OVER-CONFIDENCE IS PERVASIVE AMONGST SECURITY PROFESSIONALS
2007 E-Crime Watch Survey shows security incidents, electronic crimes and their impact steady versus last year.

Framingham, MA—Sept. 11, 2007—*CSO* magazine today releases results of the 2007 E-Crime Watch Survey. This year's study revealed that while security events and electronic crimes were steady against last year's findings, there are real concerns that security executives may be becoming over confident.

Conducted with the U.S. Secret Service, Carnegie Mellon University Software Engineering Institute's CERT® Program and Microsoft Corp., the fourth annual survey polled 671 security executives and law enforcement officials on a variety of security topics, including commitment to security, the source of e-crimes, the top e-crimes professionals are experiencing, methods of attack, security technologies being deployed to defend against attacks, and the legal steps organizations are taking after they've been attacked.

"There is little doubt that organizations have learned a tremendous amount about security in the last five years and are making serious headway in understanding and combating threat," said Bob Bragdon, publisher of CSO Magazine. "At the same time, we saw signs in this study that organizations think they have things handled, which is concerning given the recent rise in targeted, financially motivated attacks."

A key indication of the study was that while 57% of participants said they are increasingly concerned about the potential effects of e-crime, and 49% of them reported experiencing an e-crime in 2006 vs. 38% the prior year, other responses suggested they are not prioritizing security as much as they have in previous years. For example, 69% of respondents said they are more prepared to deal with those threats than they have been in the past, yet these same organizations said they've trimmed spending on IT security by 5% and corporate security by 15%.

"You should never let down your guard when it comes to cybersecurity," said Jeff Jones, director of Trustworthy Computing for Microsoft. "Crime is a fact of life in the digital world just as it is in the physical world; even with the best security posture, you must still steadily guard against potential threat."

The Source of Crimes: Insiders, Outsiders and the Unknown

Part of guarding against threat is understanding its source, and so the survey posed several questions to compare cybercrimes by insiders and outsiders.

When asked who caused more damage (in terms of cost or operations), results were fairly close (insiders 34%, outsiders 37%, unknown 29%). But by their actions, participants indicated they may not be giving as much attention to insider threats as would seem justified. For example, background checks dropped from use in 73% of the organizations last year to only 57% this year, account/ password management policies dropped from 91% of the organizations last year to 84% this year, employee monitoring from 59% to 42%, and employee security awareness training from 68% last year to 38% this year.

"It is important that organizations are proactive in their approach to mitigating insider threats," says Dawn Cappelli, Senior Member of the Technical Staff at CERT. "Defense-in-depth isn't just about putting adequate technology in place, it's also about paying attention to your people and implementing policies and procedures to reduce the likelihood of an insider attack. Our research has shown that those very policies and practices that respondents are cutting back on are critical in mitigating insider threats."

The potential for damage from an insider attack is clear. Three of the top four e-crimes experienced this year were widespread attacks not targeted at an individual organization; insider attacks, on the other hand, were targeted at their organization. Survey results show that most insiders targeted proprietary information, including intellectual property, customer and financial information. Indeed, unauthorized access to/use of corporate information, systems or networks was the most common insider e-crime (experienced by 27% of respondents who experienced e-crime). Theft of intellectual property was the second most common e-crime (24%), theft of other information (including financial and customer records) was #3 (23%) and fraud (credit card, etc.) was #4 (19%).

Also of note was a shift in the methods being used by insiders to commit e-crimes. The use of social engineering techniques (gaining access through manipulation of a person or persons who can permit or facilitate access to a system or data) jumped to become the #1 method (45% v. 38% last year) followed by individuals using compromised accounts (39%), copying information to mobile devices like USB drives or iPods (36%), and use of their own account (35%). The use of sophisticated technologies like password crackers or sniffers jumped from being used by insiders in 17% of the organizations last year to 31% this year.

