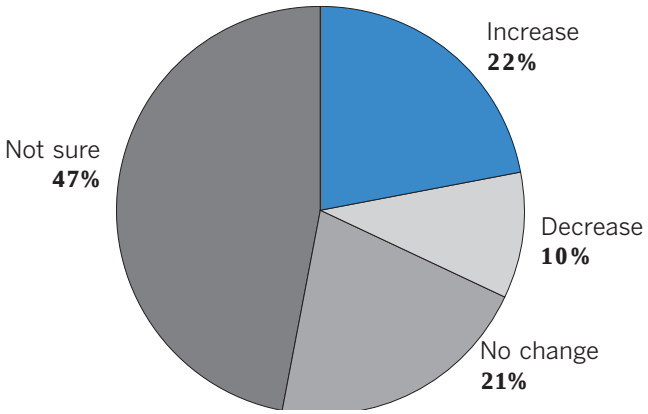
* Monetary loss data not comparable to 2004 figures due to change in question format implemented to collect more precise data.

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

Direction of Electronic Crime Losses

One in five respondents (22%) say that monetary losses caused by electronic crime increased in 2004 while 10% report a decrease and 21% say monetary losses caused by electronic crime stayed the same in 2004 compared to 2003. Nearly half (47%) could not say how monetary losses changed from year to year.

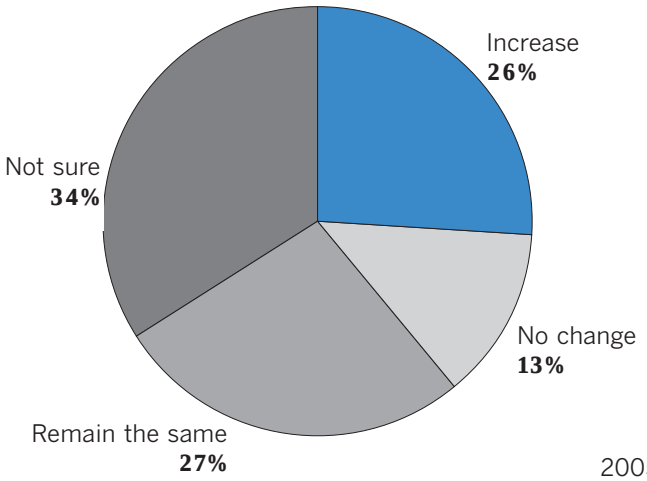
In 2004, did monetary losses to your organization from electronic crime increase, decrease or remain the same compared to 2003?



2005 Results (base: 723)

When asked to predict the direction of monetary losses from electronic crime in 2005, over one half of respondents (53%) expect monetary losses to either increase or remain the same. Only 13% expect monetary losses resulting from electronic crime to decrease, while one third (34%) are unsure.

In 2005, do you expect monetary losses to your organization from electronic crime will increase, decrease or remain the same compared to 2004?



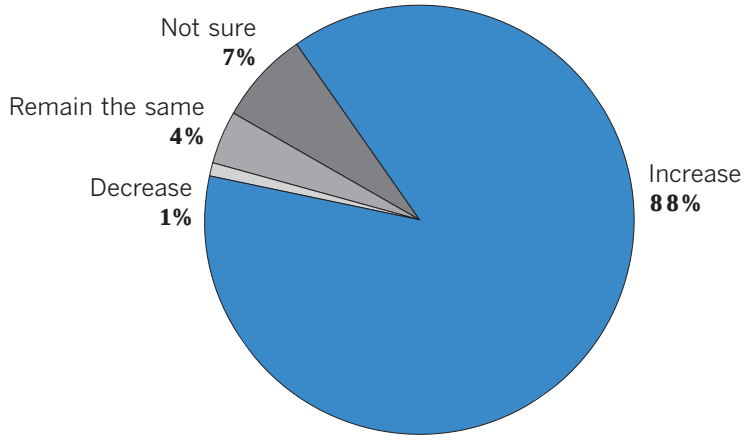
2005 Results (base: 819)

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

Prevalence of Electronic Crime

The majority of respondents (88%) believe the prevalence of electronic crime in 2005 will increase compared to 2004. Only one percent expect that electronic crime will be less prevalent in 2005, four percent expect it to stay the same and 7% are unsure.

In your opinion, do you believe the prevalence of electronic crime in 2005 will increase, decrease or remain the same as 2004?



2005 Results (base: 819)

Types of Losses

The following table breaks out specific types of losses experienced by respondents' organizations. Twelve percent (12%) of respondents say their organizations experienced some type of critical loss, down from 18% in last year's survey. The percentage of respondents indicating no losses increased to 17% from 8% in the 2004 survey.

Which of the following types of losses did your organization experience in 2004? (base: among those experiencing electronic crimes)	2005 (base: 554)
(NET) Non-critical losses	58%
Non-critical operational losses	50%
Non-critical financial losses	26%
Harm to reputation	12%
(NET) Critical losses	12%
Critical operational losses	11%
Critical financial loss	2%
Loss of life	1%
Other type of loss	6%
Not applicable – no losses experienced	17%
Don't know/not sure	17%

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

Types of Electronic Crimes Committed

Among respondents whose organizations experienced electronic crimes in 2004, eighty-two percent (82%) cite virus or other malicious code as the most prevalent type of electronic crime or action followed by spyware (61%), phishing (57%) and illegal generation of spam email (48%). Phishing, not technically a crime but a precursor to fraud and/or identity theft, shows the largest single percentage increase year over year jumping to 57% from 31% reported in last year's survey.

Which of the following electronic crimes were committed against your organization in 2004? (base: among those experiencing electronic crimes)	2005 (base: 554)	2004* (base: 342)
Virus or other malicious code	82%	77%
Spyware	61%	N/A
Phishing	57%	31%
Illegal generation of spam email	48%	38%
Unauthorized access to information, systems or networks	43%	47%
Denial of service attacks	32%	44%
Rogue wireless access point	21%	N/A
Exposure of private or sensitive information	19%	N/A
Fraud	19%	22%
(2004: Employee) Identity theft	17%	12%
Password sniffing	16%	N/A
Theft of intellectual property	14%	20%
Zombie machines on organization's network	13%	N/A
Theft of other (proprietary) info	12%	16%
Sabotage	11%	18%
Web site defacement	9%	N/A
Extortion	2%	5%
Other	4%	11%
Don't know/not sure	3%	8%

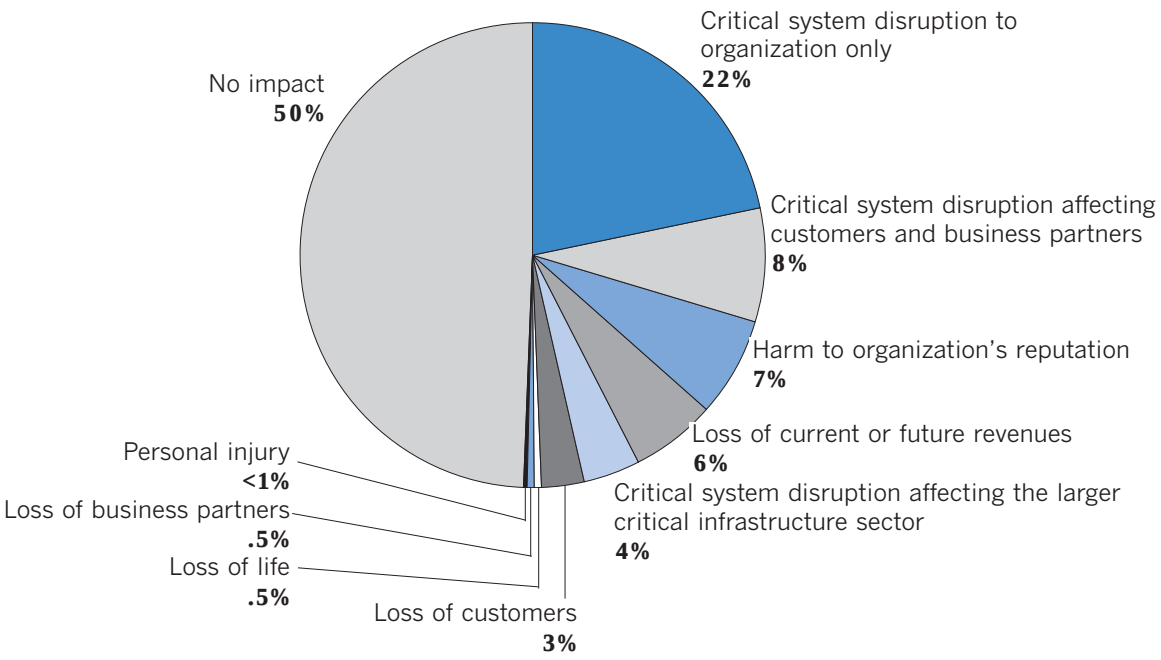
* timeframe: 2003

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

Consequences of Insider Intrusions

Twenty-two percent (22%) of respondents report that the most adverse consequence that ever occurred from an insider intrusion is critical system disruption to the organization only. One half (50%) of respondents report no impact as a result of insider intrusions, up from 41% in last year's survey.

With respect to your organization, what is the most adverse consequence that has ever occurred from an insider network, data, or system intrusion?



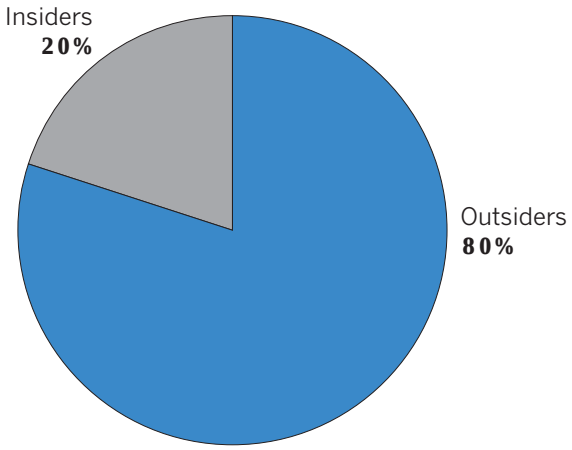
2005 Results (base: 819)

Who Are The Criminals?

Average Percent of Electronic Crimes by Outsiders vs. Insiders

Organizations appear to be doing a better job identifying criminals. Only 19% of respondents experiencing electronic crimes or intrusions in 2004 do not know whether insiders or outsiders were the cause, down from 30% in last year's survey. Respondents who identify the culprit indicate that an average of 80% of the attacks come from outsiders and 20% from insiders (a drop from 29% in the 2004 survey).

Mean Percent of Electronic Crimes Caused by Outsiders vs. Insiders (base: among those experiencing electronic crimes)



2005 Results (base: 554)

Number of Electronic Crimes by Outsiders vs. Insiders

The following tables break out the source of electronic crimes or intrusions and support that a greater percentage of electronic crimes (or network, system or data intrusions) were carried out by outsiders in 2004 compared to the previous year.

How many electronic crimes or network, system or data intrusions are known or suspected to have been caused by... OUTSIDERS (base: among those experiencing electronic crimes)	2005 (base: 554)
None	4%
1 or more (NET)	77%
1-9	42%
10-49	19%
50-99	5%
100-249	4%
250 or more	7%
Mean	102
Median	5
Don't know	19%

How many electronic crimes or network, system or data intrusions are known or suspected to have been caused by... INSIDERS (base: among those experiencing electronic crimes)	2005 (base: 554)
None	43%
1 or more (NET)	39%
1-9	24%
10-49	10%
50-99	2%
100-249	2%
250 or more	1%
Mean	10
Median	0
Don't know	19%

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

Type of Electronic Crime by Source

The following table breaks out specific types of incidents by the source, if known—outsiders or insiders.

