FOR IMMEDIATE RELEASE

SURVEY SHOWS E-CRIME INCIDENTS ARE DECLINING YET IMPACT IS INCREASING

2006 E-Crime Watch Survey from CSO Magazine Reveals Insider Threats are on the Rise

Framingham, MA—Sept. 6, 2006—*CSO* magazine today releases results of the 2006 E-Crime Watch survey, which reveals a decline in security events[1], yet an increase in the financial and operational losses caused by such electronic crime[2] incidents. The third annual survey of 434 security executives and law enforcement personnel was conducted in cooperation with the U.S. Secret Service, Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center and Microsoft Corp.

According to findings, while the average number of security events per respondent continues to decline (34 in the last 12 months vs. 86 in 2005 and 136 in 2004), the impact of these crimes is increasing as reflected by both financial and operational losses. Sixty-three percent of respondents report operational losses as a result of e-crime, with 40 percent reporting financial losses (averaging $740,000 vs. $507,000 in 2005) and 23 percent reporting harm to their organization's reputation.

According to Bob Bragdon, publisher of *CSO* magazine, "Better perimeter technologies are helping organizations fight against e-crime's depleting effect on time, money and resources; however, we're also seeing increased reports of 'harm to reputation' and 'lost current/future revenues.'"

Offenders:

Survey results also show that while respondents continue to be most concerned with intruders from outside their organization (58 percent of events were reportedly committed by outsiders[3]; 27 percent by insiders[3]), the insider threat is getting worse. Of those organizations experiencing security events, the majority (55 percent) report at least one insider event (up from 39 percent the year prior).

"Just having policies in place is not good enough — organizations need to focus on implementation and enforcement of their policies," says Dawn Cappelli, Senior Member of the Technical Staff at CERT. "Nearly all respondents report having account and password management policies yet over half of the insiders compromised accounts, a third used backdoors and others used password crackers or sniffers."

As for the types of e-crime incidents, survey results reveal automated attacks like viruses, worms, and malicious code remain the most common form of e-crime with 72 percent of respondents reporting such incidents. Other common offenses include unauthorized access to or use of information systems or networks (60 percent), spyware (51 percent) and illegal generation of spam email (40 percent). While automated attacks have increased the number of incidents, targeted attacks are also on the rise with theft of proprietary information such as customer records reported by 36 percent, system sabotage by 33 percent and theft of intellectual property by 30 percent.

Preparedness and Response:

The 2006 E-Crime Watch survey reveals the most effective e-crime fighting technologies include statefull firewalls (87 percent), electronic access or control systems (86 percent), password complexity (80 percent), network-based anti-virus (74 percent) and encryption (74 percent). The study also shows continued investment in security with respondent organizations spending an average of $20 million on IT security and $19 million on physical security.

“The results of the E-Crime Watch survey show some progress, but also point to the work ahead,” says Doug Cavit, chief security strategist for Trustworthy Computing at Microsoft. “Along with our own research and dialogue with customers and partners, the survey reaffirms that organizations need to continue to invest not only in technology solutions, but also in partnerships to assist in the development of policies and best practices that can help fight evolving cyber crime threats.”

Overall, the survey shows organizations have better visibility into what is going on in their enterprises and are better prepared to respond. The majority of respondents (69 percent) say they are more prepared to prevent, detect, respond and recover from cyber security threats to the organization than in the past year. At the same time, more than half (56 percent) are more concerned about those threats than they were a year ago.

According to Ron Layton, Assistant to the Special Agent in Charge of the Criminal Investigative Division of the United States Secret Service, “The key is for law enforcement and the private sector to build and maintain close relationships regarding e-crime threats and incidents. It is law enforcement's hope that businesses and organizations will feel more comfortable and prepared to report cyber crime incidents to law enforcement.”