The survey found no major changes in e-crimes being perpetrated by outsiders, although there were marked jumps in the illegal generation of SPAM email (53% vs. 40% last year) and phishing attacks (46% vs. 31% last year). The top five e-crimes perpetrated by outsiders were: virus, worms or other malicious code (experienced by 74% of respondents), unauthorized access to/ use of information, systems or networks (experienced by 55%), illegal generation of SPAM email (experienced by 53%), spyware (not including adware – experienced by 52%), denial of service attacks (experienced by 49%), and phishing (experienced by 46%).

Electronic Crime Trends:

Of some concern is that most e-crimes, whether perpetrated by an insider or an outsider, are handled internally without involving legal action or law enforcement (67% for insiders, 66% for outsiders.) Given the growth in the number of crimes involving the theft of personally identifiable information, and the breach notification laws that have been passed, it is concerning to see that organizations continue to handle so many cases within their own walls. When asked why they had not referred these e-crimes for legal action, respondents echoed last year's findings that either the damage level was insufficient to warrant prosecution (40%), there was a lack of evidence (34%), or that they could not identify the individuals responsible (28%).

Best Practices in Preventing Electronic Crimes:

The survey found that the most effective technologies were: Statefull firewalls (maintaining its position as #1 at 82%), access controls (new to this year's survey at 79%), electronic access controls (78%), application layer firewalls (72%), and host-based anti-virus (70%). The least effective technologies were: manual patch management, surveillance, password complexity, badging, and RBL-based SPAM filtering.

These results show high levels of confidence in traditional perimeter technologies. But these all have limited effectiveness – enterprise perimeters are no longer clearly defined and the respondents' reliance upon traditional perimeter technologies may leave them exposed to attacks that bypass the perimeter.

On the other hand, the survey found that organizations are relying upon processes and policies to secure against insider threats. Inappropriate use policies and segregation of duties, tools that have always been

available to management, are finding increased acceptance as effective means to ensure compliance and supplement technological means of securing information assets.

About the 2007 E-Crime Watch Survey

The 2007 eCrime Watch survey was conducted by CSO magazine in cooperation with the U.S. Secret Service, Carnegie Mellon University Software Engineering Institute's CERT® Program and Microsoft Corp. The survey was deployed July 26, 2007, through August 13, 2007. An email invitation containing a link to the survey was sent to 15,000 CSO magazine readers and members of the US Secret Service's Electronic Crime Task Forces, yielding 671 respondents. Margin of error is +/- 3.79 percent. Respondent answers cover the period between July 2006 and June 2007.

NOTE TO EDITORS: Complete results attached below. Any references to the data from the 2007 E-Crime Watch survey must be sourced as originating from the following: CSO magazine, U.S. Secret Service, CERT® Program, Microsoft Corp.

1. **Security Event**: An adverse event that threatens some aspect of computer security.
Note: For the purposes of this survey, Security Events do NOT include: receipt of 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.

Events DO include (but are not limited to):
- 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.
- Loss or theft of backup tapes, laptops with sensitive data, mobile devices with sensitive data or other inadvertent exposure of data.

2. **Electronic Crime** (eCrime): A crime (an illegal act) that is carried out using a computer or electronic media. **Intrusion**: An incident in which an organization's computing systems are compromised by an unauthorized individual or individuals.

3. **Insider**: Current or former: employee, service provider or contractor. **Outsider**: Someone who has never had authorized access to an organization's systems or networks.

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 federally funded research and development center sponsored by the U.S. Department of Defense. Home to the CERT Coordination 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.

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
Sue Yanovitch
508.935.4448

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

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

2007 E-Crime Watch Survey – Survey Results
Conducted by *CSO* magazine in cooperation with the U.S. Secret Service,
CERT® Coordination Center and Microsoft Corp.

OVERALL RESULTS

E-Crime Watch Survey 2007
Field Dates .....July 26, 2007 – August 13, 2007
Total completed surveys.....671
Margin of Error .....+/- 2.1%

NOTE TO EDITOR

Complete results attached below. Any references to the data from the 2007 eCrime Watch survey must be sourced as originating from the following: *CSO* magazine, U.S. Secret Service, CERT® Program, Microsoft Corp.