You indicated the following types of electronic crimes were committed against your organization last year. Please indicate the source of these crimes, if known. (base: among those experiencing that particular form of electronic crime)	Outsider	Insider	Unknown
Virus or other malicious code (base: 453)	85%	14%	10%
Spyware (base: 338)	89%	11%	7%
Phishing (base: 316)	92%	2%	7%
Illegal generation of spam email (base: 266)	89%	11%	8%
Unauthorized access to information, systems or networks (base: 237)	58%	54%	8%
Denial of service attacks (base: 179)	88%	11%	8%
Rogue wireless access point (base: 117)	29%	72%	8%
Exposure of private or sensitive info (base: 106)	47%	56%	9%
Fraud (base: 105)	80%	35%	5%
Identity theft (base: 95)	81%	23%	12%
Password sniffing (base: 86)	74%	34%	4%
Theft of intellectual property (base: 75)	33%	64%	16%
Zombie machines on organization's network (base: 73)	77%	20%	10%
Theft of other (proprietary) info (base: 65)	54%	55%	9%
Sabotage (base: 61)	59%	44%	8%
Web site defacement (base: 50)	92%	6%	6%
Extortion (base: 10)	60%	30%	10%

Groups Posing Greatest Cyber Security Threat

Thirty- seven percent (37%) of respondents say hackers posed the greatest cyber security threat to their organizations last year, down slightly from 40% in the 2004 survey. Insiders rank second with 23% citing current or former employees as the greatest threat, down from 28% in the 2004 survey. One in five respondents (21%) is unsure which group posed the greatest threat.

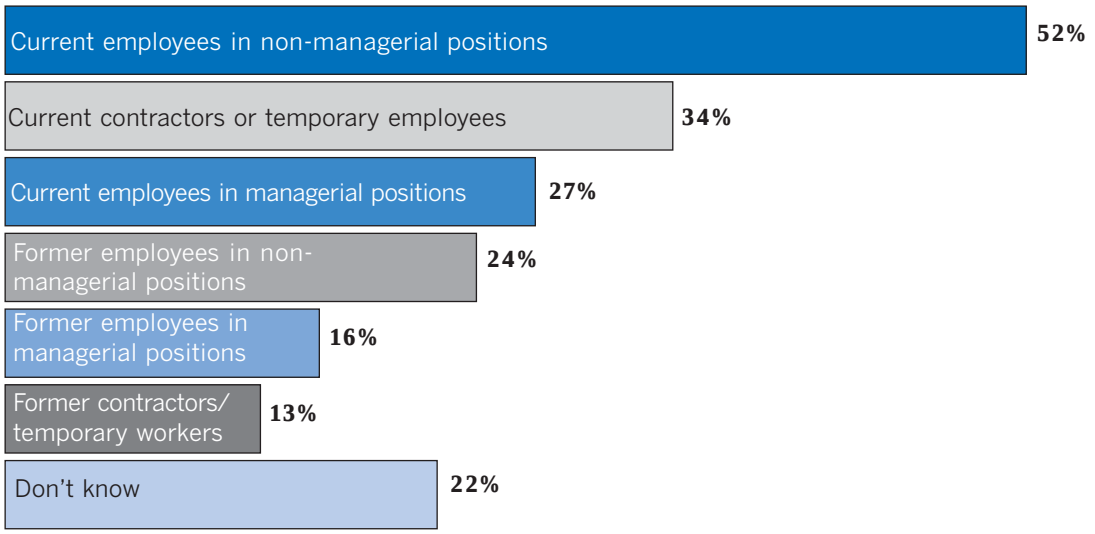
Which of the following groups posed the greatest cyber security threat to your organization in 2004?	2005 (base: 819)
Hackers	37%
Current employees	18%
Foreign entities	6%
Former employees	5%
Information brokers	3%
Current service providers/consultants/contractors	2%
Terrorists	2%
Customers	2%
Suppliers/business partners	1%
Competitors	1%
Former service providers/consultants/contractors	1%
Don't know/not sure	21%

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

Sources of Insider Intrusions

One in five (22%) respondents is unsure the source of insider intrusions last year, up from 9% in the 2004 survey. Slightly over one half (52%) of respondents experiencing insider intrusions say "current employees in non-managerial positions" are the cause. This figure is significantly lower than last year's findings where nearly three quarters (73%) of those experiencing insider intrusions pointed to "current employees in non-managerial positions" as the cause of one or more intrusions. The percentage of those pointing to "current employees in managerial positions" as the culprit also dropped (38% to 27%) as did "former employees in non-managerial positions" (31% to 24%).

Please indicate all sources of insider intrusions in 2004 (base: those experiencing insider intrusions).



2005 Results (base: 214)

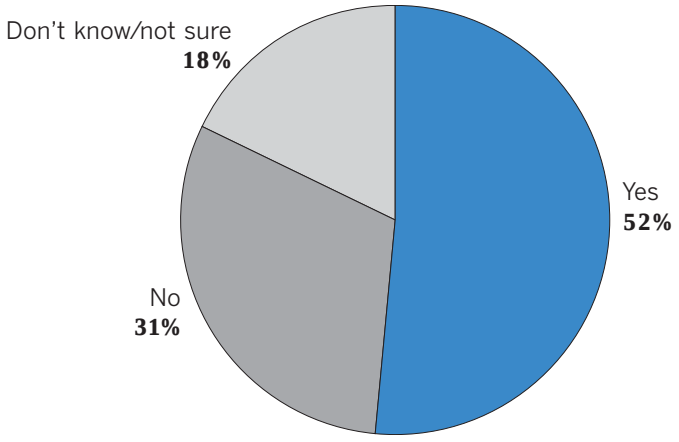
NOTE: percents may not sum to 100 due to rounding.

Monitoring

Formal Tracking Process

Over one half (52%) of respondents say their organization has a formal process or system in place for tracking electronic crime attempts, consistent with last year's findings. Thirty-one percent (31%) say their organization does not have a formal process or system in place for tracking electronic crime attempts, down from 37% in last year's survey (see table below).

Does your organization have a formal process or system in place for tracking electronic crime attempts?



2005 Results (base: 819)

Monitoring for Misuse & Abuse

Consistent with last year's findings, 81% of respondents say their organizations monitor computer systems for misuse or abuse by employees or contractors. Of that group, nearly two-thirds (64%) monitor both systems and networks, 11% networks only and 5% systems only.

Does your organization monitor its computer systems and networks for misuse or abuse by employees or contractors?	2005 (Base: 819)
Yes (Net)	81%
Systems only	5%
Networks only	11%
Both systems & networks	64%
No	12%
Don't know/not sure	7%

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

Responding & Reporting

Formal Plan for Responding & Reporting

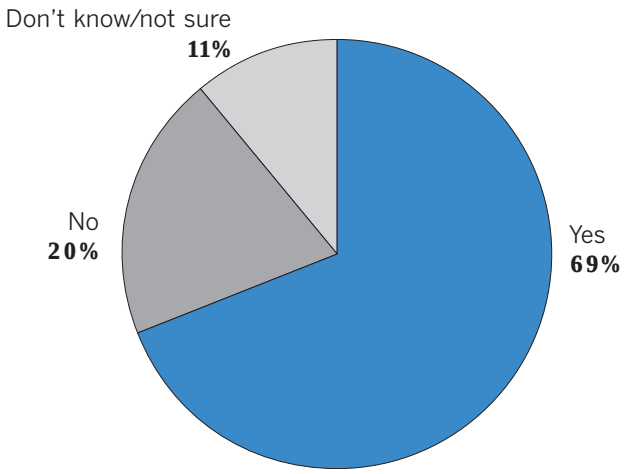
Forty-six percent (46%) of respondents report that their organizations have formalized plans outlining policies and procedures for reporting and responding to electronic crimes, down slightly from 50% last year (see table below).

Does your organization have a formalized plan outlining policies and procedures for reporting and responding to electronic crimes committed against your organization?	2005 (base: 819)
Yes	46%
No (Net)	39%
No, planning to implement next 12 months	18%
No plans at this time	20%
Don't know/not sure	15%

Internal Reporting of Misuse or Abuse

Sixty-nine percent (69%) of respondents' organizations require internal reporting of misuse or abuse of computer access by employees or contractors, fairly consistent with last year's findings (72%).

Does your organization require internal reporting of misuse or abuse of computer access by employees or contractors?



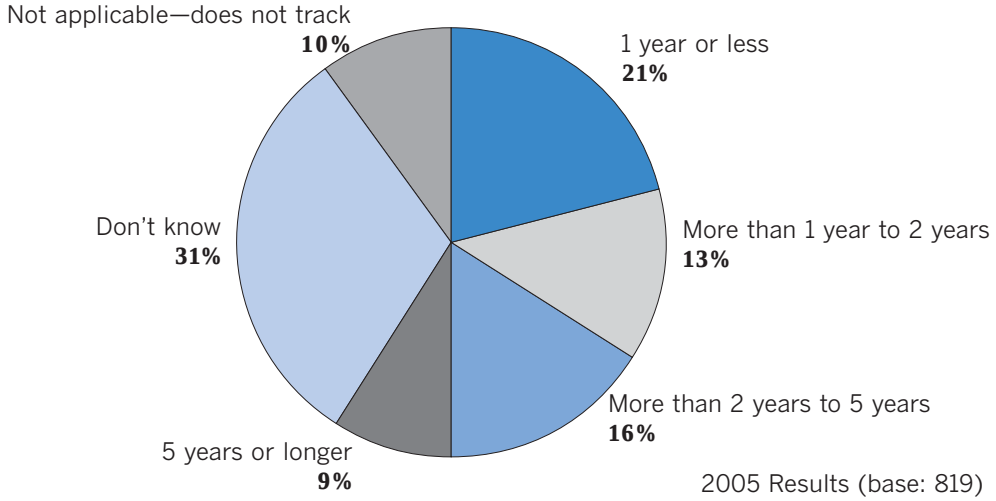
2005 Results (base: 819)

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

Record Keeping

One in five respondents (21%) say their organization keeps records on intrusions for a year or less, 29% between one and five years and 9% for five years or longer. These figures are fairly consistent with last year's findings (see table below). One third (31%) don't know how long their organization keeps records surrounding intrusions (up from 26%). Ten percent (10%) say their organizations' do not track network, data and system intrusions, down from 20% in last year's survey.

How far back does your organization keep records on or otherwise keep track of network, data and system intrusions?



Responding to Intrusions

Among organizations experiencing intrusions, the majority of respondents (78%) report that one or more cases was handled internally without involving legal action or law enforcement. Only nineteen percent (19%) report that one or more intrusions was handled externally by notifying law enforcement, sixteen percent (16%) internally with legal action and 4% externally by filing a civil action.

How Intrusions Handled (base: 554 – those experiencing electronic crimes)	Internally without involving legal action or law enforcement	Internally with legal action	Externally by notifying law enforcement	Externally by filing a civil action
None	6%	69%	65%	80%
1 or more (NET)	78%	16%	19%	4%
1	6%	4%	7%	1%
2	9%	4%	2%	1%
3-5	19%	3%	4%	1%
6-9	7%	1%	1%	0%
10-24	16%	2%	3%	0%
25 or more	22%	3%	2%	1%
Mean	84	6	5	<1%
Median	6	0	0	0
Don't know	16%	16%	16%	16%

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

Reasons Intrusions Not Referred for Legal Action

Fifty-nine percent (59%) of respondents reporting electronic crimes or intrusions at their organizations report that these incidents were not referred for legal action because of insufficient damage levels to warrant prosecution. One half (50%) cite lack of evidence or information to prosecute as the reason for not pursuing while fifteen percent (15%) cite concerns about negative publicity.