About the 2006 E-Crime Watch Survey
The 2006 E-Crime Watch survey was conducted by *CSO* magazine in cooperation with the U.S. Secret Service, Carnegie Mellon University Software Engineering Institute’s CERT® Coordination Center and Microsoft Corp. The survey was deployed June 28, 2006, through July 30, 2006. An email invitation containing a link to the survey was sent to 15,000 *CSO* magazine readers (CSOs, security and law enforcement professionals), yielding 434 respondents. Margin of error is +/- 3.4 percent. Respondent answers cover the period between July 2005 and June 2006.

NOTE TO EDITORS: Complete results attached below. Any references to the data from the 2006 E-Crime Watch survey must be sourced as originating from the following: *CSO* magazine, U.S. Secret Service, CERT Coordination Center, Microsoft Corp.

[1] “Security Event” is defined as an adverse event that threatens some aspect of computer security. This does not include spam; phishing emails sent to employees; virus-carrying emails or routine network and port scanning activity that are blocked by standard perimeter defenses; discovery of vulnerabilities in packaged software. It does include actual virus infections (a single outbreak affecting multiple machines is one “Event”) or worms or denial-of-service attacks that affect system performance/availability, anomalous Internet/network activity that appears targeted specifically at your organization, including successful or unsuccessful targeted hacks/exploits, and loss or theft of backup tapes or laptops with sensitive data, or other inadvertent exposure of data.
[2] “Electronic crime” is defined as a crime (an illegal act) that is carried out using a computer or electronic media.
[3] “Insider” is defined as current employee, service provider or contractor. “Outsider” is defined as a non-employee or non-contractor, currently or previously.

About *CSO* Magazine
Launched in 2002, *CSO* magazine, its companion website (www.CSOonline.com) and the CSO Perspectives™ conference provide 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 magazine is read by 27,000 security leaders from the private and public sectors. The U.S. edition of the magazine and website are the recipients of 80 awards to date, including the American Society of Business Publication Editor’s Magazine of the Year award as well as eleven Jesse H. Neal National Business Journalism Awards. Licensed editions of *CSO* magazine are published in Australia, France, Poland 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. In addition, *CSO* magazine produces a series of one-day events on privacy and data assurance. *CSO* magazine, CSOonline.com and the CSO Perspectives

conference are produced by International Data Group's award-winning business unit: CXO Media Inc.

About CERT
The CERT® Program is located at Carnegie Mellon University's Software Engineering Institute (SEI) in Pittsburgh, Pennsylvania, U.S.A. The SEI is a Department of Defense-sponsored federally funded research and development center. CERT's primary goals are to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit and ensure survivability – the continuity of critical services – in spite of successful attacks, accidents, or failures. The four major areas of work that constitute the CERT Program, which includes the well-known CERT Coordination Center (CERT/CC) are vulnerability and incident analysis, education and training, research and development, and evaluations and best practices.

About the Secret Service's Electronic Crimes Task Forces (ECTF)
The USA PATRIOT ACT OF 2001 (HR 3162, 107th Congress, First Session, October 26, 2001, Public Law 107-56) mandated the United States Secret Service 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, 24 ECTFs are proving successful in Atlanta, GA; Baltimore, MD; Birmingham, AL; Boston, MA; Buffalo, NY; Charlotte, NC; Chicago, IL; Cleveland, OH; Columbia, SC; Dallas, TX; Houston, TX; Las Vegas, NV; Los Angeles, CA; Louisville, KY; Miami, FL; Minneapolis, MN; New York, NY / Newark, NJ; Oklahoma City, OK; Orlando, FL; Philadelphia, PA; Pittsburgh, PA; San Francisco, CA; Seattle, WA; and Washington, DC.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

CONTACTS:
CSO magazine
Karen Fogerty
508.935.4091

Software Engineering Institute CERT Program
Kelly Kimberland
412-268-8467

U.S. Secret Service
Office of Public Affairs
202-406-5708

2006 E-Crime Watch Survey – Complete Survey Results

Conducted by *CSO* magazine in cooperation with the U.S. Secret Service, CERT® Coordination Center and Microsoft Corp.