1. **Security Event**: An adverse event that threatens some aspect of computer security.
Note: For the purposes of this survey, Security Events do NOT include: receipt of 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.

Events DO include (but are not limited to):
- 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.
- Loss or theft of backup tapes, laptops with sensitive data, mobile devices with sensitive data or other inadvertent exposure of data.

2. **Electronic Crime** (eCrime): A crime (an illegal act) that is carried out using a computer or electronic media. Intrusion: An incident in which an organization's computing systems are compromised by an unauthorized individual or individuals.

3. **Insider**: Current or former: employee, service provider or contractor. **Outsider**: Someone who has never had authorized access to an organization's systems or networks.

This study covers the period of time during the last 12 months (July 2006 – June 2007).

SECTION ONE: RESPONDENT PROFILE

1) Is your organization public or privately held?

Public sector	44%
Private sector	56%

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

Information Technology and Telecommunications	24%
Government	17%
Banking and Finance	14%
Public Health	5%
Transportation	3%
Defense Industrial Base	2%
Emergency Services	2%
Energy: electric utilities	2%
Food	2%
Energy: gas and oil	2%
Chemical Industry and Hazardous Materials	1%
Postal and Shipping	<1%
Agriculture	<1%
Water	<1%
Not applicable	26%

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

Information and Telecommunications	12%
Banking and Finance	12%
Government	9%
Education	8%
Health Care	7%
Electronics/ Technology	6%
Federal Law Enforcement/ Security (non-emergency services)	6%
Services	6%
Retail, consumer products	3%
Insurance	3%
Construction/ Real Estate	2%
State or County Law Enforcement/ Security (non emergency services)	2%
Transportation	2%
Defense Industrial Base	2%
Wholesale	2%
Gas & Oil	2%
Military	1%
Pharmaceutical	1%
Research/ Development	1%
Electric Power	1%
Food	1%
Emergency Services	1%
Retail, food/ drink	1%
Agriculture	<1%
Natural Resources/ Mining	<1%
Chemical	<1%

Hazardous Materials ..... <1%
Water ..... <1%
Other 10%

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 7%
50,000 - 99,999 ..... 4%
30,000 - 49,999 ..... 2%
20,000 - 29,999 ..... 2%
10,000 - 19,999 ..... 6%
7,500 - 9,999 ..... 4%
5,000 - 7,499 ..... 8%
2,500 - 4,999 ..... 8%
1,000 - 2,499 ..... 9%
500 - 999 ..... 8%
100 - 499 ..... 18%
Under 100 ..... 24%
Don't know 1%
Mean 15,612
Median 938

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

Director/ Manager of any of the following (NET) 34.4%
IS/ IT/ communications/ networking 21.2%
Security 8.2%
Non-IT or security-related function (i.e., finance/ accounting, operations) 5.1%
Corporate Management (NET) 27.6%
Chief Information Officer (CIO) or Chief Technology Officer (CTO) 15.6%
Corporate non-IT management (i.e., CEO, President, CFO, Treasurer, COO, General Manager, Managing Director) 7.5%
Chief Security Officer (CSO) or Chief Information Security Officer (CISO) 4.5%
Law Enforcement/ Prosecutor (NET) 11.6%
Detective/ Case Agent 7.2%
Supervisor 2.1%
Command Officer 0.4%
Deputy Chief/ Chief Deputy/ 1st Assistant 0.3%
Chief/ Sheriff/ Director 0.1%
Other 1.5%
EVP, Senior VP, VP of any of the following (NET) 8.9%
IS/ IT/ communications/ networking 4.5%
Security 2.5%
Non-IT or security-related function (i.e., finance/ accounting, operations) 1.9%
Other (NET) 17.4%
Staff 10.3%
Consultant 7.2%

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	3%
$100 to $249.9 Million	1%
$50 to $99.9 Million	1%
$25 to $49.9 Million	1%
$10 to $24.9 Million	3%
$5 to $9.9 Million	3%
$1 to $4.9 Million	8%
$500,000 to $999,999	4%
$250,000 to $499,999	5%
$100,000 to $249,999	8%
$50,000 to $99,999	10%
Less than $50,000	31%
Don't know/ Not Applicable	22%
Mean	$19,274,000
Median	$89,000