If any intrusions were not referred for legal action, please indicate the reason(s) not referred. (Asked to those experiencing electronic crimes)	2005 (base: 554)
Damage level insufficient to warrant prosecution	59%
Lack of evidence/not enough info to prosecute	50%
Concerns about negative publicity	15%
Concerns that competitors would use to advantage	7%
Unaware we could report these crimes	6%
Prior negative response from law enforcement	6%
Other	14%
Don't know	7%

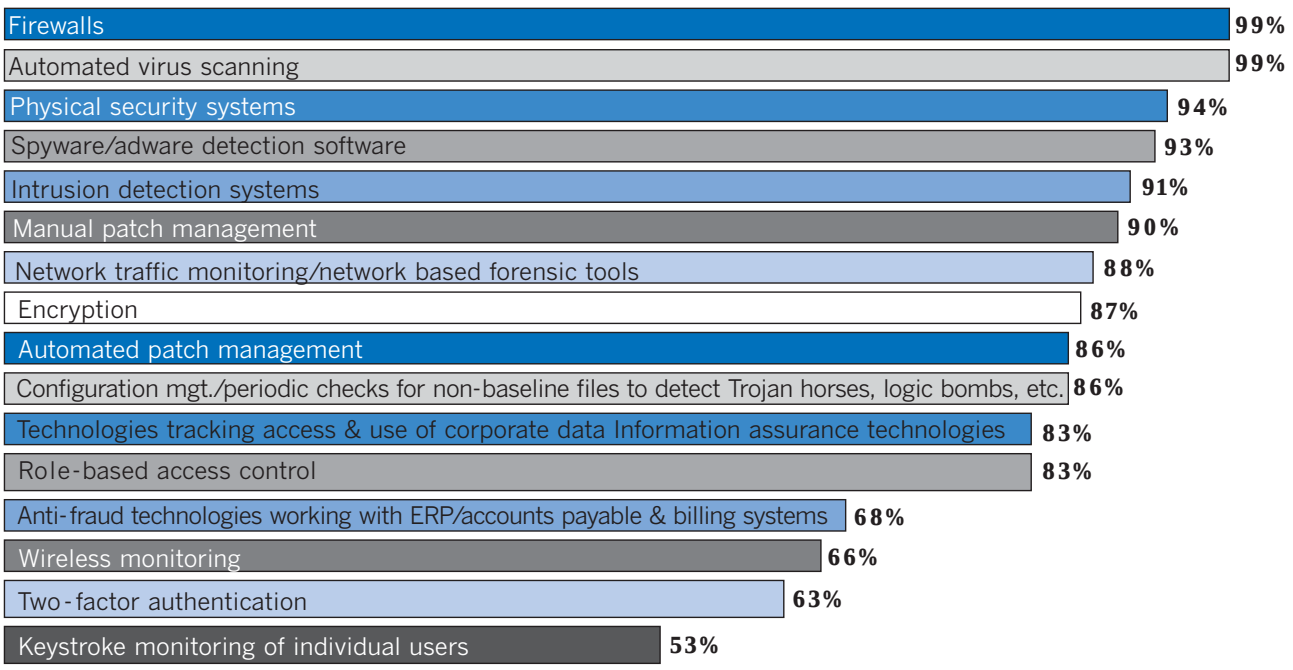
NOTE: percents may not sum to 100 due to rounding.

Best Practices—Technologies

Technologies Installed

Firewalls and automated virus scanning are used by nearly all of respondents' organizations (99%) followed by physical security systems (94%), spyware/adware detection software (93%) and intrusion detection systems (91%). The following table breaks out the percent of respondents with each type of technology in place at their organizations.

Technologies in Use



2005 Results (base: 819)

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

Most Effective Technologies

Among the technologies in use, firewalls is listed as most effective at 68%, followed by automated virus scanning (66%), encryption (58%), two-factor authentication (56%) and intrusion detection systems (50%). The following table shows the percentage of respondents rating each technology extremely or very effective in detecting and/or countering misuse or abuse of computer systems and networks.

Most Effective (Extremely or Very Effective) Technologies in Use (2005 base: among those with technology in use at organization)	2005	2004
Firewalls (base: 810)	68%	71%
Automated virus scanning (base: 810)	66%	N/A
Encryption (base: 715)	58%	N/A
Two-factor authentication (base: 517)	56%	56%
Intrusion detection systems (base: 743)	50%	N/A
Physical security systems (base: 771)	49%	48%
Network traffic monitoring/network based forensic tools (base: 722)	46%	N/A
Spyware/adware detection software (base: 758)	43%	N/A
Role-based access control (base: 677)	42%	44%
Automated patch management (base: 704)	40%	39%
Configuration management/periodic checks for non-baseline files to detect Trojan horses, logic bombs, etc. (base: 704)	39%	N/A
Technologies tracking access & use of corporate data/information assurance technologies (base: 682)— 2004: that track the access & use of corporate data	35%	35%
Anti-fraud technologies working with ERP/accounts payable & billing systems (base: 560)	28%	33%
Wireless monitoring (base: 544)	26%	26%
Keystroke monitoring of individual users (base: 434)	22%	24%
Manual patch management (base: 741)	21%	26%

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

Least Effective Technologies

Manual patch management, a common strategy in use, is rated by respondents as the single least effective technology. The following table shows the percentage of respondents rating each technology not very or not at all effective in detecting and/or countering misuse or abuse of computer systems and networks.

Least Effective (Not Very or Not At All Effective) Technologies in Use (base: among those with technology in use at organization)	2005
Manual patch management (base: 741)	26%
Keystroke monitoring of individual users (base: 434)	22%
Wireless monitoring (base: 544)	15%
Spyware/adware detection software (base: 758)	12%
Technologies tracking access & use of corporate data/information assurance technologies (base: 682)	12%
Physical security systems (base: 771)	8%
Automated patch management (base: 704)	7%
Anti-fraud technologies working with ERP/accounts payable & billing systems (base: 560)	6%
Configuration management/periodic checks for non-baseline files to detect Trojan horses, logic bombs, etc. (base: 704)	6%
Network traffic monitoring/ network based forensic tools (base: 722)	6%
Two-factor authentication (base: 517)	6%
Intrusion detection systems (base: 743)	5%
Role-based access control (base: 677)	5%
Encryption (base: 715)	4%
Automated virus scanning (base: 810)	3%
Firewalls (base: 810)	2%

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

Best Practices– Policies & Procedures

Security Policy

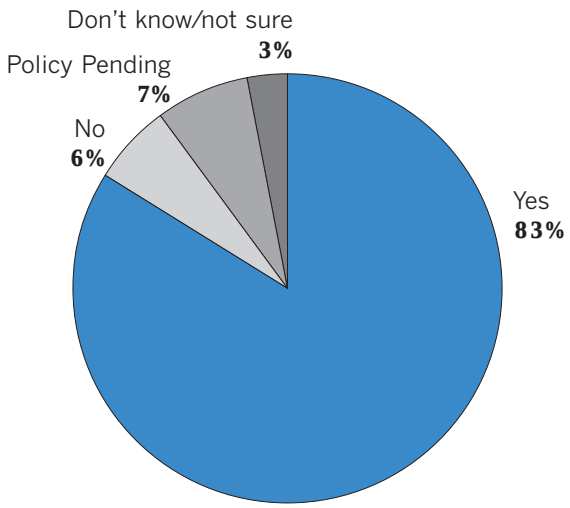
Among those security respondents with a security policy in place at their organization, nearly half (46%) say their organization only updates the policy on an as needed basis and 28% update the policy annually (see table below). These findings are fairly consistent with last year's finding.

How often does your organization review or update its security policy? (base: those with policy in place)	2005 (base: 681)
Monthly	N/A
Every 6 months	5%
Annually	28%
As needed	46%
Other	2%
Don't know	19%

Written Inappropriate Use Policy

Consistent with last year's survey results, eight out of 10 respondents' organizations (83%) 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.

Does your organization have a written inappropriate use security policy for use of networks, data, and systems?



2005 Results (base: 819)

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

Written Inappropriate Use Policy (continued)

Among security and law enforcement executives with inappropriate use policies in place, 54% require employees to review their organization's written inappropriate use policy when hired. Over one quarter (27%) of respondents say employees are required to review and accept the policy on an annual basis. Nearly one in ten (9%) of respondents say employees must review and accept the policy each time data is accessed. Twelve percent (12%) say their organizations do not require employees to review the inappropriate use policy.

Are employees required to review and accept the written inappropriate use policy on any periodic basis? (base: those with policy in place)	2005 (base: 681)
Yes, upon employment	54%
Yes, upon accessing data	9%
Yes, every six months	1%
Yes, annually	27%
Yes, periodically	14%
No	12%
Don't know/not sure	4%

Hardcopy distribution (62%) is the most frequently cited means for distributing inappropriate use policies, up from 57% in the 2004 survey. Email (47%) is also a popular method of communication, consistent with last year's findings. The percentage of respondents indicating that their organizations communicate written inappropriate use policies by web reference or direct communication both decreased from last year's survey.

How does your organization communicate the written inappropriate use policy to its employees and contractors? (base: those with policy in place)	2005 (base: 681)
Hardcopy distribution	62%
Electronic mail	47%
Web reference	39%
Training materials	31%
Direct communication from managers	29%
Training classes	24%
Other	3%
Don't know	1%

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

Policies & Procedures in Place

The top five policies or procedures in place at respondents' organizations are account/password management policies (74%), formal inappropriate use policies (71%), education & awareness programs (67%), monitoring Internet connections (65%) and corporate security policies (62%). The following table shows the percentage of respondents with a particular policy or procedure in place at their organization to prevent or reduce electronic crime.

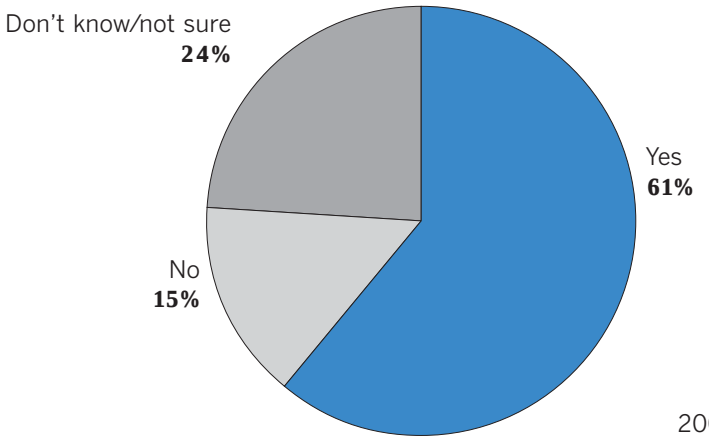
Which of the following security policies and procedures does your organization use to attempt to prevent or reduce electronic crime?	2005 (base: 819)
Account/password management policies	74%
Formal inappropriate use policy	71%
Employee education & awareness programs	67%
Monitor Internet connections	65%
Corporate security policy	62%
Require employees/contractors to sign acceptable use policies	59%
Conduct regular security audits	57%
Periodic risk assessments	55%
Employee/contractor background examinations	48%
New employee security training	46%
Periodic systems penetration testing	44%
Segregation of duties	43%
Employee monitoring	42%
Random security audits	40%
Mandatory internal reporting to management of misuse or abuse by employees & contractors	35%
Use of incident response team	34%
Include security in contract negotiations with vendors/suppliers	34%
Regular security communication from management	33%
Storage & review of e-mail or computer files	30%
Hired a CSO or CISO	24%
Government security clearances	22%
Use of "white hat" hackers	14%
None of the above/not sure	8%

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

Policies & Procedures in Place

Sixty-one percent (61%) of respondents say that policies and/or procedures in place at their organizations have supported or played a role in the deterrence, detection, termination or prosecution of an individual.

Have any security policies and procedures at your organization supported or played a role in the deterrence, detection, termination or prosecution of an individual?



2005 Results (base: 819)

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

In terms of deterrence, regular security communication from management and new employee security training tie as the most frequently cited deterrents to electronic crime (80%). The use of white hat hackers is the most frequently cited policy or procedure that played a role in detecting e-criminals, although this procedure is used at only 14% of respondents' organizations. Employee monitoring (37%) is most frequently credited as playing a role in the termination of an employee. Use of an incident response team is cited by 15% of roughly one-third of respondents utilizing this policy as having supported or played a role in the prosecution of an alleged criminal. The table below provides a complete breakout.