SECTION ONE: RESPONDENT PROFILE

1) Is your organization public or privately held?

Public sector	55%
Private sector	45%

2) Please indicate the critical infrastructure sector to which your organization belongs:

Government	19%
Information Technology and Telecommunications	18%
Banking and Finance	15%
Public Health	7%
Defense Industrial Base	4%
Transportation	3%
Emergency Services	3%
Energy: electric utilities	2%
Food	1%
Postal and Shipping	1%
Chemical Industry and Hazardous Materials	1%
Agriculture	<1%
Energy: gas and oil	<1%
Water	<1%
Not applicable	25%

3) Which of the following best describes your organization's primary industry?

Government	15%
Banking and Finance	12%
Information and Telecommunications	10%
Education	8%
Health Care	8%
Electronics/ Technology	7%
Services	5%
Insurance	3%
State or County Law Enforcement/ Security (non emergency services)	3%
Retail, consumer products	3%
Military	3%
Defense Industrial Base	2%
Pharmaceutical	2%
Transportation	2%
Construction/ Real Estate	2%
Emergency Services	2%
Electric Power	1%
Federal Law Enforcement/ Security (non-emergency services)	<1%
Agriculture	<1%
Food	<1%
Retail, food/ drink	<1%
Wholesale	<1%
Natural Resources/ Mining	<1%
Research/ Development	<1%
Chemical	<1%
Gas & Oil	<1%
Nuclear Power	<1%

Postal and Shipping	<1%
Other	8%

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

100,000 or more	9%
50,000 - 99,999	5%
30,000 - 49,999	6%
20,000 - 29,999	4%
10,000 - 19,999	9%
7,500 - 9,999	2%
5,000 - 7,499	9%
2,500 - 4,999	11%
1,000 - 2,499	12%
500 - 999	10%
100 - 499	10%
Under 100	11%
Don't know	1%
Mean	21,504
Median	3,776

5) Which of the following best describes your job title?

Director/ Manager of any of the following (NET)	**46.5%**
Security	24.2%
IS/ IT/ communications/ networking	17.5%
Non-IT or security-related function (i.e., finance/ accounting, operations)	4.8%
Corporate Management (NET)	**25.1%**
Chief Security Officer (CSO) or Chief Information Security Officer (CISO)	10.6%
Chief Information Officer (CIO) or Chief Technology Officer (CTO)	9.9%
Corporate non-IT management (i.e., CEO, President, CFO, Treasurer, COO, General Manager, Managing Director)	4.6%
EVP, Senior VP, VP of any of the following (NET)	**7.8%**
IS/ IT/ communications/ networking	3.9%
Security	3.5%
Non-IT or security-related function (i.e., finance/ accounting, operations)	0.5%
Law Enforcement/ Prosecutor (NET)	**6.9%**
Detective/ Case Agent	1.8%
Supervisor	1.6%
Command Officer	1.2%
Chief/ Sheriff/ Director	0.7%
Deputy Chief/ Chief Deputy/ 1st Assistant	0.2%
Prosecutor	0.2%
Other	1.2%
Other (NET)	**13.6%**
Staff	7.8%
Consultant	5.8%

6) What was your organization's approximate annual budget for products, systems, services and/ or staff during the last 12 months?

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, anomaly detection systems, etc.)

Over $250 Million	2%
$100 to $249.9 Million	2%
$50 to $99.9 Million	2%
$25 to $49.9 Million	2%
$10 to $24.9 Million	4%
$5 to $9.9 Million	5%
$1 to $4.9 Million	14%
$500,000 to $999,999	7%
$250,000 to $499,999	7%
$100,000 to $249,999	12%
$50,000 to $99,999	8%
Less than $50,000	16%
Don't know/ Not Applicable	21%
Mean	$20,236,000
Median	$414,000

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.)