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	1%
$50 to $99.9 Million	1%
$25 to $49.9 Million	1%
$10 to $24.9 Million	2%
$5 to $9.9 Million	4%
$1 to $4.9 Million	7%
$500,000 to $999,999	3%
$250,000 to $499,999	4%
$100,000 to $249,999	8%
$50,000 to $99,999	8%
Less than $50,000	30%
Don't know/ Not Applicable	30%
Mean	$16,158,000
Median	$82,000

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

ANY (NET)	86%
Decisions regarding information security	70%
Decisions regarding corporate/ physical security	48%
Decisions regarding referral of potential electronic crime to law enforcement	51%
Investigations or prosecution of electronic crime	47%
Audit reporting concerning fraud or electronic crimes	43%
Decisions regarding handling of employee policy violations	48%
None of the above	14%

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	29%
ANY (NET)	66%
1	10%
2	13%
3	8%
4	4%
5	5%
6 to 9	5%
10 to 14	6%
15 - 19	2%
20 - 29	2%
30 - 49	3%
50 - 99	3%
100 - 199	2%
200 or more	4%
Mean (incl. 0)	140
Median (incl. 0)	2
Mean (excl 0)	201
Median (excl 0)	4

2) Did the total number of security events experienced by your organization increase, decrease or remain the same (July 2006 - June 2007) when compared to the prior 12 months (July 2005 - June 2006)?

Increased	33%
Decreased	19%
No Change	28%
Don't know/ not sure	20%

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: 443)

0%/ None	24%
ANY (NET)	76%
1% - 9%	2%
10% - 19%	3%
20% - 29%	4%
30% - 39%	3%
40% - 49%	1%
50% - 59%	10%
60% - 69%	3%
70% - 79%	4%
80% - 89%	4%
90% - 99%	7%
100%	36%

Mean 58
Median 70

INSIDERS: Current or former employees or contractors) (Base: 443)

0%/ None 51%
ANY (NET) 49%
1% - 9% 4%
10% - 19% 5%
20% - 29% 8%
30% - 39% 3%
40% - 49% 1%
50% - 59% 9%
60% - 69% 2%
70% - 79% 3%
80% - 89% 3%
90% - 99% 3%
100% 10%
Mean 26
Median ..... -

UNKNOWN (Base: 443)

0%/ None 67%
ANY (NET) 33%
1% - 9% 3%
10% - 19% 8%
20% - 29% 5%
30% - 39% 1%
40% - 49% 1%
50% - 59% 3%
60% - 69% ..... <1%
70% - 79% 1%
80% - 89% ..... <1%
90% - 99% ..... <1%
100% 11%
Mean 17
Median ..... -

Mean Summary of Security Events Caused by Outsiders vs. Insiders vs. Unknown: (Base: 443)

Outsiders 58%
Insiders 26%
Unknown 17%

4) Of the security events your company experienced during the past 12 months, what percentage of these events were: Targeted attacks aimed at your company, your employees, or your resources specifically?

0%/ None	60%
ANY (NET)	40%
1% - 9%	3%
10% - 19%	4%
20% - 29%	5%
30% - 39%	2%
40% - 49%	1%
50% - 59%	11%
60% - 69%	1%
70% - 79%	3%
80% - 89%	1%
90% - 99%	1%
100%	10%
No Answer	<1%
Mean	22%
Median	-

5) Of the security events your company experienced during the past 12 months, what percentage of these events were: Non-specific or incidental attacks/malware that happened to impact your company, employees or resources?

0%/ None	10%
ANY (NET)	90%
1% - 9%	<1%
10% - 19%	1%
20% - 29%	2%
30% - 39%	2%
40% - 49%	1%
50% - 59%	11%
60% - 69%	2%
70% - 79%	3%
80% - 89%	4%
90% - 99%	6%
100%	60%
No Answer	<1%
Mean	78%
Median	100%

6) Among those targeted attacks aimed at your company, have the number of those attacks increased or decreased when compared to the prior year?