In your opinion, have any of the following security policies and procedures at your organization supported or played a role in the... a. Deterrence of a potential e-criminal?; b. Detection of an e-criminal?; c. Termination of an employee or contractor? d. Prosecution of an alleged criminal? (Check all that apply per row) (base: 819)

Disposition of policies/procedures (base: total responding with policy/procedure in place)	In Use	Deterrence	Detection	Termination	Prosecution	Don't know
Account/password management policies	74%	72%	27%	6%	4%	18%
Conduct regular security audits	57%	51%	51%	17%	7%	18%
Corporate security policy	62%	69%	20%	27%	10%	17%
Employee education & awareness programs	67%	78%	17%	7%	3%	16%
Employee monitoring	42%	57%	50%	37%	11%	12%
Employee/contractor background examinations	48%	60%	30%	16%	3%	24%
Formal inappropriate use policy	71%	70%	19%	32%	6%	13%
Government security clearances	22%	58%	20%	8%	4%	29%
Hired a CSO or CISO	24%	67%	38%	16%	13%	24%
Include security in contract negotiations with vendors/suppliers	34%	72%	17%	11%	5%	20%
Mandatory internal reporting to management of misuse or abuse by employees & contractors	35%	66%	39%	32%	10%	14%
Monitor Internet connections	65%	52%	56%	31%	6%	15%
New employee security training	46%	80%	9%	9%	3%	16%
Periodic risk assessments	55%	51%	43%	5%	2%	22%
Periodic systems penetration testing	44%	48%	50%	5%	2%	20%
Random security audits	40%	61%	52%	14%	5%	14%
Regular security communication from management	33%	80%	11%	2%	2%	16%
Require employees/contractors to sign acceptable use policies	59%	74%	14%	24%	7%	19%
Segregation of duties	43%	73%	28%	7%	3%	17%
Storage & review of e-mail or computer files	30%	56%	48%	34%	12%	18%
Use of "white hat" hackers	14%	46%	59%	3%	7%	15%
Use of incident response team	34%	42%	49%	22%	15%	19%

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 33.

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 an addendum beginning on 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 (one to two sentences) the single most effective security policy or practice in place at their organizations for stopping electronic crime, security and law enforcement executives responding provided the following responses:

Authentication, Passwords

- Access and identification controls at all network levels
- Access control and education are the most effective security policy to our organization.
- Access controls
- Access controls and intrusion detection
- Access controls not only to the facility, but also to the network—we have both password and biometric requirements for sign-on.
- Access controls, audits, perimeter defenses (IDS, firewall, etc.), and antivirus
- All access privileges are based upon a PKI-based identity credential issued through a sound enrollment process. ID-PKI WORKS but it is overlooked by many organizations because of a false assumption that it is overly difficult to deploy and manage.
- Authentication required accessing the Internet, and the blocking of Internet sites via a tool, plus, use of intrusion detection software
- Control of key passwords, checks and balances on employee roles—good engineering
- Control systems
- Desktop lockdown with removal of admin rights
- Encrypted administration traffic, non-standard port usage for communication, authentication for all communication to important systems
- Encryption
- Field employees use specialized VPN.
- Forced password changes
- High minimum deposit requirement
- Implemented password synchronization process to align password values on most major systems, improving ove all password efficiency and value
- Instituting a strong password policy, and timely audit reports from HR regarding employees, coming and going
- Log all transactions and lock down computers
- Log-on warnings
- Minimum password construction
- Network passwords and firewalls
- Network, log monitoring—this is an open environment.
- Our systems security configuration benchmarks and role-based access control
- Password and frequent changes of it
- Password expiration
- Password management—requirements of password complexity and the administration of passwords
- Password management procedure is the front line of defense in preventing unauthorized access.
- Password policies and a 'closed' network system help us prevent hackers from accessing our systems.
- Password policy
- Password reset requirements
- Passwords and disclosures
- Passwords, virus scans, firewall requirements for remote users
- Quarterly changes of access codes

- Refrain from opening e-mails that are unsolicited and ensure that passwords are created in a multi-character format
- Role-based access
- Role-based access control
- Security log consolidation
- Segregation of duties/authorizations
- Strict access control over offshore contractors limiting their use of systems and information stores
- Strict password policy length and change every 3 months
- Strong password management policy and a policy to leave no network appliance logged in while stepping away. Active virus protection software, firewall and IDS implementations and management, as well as diligent patch management support these actions.
- Strong password policy
- The use of strong passwords
- Two-factor (one time passwords) required for network access
- Verification, validation and need to know on a timely basis
- Verifying with real organization spoofed phishing identities
- VPN combined with strong password
- We use strong network access control lists to limit users access to network and systems.

Conduct Regular Security Audits, Periodic Risk Assessments/System Testing

- A formalized security review for all system implementations prior to rollout
- Active risk management program
- Annual/mid-year review
- Audit trail on mainframe users who have too much security access.
- Auditing, firewalls
- Close collaboration between physical and IT security personnel in addressing issues as identified. Strong support between both teams
- Combination of security policies and regular audits/assessments
- External audit and remediation
- I think that random security audits is probably the most effective security practice. This not only alerts to potential problems but existing 'problems' are often found too.
- Integrated, collaborative incident response and defense in depth
- Intrusion detection
- Intrusion detection and IPS
- Intrusion detection, unscheduled audits and training
- Intrusion prevention systems on network, regular scans for viruses and spyware, complex random passwords
- Intrusion prevention, firewall and desktop firewall, keeping systems regularly updated with the proper patches.
- Mandatory reporting of any inappropriate access or use of data systems, coupled with random security audits
- Monitoring and periodic assessments—external vigilance
- Ongoing internal post audits
- Penetration testing and audits
- Periodic checking of SMTP relay rejection
- Periodic network security audits to evaluate network vulnerabilities are a crucial step to maintaining our network security standards.
- Periodic security auditing
- Practice: outsourcing of monitoring of Internet services
- Probably the simple fact that we have a fairly secure building and supplement that with frequent security awareness communications
- Random security audits
- Regular audits of systems and logs
- Screening e-mail from outside and monitoring Internet and e-mail use within organization

- System monitoring
- System security settings, security administration and monitoring
- System surveillance
- The most effective practice my company uses for the prevention and detection of e-crime is the constant use of intrusion testing.
- Vigilance (2 mentions)
- Vigilance, communication, and policy
- Weekly vulnerability assessments with remediation timetables
- Weekly vulnerability scans of entire Internet IP Address range and detailed application security reviews
- Written policies and periodic audit policy

Written Inappropriate Use Policy

- Appropriate use policy HIPPA privacy training
- Computer and network use policy—many input vectors for malicious code and viruses are from mobile laptops. This policy helps control the behavior of the people using them.
- Good people who can recognize and respond to problems—several general policies infer prohibition of questionable practices.
- Inappropriate usage
- Inappropriate use of PC/network resources and facilities
- Inappropriate use of WWW and downloading files
- Our inappropriate use policy seems to have had an impact and awareness on employees and students.
- Segmentation of data, host and system policy
- Strong language and enforcement of acceptable use policies are in place and followed by all employees, contractors and customers.
- The Internet acceptable use policy is the most effective policy. The Internet allows many opportunities for malicious code to enter the network from unacceptable use by employees.
- Use policy and monitoring
- Written and user-signed policies
- Written policies and periodic audit policy
- Written policy
- Written policy disseminated to all employees.

Monitor Internet Connections, Firewall, Anti-virus, Patches

- Active directory security policy promulgation for SUS/WUS automatic updates and SAV virus signature updates
- Active monitoring of network connections and usage during non-business hours
- Active monitoring of network use, Internet activity and security logs from systems and firewalls 4 up-to-date virus protection that is manually reviewed on a daily basis
- Administrative policies are in place, with some network monitoring.
- Aggressive manual patch management and vulnerability scanning
- Anti-spyware, anti-virus
- Anti-virus software—almost all of our e-crimes in 2004 were virus related. Without it we'd be crippled. The machines, which did get infected, were out of date.
- Auditing, firewalls
- Aura that IT security monitors all
- Automated antivirus and anti-spyware update systems
- Automated anti-virus and automated patch management
- Automated content scanning combined with a user awareness campaign to combat phishing attacks
- Automated monitoring of transactions in customer accounts.
- Automated monitoring tools and employee awareness and accountability initiatives
- Automated systems for anti-virus and patch management
- Automated updates for anti-virus at the gateway, messaging server, file server and desktop

- Automated virus detection
- Automated virus scanning, automated patch management
- Automatically patching our desktop computers has contributed more to the security of our systems than just about anything.
- Be aware of your surroundings and report anything or anyone that is out of place.
- Because we are a small organization, mutual trust is one, but I know, that is pretty weak. We have all of the typical firewall and virus protection in place.
- Being a Police Department we do not have a large budget for security of our network. Virus scanning and spam blocking are the biggest issues.
- Best- of- breed combination of anti-virus, anti-spam and firewall protection on the perimeter, solid role based access to critical corporate data.
- Checkpoint firewall with smart defense allows strict port filtering and known attack detection.
- Constant continuous monitoring of anomalies
- Constant monitoring of network activity and continuous awareness training via notices of impending attacks by viruses and hackers
- Continually updated virus signatures, strong firewall and IDS/IPS system and continual update/monitoring
- Continued monitoring of all network systems
- Continuous patching
- Control environment, intrusion detection
- Current virus and spyware detection software, maintaining firewalls
- Currently have Internet blocking in place that prevents users from downloading dangerous file types except from pre -approved Web sites. Preventing most spyware/viruses from entering our network
- Currently, we monitor the bandwidth at the router to identify non-standard activity.
- Deployment of firewalls
- DMZ protection and authentication with RSA
- Education and monitoring
- Education and monitoring are the most effective practices, education as in awareness and deterrence
- Effective filtering of spam
- Effective firewall with immediate updates
- Effective network monitoring
- Effective use of technology and system security
- Electronic monitoring and making it very well known by all workers you are doing it and mean business!
- E-mail and Internet monitoring; updating PCs with latest OS updates within 1 day; anti-virus software; redundant firewalls and spam firewall.
- E-mail policy that alerts staff that the company owns all e-mail—business and personal and will access when necessary.
- Employees have limited access to the Internet. This controls the incidents of attacks coming from an infected system.
- Employees manually monitoring suspicious situations
- Employing firewall and intrusion detection equipment
- External network/e-mail/Web traffic monitoring and security awareness
- Firewall (5 mentions)
- Firewall and proxy server
- Firewall in place with password access to network
- Firewall is what the system has used in past, but policies have to be evaluated.
- Firewall policies
- Firewall, current anti-virus software, including incoming e-mail virus scanning
- Firewall, systems monitoring
- Firewalls and hardware to prevent outside illegal entry, password changes and system monitoring
- Firewalls and have hired full time I.T. person
- Firewalls and spam blockers
- Firewalls are in place.

- Firewalls at perimeter of internal network and traffic management at border routers
- Firewalls, antivirus software for machines, safe practices for employees.
- Firewalls, current virus files on desktop, user education
- Firewalls, preventing outside attacks
- Hardware firewalls and penetration testing
- Having a hardware firewall, and scanning the network with current up-to-date Malware programs
- Having a written security policy in place has made the most difference internally. Firewalls have been the most effective externally.
- Having an effective firewall.
- Having set polices and in place and reminding employees of these polices electronically every time they log in.
- Heavy spam filtering
- I believe the single most effective policy in place for stopping e-crime is the use of our anti-spam e-mail filter which blocks spoofing of e-mails in our organization.
- I write my own Perl script signatures that look for various attacks based on reports from various organizations. This has helped to detect insiders who purposely try to circumvent IA devices in place, as it doesn't follow the normal conventions.
- Implementing outbound ACLs on routers
- Increased network monitoring and remote notification of network admin of anomalies
- Information assurance scans 'white hat' done by IA staff worldwide
- Information systems monitoring of bandwidths
- Installing software updates
- Internet control access, antivirus automatic protection, user access control
- Internet monitoring and filtering
- IT security systems detecting ad ware, spyware, viruses
- Knowledge Internet and e-mail monitoring is the biggest deterrent and helps in the amount of time needed for detection for outside attacks
- Manual checks back-up automated capabilities to move money out of the company.
- Monitor usage
- Monitoring (3 mentions)
- Monitoring (even though we don't do it)
- Monitoring all computer users
- Monitoring all server log files to check for unauthorized activity. Ethernet sniffs on a semi regular basis looking for out- of-place traffic. Would love to do more; however, management is not of the mindset that this is a real issue and as a result 'security' is still thought of as something we in IT 'play' with.
- Monitoring and investigations
- Monitoring and periodic assessments—external vigilance
- Monitoring and policy
- Monitoring and removing access from systems that are not being used
- Monitoring Internet usage and blocking access to questioned Web sites, maintenance of the firewall
- Monitoring of activity and follow through on results.
- Monitoring of network/internet access.
- Monitoring of our networks—utilization and pattern studies along with a closed network are effective tools
- Monitoring of personnel computer usage and Internet
- Monitoring of system network from both an internal look and external view
- Monitoring system networks
- Monitoring transaction activity
- Monitoring use
- Most effective is eyeballs over the shoulder
- Multilayered protection with firewalls, proxies and antivirus solutions on mail servers, data servers and desktops, also installed and implemented Airfortress which encrypts all wireless data transmission
- Network antivirus and firewall
- Network filtering and computer/network monitoring