Over $250 Million	2%
$100 to $249.9 Million	2%
$50 to $99.9 Million	2%
$25 to $49.9 Million	2%
$10 to $24.9 Million	3%
$5 to $9.9 Million	5%
$1 to $4.9 Million	11%
$500,000 to $999,999	6%
$250,000 to $499,999	7%
$100,000 to $249,999	12%
$50,000 to $99,999	6%
Less than $50,000	15%
Don't know/ Not Applicable	26%
Mean	$19,022,000
Median	$367,000

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

ANY (NET)	93%
Decisions regarding information security	78%
Decisions regarding corporate/ physical security	59%
Decisions regarding referral of potential electronic crime to law enforcement	61%
Investigations or prosecution of electronic crime	52%
Audit reporting concerning fraud or electronic crimes	48%
Decisions regarding handling of employee policy violations	60%
None of the above	7%

SECTION TWO: SECURITY EVENTS

1) Please estimate the total number of security events experienced by your organization during the last 12 months (July 2005 - June 2006). 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.

0/ None	24%
ANY (NET)	**76%**
1	9%
2	9%
3	8%
4	5%
5	7%
6 to 9	5%
10 to 14	8%
15 - 19	2%
20 - 29	7%
30 - 49	3%
50 - 99	3%
100 - 199	4%
200 or more	5%
Mean (incl. 0)	25.7
Median (incl. 0)	3
Mean (excl 0)	34.1
Median (excl 0)	5

2) Did the total number of security events experienced by your organization increase, decrease or remain the same (July 2005 - June 2006) when compared to the prior 12 months (July 2004 - June 2005)?

Increased	36%
Decreased	20%
No Change	28%
Don't know/ not sure	16%

3) What percent of these events are known or suspected to have been caused by… (fill in)

OUTSIDERS (Non-employees or Non-contractors, currently or previously) (Base: 328)

0%/ None	20%
ANY (NET)	80%
1% - 9%	2%
10% - 19%	3%
20% - 29%	5%
30% - 39%	5%
40% - 49%	2%
50% - 59%	9%
60% - 69%	3%
70% - 79%	8%
80% - 89%	5%
90% - 99%	7%
100%	31%
Mean	58
Median	70

INSIDERS: Current employees or contractors) (Base: 328)

0%/ None	45%
ANY (NET)	55%
1% - 9%	5%
10% - 19%	5%
20% - 29%	9%
30% - 39%	5%
40% - 49%	2%
50% - 59%	7%
60% - 69%	4%

70% - 79%	4%
80% - 89%	2%
90% - 99%	3%
100%	9%
Mean	26.9
Median	5

UNKNOWN (Base: 328)

0%/ None	63%
ANY (NET)	37%
1% - 9%	6%
10% - 19%	7%
20% - 29%	7%
30% - 39%	1%
40% - 49%	1%
50% - 59%	3%
60% - 69%	1%
70% - 79%	<1%
80% - 89%	<1%
90% - 99%	<1%
100%	8%
Mean	15.1
Median	-

Mean Summary of Security Events Caused by Outsiders vs. Insiders vs. Unknown: (Base: 328)

Outsiders	58%
Insiders	27%
Unknown	15%

SECTION THREE: eCRIME

1) Of the security events your company experienced during the past 12 months, what percentage of these events were actual e-Crimes? (fill in) (Base: Experienced security event in last 12 months)

0%/ None	29%
ANY (NET)	38%
1% - 9%	3%
10% - 19%	5%
20% - 29%	4%
30% - 39%	2%
40% - 49%	1%
50% - 59%	3%
60% - 69%	1%
70% - 79%	2%
80% - 89%	1%
90% - 99%	2%
100%	17%

1) (con't.) Of the security events your company experienced during the past 12 months, what percentage of these events were actual e-Crimes? (fill in) (Base: Experienced security event in last 12 months)

Don't know	32%
Mean	36.5
Median	10

2) Please indicate which of the following e-Crimes were committed against your organization during the past 12 months, and the sources of these e-Crimes to the best of your knowledge. If the

source was not determined, please select “Source Unknown." If the e-Crime was not committed, please select “Not applicable" for that type of e-Crime:
Base: Experienced an e-Crime last 12 months