Increased	25%
Decreased	11%
Remained the same	64%

7) When you consider the financial losses or costs to your company from those targeted attacks aimed at your company, has the financial loss or cost increased or decreased when compared to the prior year?

Increased.....21%
Decreased.....11%
Remained the same 67%

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	51%
ANY (NET)	49%
1% - 9%	9%
10% - 19%	5%
20% - 29%	4%
30% - 39%	2%
40% - 49%	2%
50% - 59%	7%
60% - 69%	2%
70% - 79%	2%
80% - 89%	1%
90% - 99%	2%
100%	14%
No Answer	1%
Mean	26
Median	-

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*		
Virus, worms or other malicious code	74%	18%	46%	26%	15%	12%
Unauthorized access to/ use of information, systems or networks	55%	25%	30%	10%	29%	16%
Illegal generation of spam email	53%	6%	38%	17%	35%	12%
Spyware (not including adware)	52%	13%	33%	18%	34%	14%
Denial of service attacks	49%	9%	32%	14%	37%	14%
Fraud (credit card fraud, etc.)	46%	19%	28%	5%	41%	14%
Phishing (someone posing as your company online in an attempt to gain personal data from your Subscribers or employees)	46%	5%	35%	12%	43%	12%
Theft of other (proprietary) info including customer records, financial records, etc.	40%	23%	16%	6%	45%	15%
Theft of Intellectual Property	35%	24%	12%	6%	52%	14%
Intentional exposure of private or sensitive information	35%	17%	12%	9%	49%	16%
Identity theft of customer	33%	13%	19%	6%	52%	15%
Sabotage: deliberate disruption, deletion or destruction of information, systems or networks	30%	14%	14%	6%	54%	16%
Zombie machines on organization’s network/ bots/use of network by BotNets	30%	6%	19%	10%	51%	20%
Web site defacement	24%	4%	14%	7%	64%	13%
Extortion	16%	5%	9%	4%	69%	14%
Other	17%	6%	8%	7%	65%	18%
None of the Above	7%	46%	23%	61%	19%	59%

3) How these intrusions were handled based upon source:

	Insider	Outsider
	Experienced eCrime committed by Insider	**Experienced eCrime committed by Outsider**
Handled internally without involving legal action or law enforcement	67%	66%
Handled internally with legal action	12%	9%
Handled externally by notifying law enforcement	16%	23%
Handled externally by filing a civil action	5%	2%

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) 90%
Social engineering 45%
Compromised an account 39%
Copied information to mobile device (USB drive, iPod, etc.) 36%
Used their own account 35%
Password crackers or sniffers 31%
Shared account (e.g. system administrator, DBA, etc.) 31%
Used authorized system administrator access 26%
Backdoors 25%
Remote access 20%
Rootkit or Hacking Tools 18%
Malicious code inserted as part of the software development process 13%
Logic bomb 6%
Other 8%
None 4%
Don't know 6%

5) If any intrusions were not referred for legal action, please indicate the reason(s) not referred: (Base: 162)

ANY (NET) 93%
Damage level insufficient to warrant prosecution 40%
Lack of evidence/ not enough information to prosecute 34%
Could not identify the individual/ individuals responsible for committing the e-Crime 28%
Concerns about negative publicity 22%
Concerns that competitors would use incident to their advantage 13%
Prior negative response from law enforcement 9%
Unaware that we could report these crimes 7%
Other 9%
Don't know 7%

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)	72%
Operational losses	52%
Financial losses	31%
Harm to reputation	25%
Loss of Life	1%
Other	4%
Not applicable- no losses experienced in past 12 months	15%
Don't know/ not sure	13%

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)	57%
Critical system disruption (SUBNET)	23%
Critical system disruption to organization only	14%
Critical system disruption affecting Customers and business partners	8%
Critical system disruption affecting the larger critical infrastructure sector	1%
Loss of confidential or proprietary information	13%
Harm to organization's reputation	10%
Loss of current or future revenue	6%
Loss of Customers	3%
Reduction in overall corporate valuation	2%
Loss of business partners	<1%
Loss of life	<1%
Personal injury	<1%
No impact	20%
Don't know	23%