- Network monitoring
- Network- based intrusion detection system
- Our firewall, which restricts access to authorized Web sites
- Our minimum network security standards (mandating patching, firewalls, and anti-virus software) seem to be working to lower the numbers of easily compromised machines.
- Passwords, virus scans, firewall requirements for remote users
- Patch management AV/Spy update firewall checks
- Paying attention (monitoring, log review, staying awake, etc.)
- Perimeter screening and traffic monitoring - this includes egress filtering, layered virus scanning using multiple vendors on all types of traffic likely to carry a virus, log review, and strategically placed intrusion detection and prevention devices.
- Physical security and separation of critical systems
- Proactive IDS systems internal and at the perimeter
- Proper firewall setup and monitoring
- Proxy services to inhibit pop mail receipt on our WAN/LAN and in appropriate site denial
- Prudent use of hardware and software monitoring
- Random screening or monitoring of e-mail system and network systems
- Regular scrutiny of firewall and IDS logs to prevent abuse/intrusion/attacks
- Restrictive firewall rule sets—like a brick wall these things shield us from the least and the worst of threats day in and day out with only their setup and maintenance cost.
- Screening customers up front prior to allowing them on the network, and then, constant monitoring of the network
- Security awareness program firewall, IDS, anti-spam and antivirus enterprise -wide solutions
- Small, private network with strong perimeter protection, keep OS up to date, continuous antivirus, anti-spam, and e-mail encryption for sensitive material. Also, we do not use factory port defaults on our servers; deny everything, allow by exception.
- Software detection and blocking
- Starting with a default deny policy for everything and only allowing access to things that have a business need, i.e. no IM or Web mail access is allowed at work.
- Strict ACLs, along with instant patching
- Stringent control of desktops and limiting the ability of workstation users to perform inappropriate actions, such as using non-licensed software, introducing viruses or worms, or accessing confidential corporate data
- Strong firewall, e-mail filtering, spyware removal
- Strong network access policies and continuously updated firewalls and virus scanning technology
- Strong password management policy and a policy to leave no network appliance logged in while stepping away. Active virus protection software, firewall and IDS implementations and management, as well as diligent patch management support these actions.
- System security settings, security administration and monitoring
- Text only e-mails consent from receiver first for attachments before sending. All senders must be in address book. No more Outlook, or Outlook Express
- The AV infrastructure we have put in place
- The firewalls and frequent virus definition updates
- The monitoring of system and network usage has been effective in stopping and detecting misuse of the system and in stopping e-crime.
- The most effective practice is a secure firewall and vigilance in monitoring our network.
- The only security policies in place at this time are the firewalls and spam blockers. I don't know that either of these is effective at all.
- The requirement for base-line security protections wherever there is a significant exposure (ISP connections, etc.)
- The use of proxy and firewalling of contractors
- There is no single most important, it takes a battery of tools and practices that include, anti-virus, spyware, anti-spam, firewall, and network security monitoring tools.
- This company has implemented ISO 17799 at all data centers and corporate headquarters Through this implementation, the company has developed a defense in depth, multi-layered security architecture to provide the organization and customers with the confidentiality, integrity, and availability of their assets as required by the corporate security policy. This company will practice the policies of least privilege and need-

to-know throughout the company.

- URL blocking and policy
- Use and maintenance of firewalls keeping outsiders out
- Use Macintosh computers behind their own firewall and a firewall/router on our networks.
- Use of a written security policy and network monitoring
- Use of corporate firewalls
- Use of firewalls; encryption of highly sensitive information
- Use of Internet access monitoring and keystroke logging to deter and detect abuse
- Use of network firewall that was upgraded in 2004
- Use of open source software
- Using a firewall and Web filtering that integrates AD with the firewall
- Using a Web sense server to filter out and control where people can go in terms of sites
- Virus blocker and automatic patch management
- Virus checking
- Virus detection regular automatic updating
- Virus software
- Virus-spyware protection software
- We have several, our automated virus protection has been very successful but we also have a highly developed computer forensics program, which has paid large dividends during the investigative phase.
- Web and e-mail filtering has provided a most effective security practice that has freed us to look for other security problems. Our written employee policy is also a good deterrent.
- Web site DMZ protections
- Web traffic monitor

Employee Monitoring

- A layered approach to infrastructure protection and diligent event/employee activity logging and monitoring
- Accountability by managers and supervisors to monitor their departments, coupled with a least-rights privilege model and random audits
- Briefing/monitoring of employee actions
- Close monitor of terminating users
- Computer technicians are very knowledgeable and competent. They are vigilant about unauthorized activities on the network.
- Having policies in place that outline acceptable use and informing employees that their use of the system may be monitored.
- Limit access to trusted employees
- Limited access to secure information
- Limited physical and online access to systems and networks, based upon segregation of duties
- Limiting downloads
- Limits on Internet connectivity (required audits, monitoring, etc.)
- Limits on Web sites visited and protection of e-mail attachments
- Routinely making employees aware they are being monitored.
- The threat of individual ability to monitor all actions on the PC
- Mandatory reporting of any inappropriate access or use of data systems, coupled with random security audits
- Information security policy to allow investigations and monitoring of employee electronic activities
- Policy regarding monitoring and that we reserve the right to monitor and will monitor.
- Stringent control of desktops and limiting the ability of workstation users to perform inappropriate actions, such as using non-licensed software, introducing viruses or worms, or accessing confidential corporate data.

Corporate Security Policy

- Policy regarding monitoring and that we reserve the right to monitor and will monitor.
- A good policy in which the user signs off

- Acceptable use
- Acceptable use of e-mail and Web access
- Acceptable use policy (5 mentions)
- Acceptable use policy because it delineates rights and obligations of the employee as well as the company.
- Access to bank and customer information must only be granted to employees on a business need-to-know basis. All servers, workstations, and other network devices must be configured to meet or exceed the bank's minimum security requirements' for that platform and/or system, including the installation and use of UBOC standard anti-virus software.
- Code of conduct
- Computer use policy
- Conditions of use policy
- Consistent application of the existing policies, including disciplinary steps
- Corporate code of business conduct policy and acceptance
- Corporate credo
- Development of policies
- Direct and solid policy relating to use
- Due diligence in all matters
- Information security policy to allow investigations and monitoring of employee electronic activities
- Information security program policy
- Linking physical building access to automated security access. They used to be 2 separate processes, now they are one, monitored by HR.
- Mandatory security policy acceptance for all employees and any contacted work, including the contractor's sub-contractors. Penalties are enforced.
- Nervous network administrators
- Notifying the faculty, staff and students that monitoring does occur and issue bulletins about the detections
- Our acceptable use policy reminders appear to have an interesting effect. They jar the memory of employees who may have observed something and then feel inclined to report it.
- Our electronic communications policy, it is pretty comprehensive.
- Our enterprise protection policy outlines the necessary security and acceptable use of both physical and intellectual property.
- Our Internet and systems usage policy is the most effective.
- Partition disk, to expose to the Internet only a portion of the hard disk—generally, all the important document are kept on a computer that is not connected to the Internet or to a network
- Perimeter defense practices are good.
- Policy, communication and audits
- Privacy- security incident reporting policy—you can't manage what you can't measure, so it is critical to capture all 'suspected' security incidents, no matter how small or insignificant. Only by capturing all data and reporting it back to all members of the workforce (not just employees), can you start to change corporate culture and individual behavior.
- Segregation of duties
- The firm's technology security policy which serves as the foundation by which periodic compliance assessments are performed by both IT security analysts and internal auditors
- The most effective policy we have in place is our overall enterprise security policy, which summarizes all aspects of security control within our environment.
- The most effective policy we have is our Internet and e-mail usage guidelines. It was developed by IT and approved by management and our lawyers.
- Writing incident reports for every action employees do that violates organization policy and the physical removal of the system
- You are being electronically monitored. Please act accordingly.
- Practice: outsourcing of monitoring of Internet services
- Strong language and enforcement of acceptable use policies are in place and followed by all employees, contractors and customers.
- Starting with a default deny policy for everything and only allowing access to things that have a business need, i.e. no IM or Web mail access is allowed at work.

- This company has implemented ISO 17799 at all data centers and corporate headquarters. Through this implementation, the company has developed a defense in depth, multi-layered security architecture to provide the organization and customers with the confidentiality, integrity, and availability of their assets as required by the corporate security policy. This company will practice the policies of least privilege and need-to-know throughout the company.
- URL blocking and policy
- Web and e-mail filtering has provided a most effective security practice that has freed us to look for other security problems. Our written employee policy is also a good deterrent.
- Combination of security policies and regular audits/assessments
- Having a written security policy in place has made the most difference internally. Firewalls have been the most effective externally.
- Have a written security policy in place and train employees in its application.

Employee Education & Awareness Programs, New Employee Security

- Advising all employees of their responsibility for protecting data and guaranteeing fast action when a breach occurs.
- Aggressive employee training and awareness reinforcement on policies and prevention of compromises
- All employees will receive training on IT security policies. Computer users are responsible and accountable for all computer use, data and files associated with their account.
- Annual security awareness training
- Awareness and education
- Awareness and system tools
- Awareness of what is happening to others similar to ourselves—we are a small business.
- Awareness program about viruses, password policies, threats
- Awareness training
- Awareness training for employees
- Awareness, automated detection programs
- Awareness, education and mindset - security is not a device or a policy. It is an attitude.
- Combined network monitoring tools and AV notification systems are used to keep the support services group informed and prepared to address problems as they appear.
- Communication to the user
- Comprehensive employee security awareness programs, including ongoing training—Programs are backed and endorsed by senior management.
- Continuous user education and awareness
- Customer education
- Educated and trained staff
- Education
- Education and monitoring
- Education and monitoring are the most effective practices, education as in awareness and deterrence
- Education and reminder at a high profile level concerning security for the organization and protection against harm to corporate resources critical to the survival of the firm
- Education and training of system users
- Education is the most effective security policy.
- Education of personnel through internal training program
- Education of users
- Employee awareness
- Employee awareness training (3 mentions)
- Employee education and good firewall policies
- Employee education on current scams and social engineering practices and ways to detect and avoid
- Employee education programs staring with new hires and also through periodic department level outreach
- Employee monitoring
- Employee monitoring and central system monitoring
- Employee training and testing

- Employee training.
- External network/e-mail/Web traffic monitoring and security awareness
- Firewalls, current virus files on desktop, user education
- Good understanding of risks by a large number of employees
- Have a written security policy in place and train employees in its application.
- Hiring and retaining people we trust, everything else is secondary, IMHO.
- Hiring good people and training them well
- Informal, but consistent, reminders to staff to update and maintain their firewalls, anti-virus software, and anti-spyware software
- Keeping all advised as to potential threats and requires watchfulness before accessing potentially harmful sites/links
- Knowledge and training
- Knowledge Internet and e-mail monitoring is the biggest deterrent and helps in the amount of time needed for detection for outside attacks
- Laptop/desktop policies and education
- Making people aware of the risks and potential damage
- Need to have policy in place and communicated to employees—no effective policy
- Need-to-know information policy
- Ongoing training and IT upgrades to help reduce e-crime
- Online awareness training is required yearly.
- Our security awareness policy, practices and program
- Periodic security awareness and education bulletins via e-mail to all employees and contractors
- Reinforcing employee awareness through periodic communications and publicizing the successes of our current detection systems and processes
- Security awareness and training is required for all employees on a regular basis.
- Security awareness program firewall, IDS, anti-spam and antivirus enterprise -wide solutions
- Security awareness training (2 mentions)
- Security awareness.
- Security charter endorsed by management, new hire orientation by security staff
- Security education
- Security education and awareness training from day one until termination—strong policies that are easily enforceable
- Security education and awareness...policies are good, tools are great, but just like with the fight against terrorists, you need the users to know what is suspicious activity and to report it!
- Security training and knowledge of monitoring by employees
- The annual updates of policies and procedures w/signatures stating you are aware of those procedures.
- Training and awareness
- Training and explanation of the policy
- Training is the most important.
- Training personnel on expected conduct and consequences for violations
- Unknown—investigating internal intrusions not my core function
- Unquestionably the greatest tool is training and awareness of the employees and users. They are a highly effective tool for identifying weaknesses and exposures as well as counterproductive behavior.
- Use policy and monitoring
- User awareness of ongoing audit program and expectations of appropriate use
- User awareness training
- User awareness training, strong authentication policy
- User education
- User- authenticated network access
- We educate our employees in appropriate behavior, monitor employees on a casual basis, as we come in contact with their equipment, and build a spirit of cooperation and loyalty to the organization.