	Committed (net)	**Insider**	**Outsider**	**Source Unknown**	**Not Applicable**	**Don’t Know**
(Base)		Committed	Committed	Committed		
Theft of Intellectual Property	30%	63%	45%	5%	60%	10%
Theft of other (proprietary) info including customer records, financial records, etc.	36%	56%	49%	9%	56%	8%
Denial of service attacks	36%	0%	84%	20%	51%	13%
Virus, worms or other malicious code	72%	23%	80%	16%	21%	7%
Fraud (credit card fraud, etc.)	29%	47%	69%	18%	63%	9%
Identity theft of customer	19%	46%	79%	4%	70%	11%
Illegal generation of spam email	40%	10%	78%	20%	49%	10%
Phishing (someone posing as your company online in an attempt to gain personal data from your Subscribers or employees)	31%	0%	77%	26%	58%	11%
Unauthorized access to/ use of information, systems or networks	60%	47%	60%	13%	35%	6%
Sabotage: deliberate disruption, deletion or destruction of information, systems or networks	33%	49%	41%	15%	56%	12%
Extortion	33%	49%	41%	15%	56%	12%
Web site defacement	14%	22%	78%	6%	74%	12%
Zombie machines on organization’s network/ bots/use of network by BotNets	20%	16%	72%	28%	66%	14%
Intentional exposure of private or sensitive information	11%	71%	36%	7%	79%	10%
Spyware (not including adware)	51%	17%	73%	17%	37%	12%
Other	11%	50%	43%	21%	70%	19%

3) How these intrusions were handled based upon source:

	Insider	**Outsider**
Base	Experienced eCrime committed by Insider	Experienced eCrime committed by Outsider
Handled internally without involving legal action or law enforcement	72%	75%
Handled internally with legal action	13%	6%
Handled externally by notifying law enforcement	14%	18%
Handled externally by filing a civil action	2%	1%

4) Please indicate all mechanisms used by insiders in committing electronic crimes against your organization in 2005 (Base: Experienced e-Crime committed by insiders):

ANY (NET)	86%
Compromised an account	51%
Used authorized system administrator access	46%
Remote access	39%
Social engineering	38%
Backdoors	32%
Password crackers or sniffers	17%
Malicious code inserted as part of the software development process	10%
Logic bomb	3%
Other	10%
None	6%
Don't know	9%

5) If any intrusions were not referred for legal action, please indicate the reason(s) not referred: (Base: 126)

ANY (NET)	70%
Damage level insufficient to warrant prosecution	54%
Lack of evidence/ not enough information to prosecute	48%
Could not identify the individual/ individuals responsible for committing the e-Crime	34%
Concerns about negative publicity	11%
Prior negative response from law enforcement	5%
Unaware that we could report these crimes	4%
Concerns that competitors would use incident to their advantage	3%
Other	5%
Don't know	3%

6) Which of the following types of losses did your organization experienced during the past 12 months as a result of e-Crime? (Base: experienced an eCrime in the last 12 months)

ANY (NET)	80%
Operational losses	63%
Financial losses	40%
Harm to reputation	23%
Other	2%
Not applicable- no losses experienced in past 12 months	13%
Don't know/ not sure	6%

7) With respect to your organization, what is the most adverse consequence that has ever occurred from a security event caused by an insider?

ANY (NET)	66%
Critical system disruption (SUBNET)	36%
Critical system disruption to organization only	23%
Critical system disruption affecting Customers and business partners	10%
Critical system disruption affecting the larger critical infrastructure sector	3%
Harm to organization's reputation	15%
Loss of current or future revenue	11%
Loss of Customers	3%
Personal injury	1%
Loss of life	<1%
Loss of business partners	<1%
No impact	18%
Don't know	16%

8) Please estimate the total monetary value of losses your organization sustained due to e-Crime during the past 12 months. (Base: experienced an eCrime last 12 months)