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	10%
ANY (NET)	23%
Less than $10,000	8%
$10,000 - $49,999	5%
$50,000 - $99,999	2%
$100,000 - $499,999	2%
$500,000 - $999,999	1%
$1 million or more	5%
Don't know	63%
Mean	$465,700
Median	$1,000

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 2005 – June 2006)? (Base: experienced an eCrime last 12 months)

Increase	30%
Decrease	13%
Remain the same	18%
Not sure	39%

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	26%
Current employees	19%
Foreign entities	6%
Former employees	6%
Information brokers	3%
Customers	3%
Current service providers/ consultants/ contractors	2%
Former service providers/ consultants/ contractors	2%
Suppliers/ business partners	1%
Terrorists	1%
Competitors	1%
Don't know/ not sure	30%

2) In general, which electronic crimes were more costly or damaging to your organizations, those perpetrated by…?

Outsider: Someone who has never had authorized access to an organization's systems or networks	37%
Insider: Current or Former: employee, service provider or contractor	34%
Don't know	29%

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

Yes	52%
No (NET)	36%
No, but planning to implement formalized plan within next 12 months	17%
No plans for formalized plan at this time	21%
Don't know/ not sure	12%

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

1 year or less	13%
More than 1 year to 2 years	14%
More than 2 years to 5 years	18%
More than 5 years	16%
Don't know	25%
Not applicable - do not track network data & system intrusions	14%

5) 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

- Password Complexity 95%
- Statefull Firewalls 94%
- Heuristics-based SPAM filtering 93%
- Electronic access control systems 89%
- Network-based policy enforcement 89%
- Host-based Antivirus 89%
- Encryption 87%
- Manual patch management 87%
- RBL-based SPAM filtering 86%
- Application Layer Firewalls 86%
- Network-based Antivirus 86%
- Policy-based network connections & enforcement 85%
- Rights Management 85%
- Automated patch management 83%
- Change control/Configuration management systems 82%
- Wireless encryption/ protection 81%
- Host-based firewalls 81%
- Surveillance 81%
- Network IDS/IPS 81%
- Host-based policy-enforcement 79%
- Software Development Tools (& Processes) 79%
- Host-based Anti-SPAM 79%
- Multi-factor/strong authentication 78%
- Application Configuration Monitoring 76%
- Badging 76%
- Data Tracking 75%
- Network-based monitoring/forensics/ESM tool 74%
- Role-based authentication 72%
- Application Monitoring & Trending 72%
- Host-based IDS/ IPS 71%
- Host base configuration management 71%
- Application Signing 67%
- Wireless monitoring 65%
- One-time Passwords 62%
- Keystroke Monitoring 50%

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

2007 Rank	**Technology** (2007 percentage)	**2006 Rank** (last year)
1	Statefull Firewalls (82%)	1
2	Access Controls (79%)	Not asked
3	Electronic access controls (78%)	2
4	Application layer firewalls (72%)	6
5	Host-based Anti-virus (70%)	10
6	Password complexity (70%)	3
7	Encryption (69%)	5
8	Heuristics-based SPAM filtering (69%)	7
9	Network-based policy enforcement (68%)	9
10	Network-based Anti-Virus (65%)	4

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

2007 Rank	**Technology** (2007 percentage)	**2006 Rank** (last year)
1	Manual Patch Management (26%)	1
2	Surveillance (18%)	2
3	Password Complexity (17%)	8
4	Badging (16%)	6
5	RBL-based SPAM filtering (15%)	13
6	Host-based Anti-SPAM (14%)	15
7	Wireless monitoring (14%)	3
8	Change control/configuration management systems (13%)	5
9	Software development tools & processes (13%)	4
10	One-time passwords (12%)	16

6) Which of the following security policies and procedures does your organization use in an attempt to prevent or reduce security events? (Base: 671)