Require Employees/contractors to Sign Acceptable Use Policies

- All inappropriate use policies
- Deterrence by signing appropriate use policy and monitoring of network communications for compliance
- Internet, PC and e-mail acceptable use policies.
- Non-disclosure agreements with employees and contractors, threat of suit
- Users must sign rules of behavior. Mandatory virus software install and maintenance
- Vetting of new employees, vendors, contractors
- Written and user-signed policies

Employee and/or Contractor Background Examinations, Government Security Clearances

- A better workforce—character does matter.
- All employees must go through an extensive background check.
- Background checks have turned up a few people that had jobs rescinded because of previous crimes. Proper firewall and IDS management has kept us pretty safe from the majority of e-crime.
- Background investigations and physical security
- Background/hiring good people
- Employee hiring requirements (background investigations, etc.)
- The government clearance processes acts as both deterrence in the possibility of losing it and filter in terms of the background investigation.
- We are a law enforcement agency. Our system has not been penetrated to my knowledge. We investigate state agencies that have experienced such security intrusions.
- We are a Law Enforcement Agency. We investigate and file charges on individuals within and from outside the organization who have violated state statues.
- Screening customers up front prior to allowing them on the network, and then, constant monitoring of the network

Corporate Security

- All employees work in teams.
- An effective CISO
- Change control and validation
- Checking by in-house computer security expert
- Creation of an effective Incident response team
- Establishing an E-crime work force (2) that is focused on fraud, etc.
- Good people who can recognize and respond to problems—several general policies infer prohibition of questionable practices.
- Having a dedicated security team to monitor both internal and external threats to the company
- Having a security department in place with proper support, assets and backing
- In my organization, the prosecution factor is paramount. I deal 100% with communication frauds from outside the organization.
- Information protection unit that is very proactive in monitoring network and Internet use.
- IT administrator constant monitoring and responding to complaints immediately by employees of attempted intrusions, anti-virus controls and spyware monitors, auto scan and auto virus updates, etc.
- Management over watch
- Management support of IS policies
- My unit is responsible for enforcing the computer laws within our jurisdiction.
- Network security forensics lab using Encase platform
- Our system runs on a network, and is monitored by our IT department.
- Physical security department has little interaction with IT security initiatives.
- Probably the simple fact that we have a fairly secure building and supplement that with frequent security awareness communication
- Relationships with local law enforcement
- Security is in the design and updating of the systems.

- We have a Fraud Center that is staffed 24X7 that monitors our network. We are in the process of installing applications that will monitor employee PC and Internet use.
- We try to stay one step ahead of the tidal wave of new attack vectors, whether in blocking access to phishing/malicious sites or removing executable content from e-mails. Well-trained IT staff is our best defense.

No Major System in Place

- Common sense
- I don't believe that we have an effective policy for stopping e-crime specifically. Our desktop firewall policy has helped the most with virus and worm infections.
- I would be difficult to determine how to measure the effectiveness of a policy.
- Need to have policy in place and communicated to employees—no effective policy
- No direct connection between internal data and Internet
- No expectation of privacy when using company information systems
- No expectation of privacy, monitoring of e-mail and Internet activities
- No local accounts on desktops or laptops, and users have very limited rights/can't install any software.
- No one policy or practice but rather their collection
- No single most effective policy or practice exists, rather a synergistic combination of policies and procedures.
- No 'single' solution is apparent, must use a variety of tactics.
- None are in place to date.
- None in place—we prosecute e-crime but only a tiny amount.
- Pending
- Small company using as much available technology as possible
- Small employee force with open communication
- We are a small company with security policies in place and a good knowledge of every employee on a personal basis.
- We are a small, highly competent firm with selected personnel who have been involved with our companies over 25 years. We are all senior people, with ownership stakes.
- We have no real practice and rely on our policy.
- We have none. Our current Director of IS does not see the need for any security measures. I am hoping to have him fired in the next month so that we can implement some practices that I would like to do, that he always denies implementation of. He is useless, and a major cause for concern in our city of 60,000.
- We talk to each other

Corporate Ethics

- Our 'code of ethics' policy seems to be the most effective deterrent system in place. We have weekly reminders sent to all employees about the possibility of attacks, dissemination of information to others and about inappropriate use of the company's hardware.
- Our most effective practice is when personnel and systems work together as one.

Include Security in Contract with Vendors/suppliers

- Mandatory security policy acceptance for all employees and any contacted work, including the contractor's sub-contractors. Penalties are enforced.
- Requirement of every employee and contractor to sign security policy and provide education Violation can and does include possible termination.

Termination of Employment, Legal Action

- Expectation of termination
- Firing employees for e-crime
- If a person violates the policy they my be fired
- Requirement of every employee and contractor to sign security policy and provide education Violation can and does include possible termination.
- Termination and reputation consequences—would never be allowed to work in the insurance industry again. Have to get my CDL

- Termination of employment
- The actual removal of an employee for abusing Internet connectivity, having it stated in policy that termination of employment is possible is far less of an impact than when it actually happens.
- The employment/annually renewed signoff on business use of technology and acknowledgement of our ability to prosecute for misuse of systems
- You may be terminated if...
- Zero tolerance for anyone misusing the computers or company networks.

Not Applicable

- I'm not in the IT sections, so I don't know.
- N/A (9 mentions)
- Security policies are not a part of my job.
- We're law enforcement— this question doesn't seem to be directly applicable to what we're designed to accomplish.

None, Don't Know

- Don't know (12 mentions)
- No comment
- None (five mentions)
- Not clear.
- Not sure (two mentions)
- Since I am not involved in our internal network security, I'm not really sure. We have a complete staff of IT security employees.
- This is a question for the CEO or IT.

Verbatim Comments—Electronic Crime Most Proud of Preventing or Solving

When asked to briefly describe (one to two 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:

Prevention of Hackers

- A hacker dropped a back door on one of our servers, and then proceeded to share a foreign version of Photoshop from our computer. It was noticed within a day (even though the files were hidden), removed and the security hole was fixed.
- A hacking from an outside that was detected and prosecuted (Not in 2004)
- All hacker attempts to penetrate our networks as indicated by our Cisco IDS.
- An outside hacker was able to perform a denial of service but our IT security was able to track the hacker's e-mail and intercept the hackers e-mail with incriminating statements to other hackers. This is an active case at (name of organization deleted).
- Attempts to plant logic bombs and password sniffers by foreign hackers (originating in China and Eastern Europe) were detected and prevented.
- By setting up an identical honeypot Web site we were able to keep a hacker busy trying to deface our Web site while I tracked him back across the Web and identified his machine location and machine name, but when I went to police and we were able to identify the hacker the police deemed the incident did not cause and 'real' damage so it was dropped without any further attempt to punish the hacker. Police don't understand the cyber world and as a result we don't even report anymore, not worth our time to do all the work and have it dropped due to no understanding of the situation.
- China company tried to break into the network for sensitive data
- Contractor accessing our network and spreading blaster
- Detected remote scan of perimeter, traced originating IP back to a local company. Coordinated investigation led to an employee of that company attempting to hack into other companies systems. Local company took corrective action but did not provide details. Attacks stopped.
- Detection of a contractor PC with unauthorized configuration—immediate action was taken with no adverse effects to the agency.

- External penetration and resulting lockdown
- Hacker attempt at a DDOS attack
- Hacker attempting to break into systems
- Hacker/Intruder
- Hackers into a Web site
- Hackers with stolen customer credentials have been prevented from removing money.
- Hacking from foreign entities
- Hacking through use of guest accounts
- Handled incidents where DOD Solaris print servers were hacked.
- Identifying who was posting confidential information on the Internet.
- Identifying, contacting and confronting a college student's remote attempt to compromise perimeter security (at 2am on a Saturday morning) within 8 minutes of the attempted compromise by a remote CERT member who was sleeping when contacted by our NOC staff.
- Mass spyware and virus distributions
- Nailed the last defacer to attempt illegal access—the little schmuck wasn't prosecuted, however: worked a deal with the San Francisco DA's office.
- Solving—unauthorized access (hacking) into employee bank records
- Stopped hackers from using our Web server as a file server
- Student attempted to alter school records
- Unauthorized wireless access points placed on the internal network.
- Various scams, sources primarily Romania, Nigeria, and 1600 Pennsylvania
- We developed filters to thwart DDoS attacks.

Intrusion Prevention

- Adverse party in legal matter attempted to break into network and was stopped by firewall and security on system; in addition, from this attempt we were able to cloak network in additional security against future intrusions
- Apparent attack on our client servers by an external entity—filtered out attack packets for 48 hrs. Attacker has not tried again.
- Breach of system allowing unauthorized insider complete physical and electronic access to the entire system—the perpetrator was caught and systems have since been hardened to guard against a repeat.
- Contractor reading another person's e-mail without permission
- Defacement of our Web site—we tracked down the defacer, arrested him, prosecuted him and convicted him. He is currently serving 3 years in Federal Prison.
- DOS attacks and phishing attempts
- Due to our network policies we have prevented any virus from affecting our network in the year 2004 and have prevented spyware from becoming a problem by managing a content control system.
- Effective spam management and potential phishing attacks via e-mail.
- Electronic mail spyware
- Foreign programs on company computers
- Identification and correction of incorrectly configured network equipment
- Intrusion detection (2 mentions)
- Moon light maze
- Multi-tiered security environment has effectively deterred outside intrusions into our network.
- Outside intrusion and unauthorized access to sensitive data.
- Patch management
- Phishing (3 mentions)
- Phishing attempts against employees
- Phishing on our secretary
- Phishing shut down by the e-mail server.
- Pilfering of customer data
- Purchasing software that monitors attempts to install cookies or spyware

- Put in place ongoing vulnerability management system
- Shutdown of student lab computers and identification of outsider, when used to generate spam
- Slammers
- Spam and mal-ware
- Spam and spyware.
- Spam forwarding was stopped cold and has been prevented since.
- Spoofing of manager e-mail account creating communications between manager and employee
- Spyware
- Spyware— lots of it and getting rid of it
- Stopped a Web site' from possible phishing event
- System and network penetration from external networks
- Taiwan based spammer was attempting to relay spam through our SMTP server. Found him and rejected him. Laughed as he tried repeated attempts to re-establish SMTP AUTH attack.
- Trojan attack by a foreign country where we were able to find ways to identify and remove various Trojans that were installed
- Try of breaking our billing service
- Unauthorized access to internal computer systems
- Unauthorized access to need to know data
- Unauthorized access to PHI
- We did a review of wireless access points and found a number of rogue sites had emerged which impacted the University's Infrastructure plans for wireless access points. An immediate cease and desist notice was issued to the operators of those rogue access points.
- We have created a truly secure boundary around our internal 'namespace' or grid, where, important information is shared by our telecommuting team members around the world.
- We prevented any serious problems with W32.Blaster by patching our systems within two weeks of the initial security bulletin.
- We were able to thwart attacks on our network through the usage of 'tiered' firewalls
- Web site attacks through locking down the web server

Prevention of Virus Attacks

- 100% virus and worm free on all 'managed' systems
- An infected contractor PC spreading a virus was caught in the first hour of being on line.
- Automated virus and latest MS patch management processes have eliminated most of our issues internally.
- Avoid disruption from major Internet virus outbreaks in the last 3 years.
- Because of our IDS running both internally and externally we have thwarted numerous viruses, worms, and Trojans by immediately shutting the switch port down rendering the infected PC harmless until it is cleaned.
- Blocking viruses is a win for us.
- Blocking worm attacks through use of effective anti-virus products and practices
- By being diligent about updating anti-virus software, installing and updating spybot removal software and keeping patch levels as up to date as possible I feel that I have prevented many additional attacks from happening, but it's just intuition as I have no specific data to back up my gut feeling. I guess the fact that no serious problems have come up is something.
- Called in and reported to the Information Security Systems Officer (ISSO) about a rapidly transmitting virus which ravaged the LAN/WAN network for 48 hours. It had come in via an e-mail attachment from an outsider.
- Detecting a virus from a system in Mexico and stopping it, with the assistance of the I.T. person in Mexico.
- Discovered a Nimda infection a couple of years ago, isolated, and contained.
- Disruption from viruses over the past 12 months
- DNS DoS caught at the beginning of the attack, quick server configuration change prevented the attack.
- Dramatic reduction in virus attacks
- Every major virus/worm incident— these have a HUGE impact.
- Firewall
- Firewalling of latest Windows exploits
- Four team members removed a worm from the network in 4 hours partially by being lucky about patch management the rest through remote scripting to detect and remove any instances. Also located the initial

source (phone vendor laptop) in less than 45 minutes from the first infection.