$0/ None	11%
ANY (NET)	39%
Less than $10,000	10%
$10,000 - $49,999	12%
$50,000 - $99,999	5%
$100,000 - $499,999	6%
$500,000 - $999,999	2%
$1 million or more	5%
Don't know	50%
Mean	$739,700
Median	$45,000

9) During the past 12 months, did monetary losses to your organization from e-crIme increase, decrease, or remain the same compared to the prior 12 months (July 2004 – June 2005)? (Base: experienced an eCrime last 12 months)

Increase	29%
Decrease	14%
Remain the same	20%
Not sure	37%

EFFECTIVENESS OF SECURITY MEASURES

1) Which of the following groups posed the greatest cyber security threat to your organization during the past 12 months?

Hackers	31%
Current employees	21%
Former employees	7%
Foreign entities	5%
Current service providers/ consultants/ contractors	5%
Former service providers/ consultants/ contractors	3%
Competitors	3%
Information brokers	2%
Terrorists	1%
Customers	1%
Suppliers/ business partners	1%
Don't know/ not sure	20%

2) Does your organization have a formalized plan outlining policies and procedures for reporting and responding to security events committed against your organization?

Yes	66%
No (NET)	28%
No, but planning to implement formalized plan within next 12 months	17%
No plans for formalized plan at this time	12%
Don't know/ not sure	6%

3) How far back does your organization keep records on or otherwise keep track of security events?

1 year or less	14%
More than 1 year to 2 years	14%
More than 2 years to 5 years	25%
More than 5 years	21%
Don't know	17%
Not applicable - do not track network data & system intrusions	9%

4) How effective do you consider each of the following technologies in place at your organization in detecting and/ or countering security events?
(Scale: Very effective, Somewhat effective, Not very effective, Not at all effective, Don’t know, Not applicable- don’t use)

Technologies in Use

Host base configuration management	100%
Password Complexity	99%
Statefull Firewalls	97%
Electronic access control systems	96%
Heuristics-based SPAM filtering	95%
Network-based Antivirus	89%
Manual patch management	89%
Surveillance	88%
Encryption	88%
Badging	87%
Network IDS/IPS	87%
Network-based policy enforcement	86%
RBL-based SPAM filtering	85%
Host-based Antivirus	85%
Application Layer Firewalls	85%
Software Development Tools (& Processes)	84%
Automated patch management	83%
Configuration management systems	83%
Rights Management	82%
Network-based monitoring/ forensics	82%
Wireless encryption/ protection	82%
Policy-based network connections & enforcement	81%
Host-based firewalls	79%
Application Configuration Monitoring	79%
Role-based authentication	76%
Multi-factor/strong authentication	76%
Host-based policy-enforcement	75%
Application Monitoring & Trending	73%
Data Tracking	73%
Host-based SPAM filtering	69%
Application Signing	68%
Host-based AntiSPAM	67%
Wireless monitoring	66%
Host-based IDS/ IPS	64%
One-time Passwords	58%
Keystroke Monitoring	45%

Top 10 Most Effective (Very Effective or Somewhat Effective) Technologies in Use (Base: respondents with technology in use)

Statefull Firewalls	87%
Electronic access control systems	86%
Password Complexity	80%
Network-based AV	74%

Encryption	74%
Application layer firewalls	73%
Heuristics-based SPAM filtering	71%
Badging	68%
Network-based policy enforcement	67%
Host-based AV	65%

Top 10 Least Effective (Not Very or Not At All Effective) Technologies in Use (Base: respondents with technology in use)

Manual patch management	29%
Surveillance	21%
Wireless monitoring	21%
Software Development Tools (&processes)	17%
Configuration management systems	16%
Badging	16%
Application monitoring & trending	16%
Password Complexity	15%
Network-based monitoring/ forensics	15%
Heuristics-based SPAM filtering	15%

5) Which of the following security policies and procedures does your organization use in an attempt to prevent or reduce security events? (Base: 434)