ANY (NET)	92%
Account/ password management policies	84%
Acceptable use policy/ Formal “inappropriate use” policy	80%
Internet connection monitoring (external)	59%
Monitor Internet connections	59%
Employee/ contractor background check	57%
Non-disclosure agreement	53%
Conduct regular security audits	51%
New employee security training	43%
Employee Assistance Program	43%
Employee monitoring	42%
Periodic risk assessments	42%
Employees required to review and accept the written inappropriate use policy on any periodic basis	50%
Periodic Security education and awareness programs	38%
Random security audits	36%
Storage & review of e-mail or computer files	36%
Intellectual property agreement	35%
Required internal reporting of misuse or abuse of computer access by employees or contractors	34%
Periodic systems penetration testing	34%
Regular account audits	34%
Include security in contract negotiations with vendors/ suppliers	33%
Regular information audits	32%
Incident response team	30%
Third party security audits of YOUR organization	27%
Regular security communication from management	27%
Software Code Review	25%
Security service level agreements (SLAs) with partners	25%
Technically enforced Segregation of duties	24%
Hired a Chief Security Officer (CSO) or Chief Information Security Officer (CISO)	23%
Public Law Enforcement partnerships	20%
Government security clearances	19%
Use of “white hat” hackers	11%
Third party security audits of PARTNER organizations	11%
None of the above/ Don’t have security policy in place	1%
Don't know	7%

7) Have any of the following security policies and procedures at your organization supported or played a role in the:
   - Deterrence of a potential criminal
   - Detection of a criminal
   - Termination of an employee or contractor
   - Prosecution of an alleged criminal

Security Policy	Deterrence of a potential criminal	Detection of a criminal	Termination of an Employee or Contractor	Prosecution of an Alleged Criminal
Employees required to review and accept the written inappropriate use policy on any periodic basis	58%	6%	35%	10%
Periodic security education & awareness programs	30%	2%	5%	2%
Technically-enforced segregation of duties	30%	4%	9%	2%
Use of “white hat” hackers	30%	13%	5%	5%
Periodic risk assessments	29%	5%	4%	2%
Periodic systems penetration testing	29%	4%	4%	3%
Third-party security audits of PARTNER organizations	29%	7%	7%	4%
Employee/ contractor background check	28%	13%	17%	1%
Government security clearances	28%	10%	13%	-
Monitor Internet connections	28%	11%	24%	3%
New employee security training	28%	4%	5%	1%
Random security audits	28%	13%	14%	3%
Regular account audits	28%	10%	14%	3%
Regular information audits	27%	9%	12%	3%
Regular security communication from management	27%	4%	4%	2%
Required internal reporting of misuse or abuse of computer access by employees or contractors	27%	9%	24%	5%
Account/ password management policies	26%	5%	9%	2%
Employee monitoring	26%	14%	29%	5%
Storage & review of e-mail or computer files	26%	6%	21%	3%
Hired a Chief Security Officer (CSO) or Chief Information Security Officer (CISO)	25%	8%	11%	3%
Incident response team	25%	18%	16%	9%
Public Law Enforcement partnerships	25%	11%	7%	14%
Conduct regular security audits	24%	11%	12%	3%
Include security in contract negotiations with vendors/ suppliers	24%	4%	9%	<1%
Non-disclosure agreement	24%	2%	8%	3%
Security service level agreements (SLAs) with partners	24%	2%	5%	<1%
Third party security audits of YOUR organization	24%	6%	4%	2%
Intellectual property agreement	22%	3%	9%	3%
Software code review	21%	3%	4%	1%
Acceptable use policy/ Formal “inappropriate use” policy	19%	5%	39%	4%
Employee Assistance Program	14%	2%	5%	<1%

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

Monthly	5%
Every 6 months	11%
Annually	28%
As needed	34%
Other	2%
Don't know	13%
No answer	8%

9) 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	57%
Less concerned	6%
Level of concern has not changed	37%

10) 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	25%

Percents calculated on total respondent base of 671 unless otherwise specified.
Percent may not sum to 100 due to rounding.

###