- Getting the network functioning after being hit with Slammer
- Halted a phishing attack in 2 hours
- Have a good security patch management practice in place.
- Have not had an attempt except for phishing and virus.
- I did find a nasty worm that was running through our system after watching my idiot boss look for the workstation that was causing it for 2 days. Yes, we were down that whole time. He would not take anyone else's advice and perform a packet capture to try and isolate the system. I stayed late on the 2nd day after he had left, yes, with the system still down, and found the workstation and removed it from the network. By using the word down, I am implying that we had no Internet access, no e-mail for those 2 days. He's a loose cannon around here and has no concept of security or anything else IT related. His latest kick was to buy a copy of Windows XP server...good luck!
- Installation of e-mail quarantine, blacklist and white list folders and disposition processing system
- Installation of firewalls to prevent spyware and Trojans
- Just preventing Trojan horses and other threats that I see are hitting our computers. Nothing too exciting but very important for our information security and avoiding becoming part of a DDOS
- Keeping the Worm(s) Blaster and Sasser from corrupting our network and our clients' networks.
- Lots of phishing scams and Liberian scams but no problems
- Maintaining our servers in a current state of patch/update level, we managed to prevent infection by SQL Slammer, and Web defacement attempts.
- Mass spyware and virus distributions
- Most of our attacks have been attempts to invade our systems with viruses, worms, Trojans, etc.
- Most viruses cannot penetrate the firewall.
- Network wide virus protection
- Nimda virus
- Numerous stops at firewall
- Our main threat is virus attack. Our anti-virus system seems to have thwarted all recent attacks.
- Our system has been lucky with stopping outside viruses.
- Providing network security through Web filtering, e-mail SPAM/SPIM and antivirus and firewalling at little to no cost to the taxpayer
- Rapid identification and mitigation of a previously unknown worm
- Sasser worm outbreak
- Several incidences of viruses introduced by outside vendors that was detected quickly and limited damage or shut down of systems.
- The use of multilayer and multiproduct anti-virus and anti-spam solutions has prevented us from having serious outages or incidents.
- Very large number of viruses caught by firewalls, avoiding downtime, which has affected several competitors more severely than ourselves
- Vigilance has been key to identifying and quickly addressing a number of virus and worm activities.
- Virus proliferation
- Virus propagation through an automated patch management and anti-viral update systems
- Virus spreading on the network
- Viruses and worms have much less impact than what we read in the newspaper.
- We are most proud of our ability to stop most viruses and malicious code from entering our network, and our ability to respond quickly and effectively in resolving intrusions that do occur.
- We believe that the firm has avoided attempted crime, intrusions, and compromised systems or networks from viruses, spyware, or phishing that originates with unsolicited commercial e-mail (spam). A combination of patching, anti-virus, spyware detection, and user education has enabled us to avoid these attacks.
- We have been very successful in deterring worms and other virus attacks from being acquired. Also, our training policy has served to guide employees in how not to spread suspect e-mails received.
- We have had only one virus get into our network over the past three years.
- We thwart numerous attacks on our Internet exposed systems by diligent patch management and very restrictive firewall policies.

Prevention of Denial of Service Attacks

- Denial of service
- Denial of service attack and the blocking of Trojans and viruses
- Denial of service attack by outsider
- We recently blocked a worm that was released on our network by a user connecting unauthorized personal equipment to the network. We were able to contain the worm and prevent a large-scale denial of service attack.
- Routine DDOS attacks are automatically blocked by our intrusion prevention system

Insider Threats

- Contractor's use of a penetration tool on our internal network, looking for vulnerabilities—walked out, the same day
- Detection/prosecution of an individual (later discovered to be a former employee) who was electronically harassing/threatening a present employees. The vast majority of E- commerce fraud attempts on our Web sites
- Disgruntled employee was planning on deleting any files they had permission to delete. All files are backed up and took extra precautions concerning that employee's access rights, etc.
- Employee in the IT department using company servers to host a Web site for playing games
- Employee providing sensitive information for a profit
- Detected outside source(s) attempting to access sensitive government procurement and schedules information— in collusion with former employee.
- Employee running Seti@home program on 100+ computers in organization
- Employees corrupted system responsible for operation of equipment at large facility.
- Fired disgruntled worker that was bragging to co -workers of pending IT sabotage; while the firing was in process, the employee's access to systems and building were shut off and deleted and building security packed his personal belongings and escorted employee to outside of building.
- Former employee attempted to ftp 'his' files after termination, through dial up RAS server. Was married to an employee and used their login access. Access logs were his downfall.
- Former IS security officer's misuse of corporate computing resources
- Found an employee selling company computer equipment on e-bay
- I contributed toward securing our network by identifying and reporting breaches in security by a system administrator who was abusing his authority to access and read confidential information.
- I don't know if I'd say I was proud of this, but we termed a guy based upon his prolific smut distribution. He sued for a wrongful termination, because he had a huge bonus coming to him if he was still employed on X date. We successfully defended the case. This helped prove that the company was willing to go to great lengths to take the moral high ground. It also saved us some big money, and taught one guy a very expensive lesson.
- Identifying an employee in the act of abusing the Internet at a remote site. They were caught and confronted while the activity was occurring.
- Inappropriate access to customer wage information
- Inappropriate handling of critical/sensitive information by insiders
- Inappropriate use of computing resources
- Inappropriate use of WWW and downloading files
- Inside user(s) accessing files they are not supposed to. Stopping viruses and Adware from disrupting the network.
- Insider social engineering colleague's user names and password to use their account for inappropriate activity
- Intentional deletion of network files restored from backup and actions taken to prevent recurrence
- Internal unintentional misuse
- Major fraud (pled to $55 mil) against company by insider
- Only 1 minor virus infection in over a year, and it was caused by an insider bringing in a laptop.
- Rapid detection of and prevention of harm by an attacker hired by a misbehaving management employee to gather information provision of solid supporting evidence for legal action
- Stopped employee data theft by monitoring cell phone records (e.g. employee calling competitor on cell phone)
- Termination of a state employee, who was using his state PC to run a private business
- The inability of employees to access inappropriate materials in the workplace

- Transfer of classified material to non-DoD (uncleared) personnel
- Was able to detect an ex employee who was using Client logins to gain access to production systems. We were able to 'plant' data that would download to the ex employee's computer system and then local law enforcement raided and seized all equipment and legally prosecuted the individual.
- We are pretty boring here. Most infractions are about employees wasting company time.
- We had a mass deletion of data (30,000+ files/folders) by an unknown user. I put procedures in place to prevent the accidental deletion of data by authorized users, and to track unsuccessful attempts to delete.
- With minimal tools and support, our network team detected and removed access to several unauthorized WAPs, which were also unprotected, installed by a tech enthusiast employee.

Efforts with Law Enforcement

- A child pornography investigation of a DoD employee; employment terminated, and upheld via MSPB hearings; criminal prosecution pending
- A yearlong investigation of a case by our incident response team (along with law enforcement) resulting in apprehension of intruders
- Arrest of electronic crime suspects
- As a detective specializing in computer forensics, I was able to detect and charge a state IT worker who was remotely accessing a server acquiring child pornography from the Internet.
- Assisting the U.S. marshals capture one the 15 most wanted criminals by using our ability to electronically locate him.
- Attempted extortion, perpetrator caught
- Being the first in the agency to address the threat and seriousness of 'malware'. Detecting and proving to management that the answer to the problem is not adding more IA devices as they can be beaten—the answer is to severely punish the offender.
- Child exploitation
- Child exploitation case that was prosecuted and predator off streets
- Computer theft (equipments + accessories), computer abuse (web surfing)
- Conviction of hacker that caused denial of service attack that impacted financial markets
- Defacement of our Web site—we tracked down the defacer, arrested him, prosecuted him and convicted him. He is currently serving 3 years in Federal Prison.
- Detection and prosecution of a now former trusted information systems management employee for embezzlement of government funds
- Detection of an attempted brute force attack on our public facing File Transfer Protocol (FTP) server— attack was detected by our newly installed Security Information Management (SIM) system. The FTP server hardening/ base lining process stopped the attack cold and provided valuable forensic evidence to confirm that the attack did fail and evidence for law enforcement to use for their investigation. Initial law enforcement investigation has lead to the discovery of compromised systems on different networks and the involvement of FBI and Secret Service.
- Detection/prosecution of an individual (later discovered to be a former employee) who was electronically harassing/ threatening a present employee.
- Discovered and prosecuted a group using DOT systems for private ventures.
- Federal court civil litigation regarding theft of trade secrets value in tens of millions
- Forensic examinations of child pornography cases
- I have been involved in numerous child pornography and traveling cases where defendants have been sentenced to long prison terms.
- I helped to prosecute an individual in a civil trial who was accusing someone else of the offense they were actually responsible for against the one they were accusing.
- I successfully prosecuted a local professor for child luring. He 'met' a 13-year old girl online and appeared to be grooming her for a meeting when he was discovered and subsequently arrested in a sting operation.
- I was the first investigator in US history to prosecute and arrest an individual for 'Spimming' spam via instant messaging. This came from an on-line extortion case of mine.
- I work organized crime cases. The current case (mortgage fraud) case brings me the most pride.
- Implementing an anti-fraud program in the online business and the prosecution of people where the losses are worth it
- Instances of child-porn use
- Investigations, such as intellectual property, that is unique to each district within the secret service

- Numerous ones, I am one of the forensic PC examiners for the county, catching and convicting of kiddies porn distributors.
- One of the computer persons and I were instrumental in securing the appropriate evidence which led to the investigation and prosecution of a child pornographer. He is serving time in a federal facility.
- Organized criminal activity with the assistance of an insider as well as the detection and prosecution of the purveyors of child pornography
- Our computer forensic capabilities have enabled us to very effective in investigating a broad variety of cases (fraud, employee misconduct, competitive intelligence probes, trade secret thief, etc). It has also enabled us to determine when a crime is not real. We have had several cases, which due to the action of Trojans and spyware looked like an intrusion by a particular organization or employee but were in fact the result of unsafe computer practices or just bad luck.
- Porn
- Potential foreign espionage
- Prevented potential data leak within US government network
- Preventing the sale of prohibited nuclear US power plant equipment to a middle-eastern country
- Supporting the secret service with operation firewall
- The apprehension of suspects involved in child pornography
- Theft of intellectual property
- Theft of proprietary information
- This agency heads countywide electronic crimes task force.
- Threats presented by use of mobile devices such as laptops and PDAs
- We go after the criminals if possible
- We have had none. We did assist the FBI in a child safety case.
- We properly discovered, confiscated, maintained chain of custody to see a child pornography distributor prosecuted and incarcerated for 5 years. Only evidence on his government hard drive was used in the prosecution even though there were boxes of evidence at his residence.