ANY (NET)	97%
Account/ password management policies	91%
Acceptable use policy/ Formal “inappropriate use” policy	91%
Employee/ contractor background check	73%
Employee education & awareness programs	68%
Conduct regular security audits	65%
Non-disclosure agreement	63%
Monitor Internet connections	60%
Employee monitoring (use of Internet/ email/ applications)	59%
Periodic risk assessments	59%
Employees required to review and accept the written inappropriate use policy on any periodic basis	57%
Required internal reporting of misuse or abuse of computer access by employees or contractors	55%
Incident response team	54%
New employee security training	54%
Periodic systems penetration testing	49%
Internet connection monitoring (external)	49%
Random security audits	48%
Segregation of duties	48%
Regular account audits	47%
Include security in contract negotiations with vendors/ suppliers	43%
Regular information audits	38%
Regular security communication from management	36%
Hired a Chief Security Officer (CSO) or Chief Information Security Officer (CISO)	32%
Storage & review of e-mail or computer files	32%
Public Law Enforcement partnerships	27%
Government security clearances	22%
Use of “white hat” hackers	13%
None of the above/ Don’t have security policy in place	0%
Don't know	2%

	Deterrence of a potential criminal	Detection of a criminal	Termination of an Employee or Contractor	Prosecution of an Alleged Criminal	None of These	Don't Know
Acceptable use policy/ Formal “inappropriate use” policy	21%	5%	50%	4%	17%	19%
Employee/ contractor background check	35%	21%	21%	2%	14%	29%
Employee monitoring (use of Internet/ email/ applications)	21%	17%	39%	7%	14%	25%
Account/ password management policies	26%	6%	13%	1%	29%	31%
Monitor Internet connections	24%	13%	24%	3%	22%	28%
Required internal reporting of misuse or abuse of computer access by employees or contractors	26%	10%	27%	5%	19%	30%
Incident response team	23%	17%	23%	10%	26%	23%
Employee education & awareness programs	31%	5%	7%	1%	28%	32%
Employees required to review and accept the written inappropriate use policy on any periodic basis	33%	4%	17%	3%	24%	29%
Conduct regular security audits	26%	10%	7%	<1%	34%	28%
Internet connection monitoring (external)	25%	12%	19%	3%	25%	31%
Periodic risk assessments	30%	8%	6%	<1%	33%	31%
Non-disclosure agreement	28%	3%	10%	3%	32%	34%
Random security audits	29%	10%	10%	1%	33%	27%
New employee security training	31%	4%	6%	-	31%	34%
Segregation of duties	29%	5%	9%	1%	31%	32%
Periodic systems penetration testing	31%	8%	4%	1%	36%	28%
Regular account audits	27%	9%	8%	1%	33%	30%
Storage & review of e-mail or computer files	27%	9%	21%	4%	20%	32%
Regular information audits	30%	7%	10%	2%	27%	34%
Include security in contract negotiations with vendors/ suppliers	23%	4%	10%	1%	36%	32%
Regular security communication from management	30%	5%	7%	2%	32%	32%
Public Law Enforcement partnerships	25%	13%	10%	8%	18%	39%
Government security clearances	27%	13%	11%	1%	12%	41%
Hired a Chief Security Officer (CSO) or Chief Information Security Officer (CISO)	21%	11%	14%	4%	29%	40%
Use of “white hat” hackers	29%	7%	3%	-	28%	40%

6) How often does your organization review or update its security policy?

Monthly	4%
Every 6 months	9%
Annually	31%
As needed	44%
Other	4%
Don't know	9%

7) Are you more concerned or less concerned about cyber security threats posed to your organization this year than those you encountered the year before?

More concerned	56%
Less concerned	5%
Level of concern has not changed	39%

8) Are you more prepared or less prepared to deal with (prevent, detect, respond, recover) cyber security threats to your organization than last year?

More prepared	69%
Less prepared	5%
Same level of preparedness	26%

Percents calculated on total respondent base of 434 unless otherwise specified.
Percent may not sum to 100 due to rounding.