

FOR IMMEDIATE RELEASE



**2004 E-CRIME WATCH™ SURVEY SHOWS
SIGNIFICANT INCREASE IN ELECTRONIC CRIMES**
2003 E-Crime Losses Estimated At \$666 Million

Framingham, MA—May 25, 2004—The 2004 E-Crime Watch survey conducted among security and law enforcement executives by *CSO* magazine in cooperation with the United States Secret Service and the Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center, shows a significant number of organizations reporting an increase in electronic crimes (e-crimes) and network, system or data intrusions. Forty-three percent (43%) of respondents report an increase in e-crimes and intrusions versus the previous year and 70% report at least one e-crime or intrusion was committed against their organization. Respondents say that e-crime cost their organizations approximately \$666 million in 2003. However, 30% of respondents report their organization experienced no e-crime or intrusions in the same period.

E-Crimes Impact

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

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

Who are the Criminals?

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

Monitoring & Reporting

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

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

Best Practices

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

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

About the 2004 E-Crime Watch Survey

The 2004 E-Crime Watch survey was conducted by *CSO* magazine in cooperation with the United States Secret Service and the CERT Coordination Center. The research was conducted to unearth e-crime fighting trends and techniques, including best practices and emergent trends.

For the purpose of this survey, an electronic crime is defined as: Any criminal violation in which electronic media is used in the commission of that crime. An insider is defined as: a current or former employee or contractor. An outsider is defined as: non-employee or non-contractor. The online survey of *CSO* magazine subscribers and members of the United States Secret Service’s Electronic Crimes Task Force members was conducted from April 15 to April 26, 2004. Results are based on 500 completed surveys. At a 95% confidence level, the margin of error is +/- 4.4%.

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

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

About CSO Magazine

CSO magazine is published by CXO Media Inc. In addition to *CSO*, CXO Media publishes *CIO* magazine (launched in 1987), www.cio.com, *The CIO Insider*, CSOonline.com and darwinmag.com. CXO Media serves CIOs, CSOs, CEOs, CFOs, COOs and other corporate officers who use technology to thrive and prosper in this new era of business. The company strives to enhance partnerships among C-level executives, as well as create opportunities for information technology (IT) and consumer marketers to reach them. In addition to magazines and websites, CXO Media produces Executive Programs, a series of conferences that provide educational and networking opportunities for corporate and government leaders. CXO Media Inc. is a subsidiary of IDG, International Data Group (IDG), the world's leading technology media, research and event company. A privately-held company, IDG publishes more than 300 magazines and newspapers including *Bio-IT World*, *CIO*, *CSO*, *Computerworld*, *GamePro*, *InfoWorld*, *Network World* and *PC World*. The company features the largest network of technology-specific Web sites with more than 400 around the world. IDG is also a leading producer of more than 170 computer-related events worldwide including LinuxWorld Conference & Expo®, Macworld Conference & Expo®, DEMO®, and IDC Directions. IDC provides global market research and advice through offices in 50 countries. Company information is available at <http://www.idg.com>.

About 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.

About the Secret Service-Led Electronic Crimes Task Forces (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 our 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; Detroit, MI; Houston, TX; Las Vegas, NV; Los Angeles, CA; Miami, FL; New York, NY; Philadelphia, PA; San Francisco, CA; Washington, DC. The current ECTF success models will be utilized for the additional 15 ECTFs scheduled to open prior to 2010.

NOTE TO EDITORS: Complete findings from the 2004 E-Crime Watch survey can be found at http://www.csoonline.com/releases/052004129_release.html. If you report any of the data from the 2004 E-Crime Watch survey, the data must be sourced as originating from: *CSO* magazine/U.S. Secret Service/CERT Coordination Center.