Prevention through Network Monitoring

- An outside vendor tried using an expired password to gain access to financial data. After a lengthy investigation he was discovered.
- Audit trails showed unusual activity— activity was related to a hacked server turned into a wares site.
- Auditing procedures found and proved employee theft via manipulation of an inherited purchasing system
- By creating an acceptable use business case policy for Internet traffic allowed us to block all ports, except those necessary to conduct business. This narrows our margin of error for attacks and allows us to pinpoint the attack much quicker. We were able to stop the SQL Slammer within in minutes, because it could not go outbound.
- Community policing of phishing sites/e-mails by our organization—we notified a South American educational Institution of a hacked computer on their network that was hosting a phishing site, which was getting traffic from a phishing e-mail mass-blast. We did the same for a small ISP here in U.S.
- Detected several users who were viewing porn on government systems that would have bypassed Web proxies and RBLs—and based on a solid investigation that I performed resulted in the employee's termination. Being one of the first persons in the agency to address the impact, dangers, and preventions of malware
- Detection of an attempted brute force attack on our public facing File Transfer Protocol (FTP) server— attack was detected by our newly installed Security Information Management (SIM) system. The FTP server hardening/base lining process stopped the attack cold and provided valuable forensic evidence to confirm that the attack did fail and evidence for law enforcement to use for their investigation. Initial law enforcement investigation has lead to the discovery of compromised systems on different networks and the involvement of FBI and Secret Service.
- Have reduced inappropriate Web site surfing
- I traced a hacker back to his location and sent him a high-resolution overhead picture of his neighborhood and asked him to stay out of my system. Then I installed the hardware firewall, and no successful hack attempt since.
- Network monitoring, logging and close unnecessary services are the most effective ways that I found of preventing or solving e-crime attempt.
- Network operations personnel are continually monitoring the system for intrusions.
- Now prevent access to inappropriate Web sites. Network traffic substantially dropped with subsequent overall performance improvement.

- Proactively monitoring for phishing attempts and bringing down phishing sites before any customers every get to the site
- Quick detection of an exploited vulnerability
- Quick remediation of the blaster virus
- Tracing sources from where worms and viruses are originating and reporting to appropriate authorities
- Tracking defacing of a Web site to its source in Baghdad during the final months of Saddam's regime
- Very secure perimeter, progress on data encryption, progress on internal security zone regulation and monitoring
- We had a kid from the Netherlands placing porno videos on a DMZ server but caught it within hours because of real-time monitoring of disk spaced utilization changes.
- We have a real-time monitoring system for telephone calls on our network, which is critical to our business
- We were able to track and terminate a customer who was caught stealing services from a private patch panel. Our manual patch panel audit and records were able to help us track down the service and our badge system was able to point out who was responsible for the theft.

Passwords

- Former employee attempted to ftp 'his' files after termination, through dial up RAS server. Was married to an employee and used their login access. Access logs were his downfall.
- Heightening the awareness that password sharing has serious consequences and would not be tolerated - ensuring that employees understood that they were responsible for any and all actions performed under their user ID and/or password.
- Identification of fraudulent attempt to gain log-on passwords - identification of 'phishing' scams
- Made Web site login hacking harder to perform
- Password policy and monitoring of failed attempts to catch employees trying to access other peoples' accounts from home over the VPN
- Restructuring user access to follow a standardized setup and the retention of all related access authorization paperwork
- Rogue HTTP Tunnels stealing passwords.
- SQL code insertion via our Web site.
- We prevented an employee from stealing our source code.

Prevention of Identity Theft, Fraud

- Access to credit card data
- Automatic debt transfer frauds, credit card frauds, identity frauds
- Brute force attack used to compromise, guess customer PINS
- Calling card fraud scam
- Counterfeit access to checking account
- Credit card skimming
- Credit card theft
- Customer data theft
- Detection of fraud transactions submitted by bogus merchants.
- Did the digital forensics for an inside fraud case.
- Expense report fraud
- Fraud
- Fraud and identity theft cases
- Fraud identity theft from employee records
- Hackers with stolen customer credentials have been prevented from removing money.
- I conducted a computer forensic exam on two computers belonging to a check- counterfeiting ring. The computers contained approximately $500,000 worth of counterfeit check information. This case led to the prosecution of 9 individuals.
- I was involved in the prosecution and conviction of an identity thief/spammer.
- I would like to eliminate those entities that pose as financial Institutions to gather personal banking information, also the issue of foreign e-messages requesting assistant to establish banking relationship in the U.S.

- Identification and neutralization of Trojan/key logger compromises of customers' personal computers by organized rings that then attempt fraudulent takeovers of these banking and/or brokerage accounts via online channels
- Identification of identity theft and subscriber fraud on a regular basis
- Identity theft
- Identity theft cases
- I'm in the fraud department of my company, so everything I do is stopping e-crimes from occurring.
- Implementing an anti-fraud program in the online business and the prosecution of people where the losses are worth it
- Implementing full disk encryption prevents inadvertent disclosure of sensitive information from laptop computers.
- Incidents involving identity theft for the purpose of committing fraudulent business transactions in the firm's mission-critical billing application.
- Internal employee credit card fraud and prosecution
- Massive e-commerce fraud originating from Ghana and Nigeria on a large coordinated scale 6 Cooperation with federal and state agencies resulted in several prosecutions and improved defensive measures.
- Most of our e-crime is fraud in the minutes of use area. We have worked extensively to develop a fraud detection system, which has helped our customers and us.
- PayPal and various bank phishing attempts.
- Payroll fraud
- Personally developing an in-house Web-based fraud management system that allows the company to identify and stop hackers and fraudsters
- Prevented a customer from using stolen credit card information to make purchases on our Web site, identifying that the cards were stolen, and reporting to police the customer information. Police were able to determine how he had stolen the credit card information from an off-line source, and effected an arrest based in part on information we provided about his attempted use of these cards on our company site.
- Showing customers how to spot fraud in emails. How they are spoofed is covered, and no one accepts an emails word for changes made by bank accounts credit cards etc. They are all trashed. Everyone CALLS to verify. Have stopped many identify thefts.
- Theft of customer data
- Those that are connected to possible terrorist activity via communications fraud
- Use of fraudulent credit card information in circulation
- Used forensic analysis to prove intent in multi-million dollar fraud case.

Increased Company Awareness

- Cut short phishing expeditions and made everyone aware of them.
- Developing policies and procedures to attempt to secure mobile data storage devices. (USB pen drives)
- In the last several years, we have not been contaminated with a virus or worm. We attribute this to awareness training along with our implementation of two different anti-viral products that are automatically updated several times per day.
- Notified IS at outset of phishing attempts that were subsequently sent to large number of employees so that warnings were posted until offending e-mail could be blocked in system
- Via security education and awareness regarding attempts at phishing financial information from employees
- We had industrial espionage at our national sales meetings and have stopped that by equipping all employees and known meeting support personnel with photo IDs for duration of meeting— and hiring security people to require IDs for admission to the meetings.
- We have been very successful in deterring worms and other virus attacks from being acquired. Also, our training policy has served to guide employees in how not to spread suspect e-mails received.

All Incidents

- All of them
- All of them—Never happened
- I'm glad for all of the prevented ones, but won't be proud until I 'retire'—there's always tomorrow... Borrowing from an old pilots' phrase— here are those that have had their networks hacked, and those that will!
- Proud of our entire system in place, as well as low incident rates

- The fact that we have had only 1 worm get in since I have been employed here. It only infected 3 machines in 2 subnets.
- The nice thing about preventing attempts is that quite often you don't know that you've prevented one.
- They were all non-threatening, no loss or damage, other than down time
- Too many to list
- Too many to list— many successful prosecutions of criminal offenders in a variety of areas— all are important.
- Too numerous

Use of Third Party to Help Prevent/solve Electronic Crime

- Bringing in tool to another company where they were able to trace a sexual harassment incident.
- By relying on an outsourced electronic mail filter (e.g. Message Labs, Postini, etc), we have eliminated not just 90% of the spam/e-mail borne viruses, but over 5 million e-mails per month that our mail server would have to handle/process.
- Censornet prevention of access to forbidden sites
- Our firm was infected with a virus that was very new and there wasn't a fix for it at the time. Our team helped the outside virus protection company write the fix.
- The incident that I am most proud of solving was an Internet based database intrusion at a third party. I identified the location and type of intrusion prior to the forensic team's arrival and investigation.

Not Pleased with Current System, Nothing Stands Out

- Actually, it was a crime that was preventable but sr. management chose to ignore a warning. Through an audit we found a large hole in our network. It was recommended to unplug the insecure network until it could be secured (1 to 2 days). Management chose to leave the network up, in which time the blaster virus gutted our network after entering through the insecure network.
- I am not proud. We need better system.
- Most go unsolved.
- My management does not recognize nor reward attempts to prevent or solve e-crime. I am told to stay out of these things even though I am the appointed security officer for the application— others supposedly handle it.
- Nothing to solve, but our architecture prevents major problems.

Not Applicable

- Being a Republican that believes in the government giving power back to the people, and having religion separate from politics, while supporting our President and loving our country, America is the best country on this planet, and we've got to set a good example, and I think we're doing a darn good job.
- N/A (42 mentions)
- No direct involvement.
- None. Electronic Crime is not part of my job description
- Not involved with this activity. I am a field investigator, not management or corporate.

Don't Know/Unknown

- Don't know (8 mentions)
- Don't know of one
- I am not aware of the circumstances.
- I'm not in the IT section, so I don't know.
- No comments (three mentions)
- Unknown—we only see hackers after they have been successful
- Unknown (three mentions)
- Unknown— investigating/preventing internal intrusions not my function
- We are a new financial institution, so we have not had a great deal of time to test our policies and practices.
- We don't know what we don't know

No Occurrences of Electronic Crime

- Cannot say we know of electronic crime attempts.
- Can't think of one
- Have no known attempts—either all of our employees are fine, upstanding, law- abiding citizens or else they are smarter than we are.
- Have not solved nor prevented any.
- I have not been involved in any in-house e-crime investigations and I am not aware of any that have occurred.
- No known hacks and no known infections.
- No successful worms, viruses, Trojan horses, or hacker attacks since 2003.
- None on my watch, yet
- None reported.
- None. (30 mentions)
- None. Electronic Crime is not part of my job description
- Proud to say that, as far as we know, there has yet to be a successful e-crime attempt against our network.
- To the best of my knowledge, except for one minor virus infection, there have been none.
- To this point, we have been extremely successful in preventing the disclosure of private information.
- We have been free of incidents up to this point. Our primary concern is with growth. With an expanding workforce and customer set, opportunities increase for out of control activity.

Cannot Disclose Information

- Can't address this question.
- Do not want to disclose.
- I am unable to discuss this matter.
- I cannot describe this in this forum.
- Prefer not to disclose
- Rather not answer at this time

Summary of News Coverage Through 7/1/05

Print

Investor's Business Daily, 5/3/05: Computer Security Efforts Appear to Pay Off in '04
The Commercial Appeal, 5/5/05: Computer Crime Drops
Security Industry Association (SIA) Newsletter, 5/05: E-Crime a Continued Threat
Investor's Business Daily, 5/9/05: DataBus: Have E-crimes Leveled Off?
USA Today, 6/30/05: Snapshot: Most Believe E-crime Will Increase
CSO magazine, 7/1/05: Pulling Threats on E-Crime

Wire

United Press International, 5/4/05: E-crime Taking Expensive Toll on Business

Online

Milwaukee Journal Sentinel.com, 5/3/05: Electronic Crime is Better But Still Bad
National Journal's Technology Daily–PM Edition, 5/3/05: eBriefs
Washington Internet Daily, 5/3/05: Security
beSpacific.com, 5/4/05: Survey Indicates Progress in Fight Against E-Crimes
Bnet.com, 5/4/05: Survey Indicates Progress in Fight Against E-Crimes
Science Daily.com, 5/4/05: E-crime Taking Expensive Toll on Business
Security IT Toolbox, 5/4/05: E-crime Taking Expensive Toll on Business
Washington Times.com, 5/4/05: E-crime Taking Expensive Toll on Business
World Peace Herald, 5/4/05: E-crime Taking Expensive Toll on Business
Commercialappeal.com, 5/5/05: Computer Crime Drops
My Weblog, 5/9/05: 2005 E-crime Watch Survey Shows E-crime Fighters Making Headway
Microsoft Certified Professional Magazine, 5/30/05: Are We Winning the Battle Against E-Crime?
ENT News, 6/1/05: Are We Winning the Battle Against E-Crime?
Astalavista.com, 6/5/05: 2005 E-crime Watch Survey

News release posted on the following websites:

ArticleInsider.com
Bloomberg
Boerse
CNN Money
DallasNews.com
ETrade Financial
Fidelity Investments
Find-it-Cleveland.com
Forbes.com
KRON 4
KVVU-TV
Motley Fool/www.fool.com
Nasdaq.com
Quicken.com
Reuters
USAToday.com/Money
Yahoo!