CONTACTS:

CSO magazine
Susan Watson
508.935.4190

CERT Coordination Center
Kelly Kimberland
412.268.8467

U.S. Secret Service
Office of Public Affairs
202.406.5708

#

2004 E-Crime Watch – Survey Results

From *CSO* magazine in cooperation with the U.S. Secret Service & CERT® Coordination Center

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

Section 1: Demographics

1) Are you personally involved in any of the following at your organization? (Check all that apply) (Base: 500)

Decisions regarding information security	79.4%
Decisions regarding referral of potential electronic crime to law enforcement	60.0%
Investigations or prosecution of electronic crimes	56.0%
Decisions regarding corporate/physical security	50.6%
Audit reporting concerning fraud or electronic crimes	43.8%

2) Is your organization a member of: (Base: 500)

Government	23.6%
Law enforcement/Prosecutor	9.6 %
Private Sector	66.8%

3) Which of the following best describes your job title? (Base: 500)

Corporate Management	23.8%
EVP, Senior VP or VP	8.8 %
Director/Manager	42.4%
Law enforcement/prosecutor	12.0%
Other	13.0%

4) How long have you been employed in this position: (Base: 500)

1 year or less	7.2%
More than 1 to 2 years	12.8%
More than 2 to 5 years	33.4%
5 plus years	46.6%

5) Please indicate the critical infrastructure sector to which your industry belongs: (Base: 500)

Government	27.6%
Information and telecommunications	19.4%
Banking and finance	14.6%
Public health	7.6%
Transportation	2.8%
Defense industrial base	2.6%
Food	2.0%

Energy	1.8%
Emergency services	1.0%
Chemical industry	0.8%
Water	0.4%
Postal and shipping	0.2%
Not applicable	19.2%

6) Which of the following best describes your organization's primary industry: (Base: 500)

Banking and finance	12.6%
Information and telecommunications	12.2%
Law enforcement/security	10.6%
Education	10.2%
Government	9.8%
Health care	7.6%
Electronics/technology	5.2%
Military	4.4%
Services	4.0%
Insurance	2.6%
Transportation	2.0%
Defense industrial base	1.4%
Electric power	1.2%
Research and development	1.2%
Wholesale	1.2%
Pharmaceutical	1.0%
Retail, consumer products	1.0%
Retail, food and drink	1.0%
Chemical industry	0.8%
Construction/real estate	0.6%
Natural resources/mining	0.6%
Agriculture	0.4%
Food	0.4%
Gas and Oil	0.4%
Water	0.4%
Emergency services	0.2%
Other	7.0%

7) What is the total number of employees in your entire organization (please include all plants, divisions, branches, parents and subsidiaries worldwide)? (Base: 500)

100,000 or more	6.2%
50,000-99,999	8.2%
30,000-49,999	6.2%
20,000-29,999	1.4 %
10,000-19,999	6.8%
7,500-9,999	2.8%

5,000-7,499	4.6%
2,500-4,999	14.6%
1,000-2,499	12.0%
500-999	11.4%
100-499	10.4%
Under 100	14.6%

8) Please estimate the number of information security personnel employed and outsourced by your organization (Base: 500)

None	7.6%
1-19	57.4%
20-49	9.4%
50-99	5.4%
100-500	7.0%
500-1,000	2.6%
Over 1,000	2.8%
Don't know	7.8%

9a) What was your organizations approximate annual budget for information and corporate/physical security products, systems, services and/or staff in 2003? (Base: 500)

Over \$250 million	2.4%
\$100 to \$249.9 million	1.6%
\$50 to \$99.9 million	1.0%
\$25 to \$49.9 million	0.8%
\$10 to \$24.9 million	5.6%
\$5 to \$9.9 million	3.8%
\$1 to \$4.9 million	13.8%
\$500,000 to \$999,999	5.4%
\$250,000 to \$499,999	7.0 %
\$100,000 to \$249,999	14.2%
\$50,000 to \$99,999	6.8%
Less then \$50,000	15.8%
Don't Know	21.8%

9b) This figure applies to: (Base: 391 – respondents providing figure)

Information security spending only	37.1%
Physical or corporate security spending only	2.6%
Combined security spending	60.4%

Section Two: Electronic Crimes

1) Did the total number of electronic crimes and network, systems or data intrusions experienced by your organization increase, decrease or remain the same in 2003 compared to 2002? (Base: 500)

Increase	42.6%
Decrease	6.2%
No change	23.0%
Don't know	28.2%

2) Please estimate the total number of electronic crimes or network, system or data intrusions experienced by your organization in 2003
(Base: 485 – respondents providing answer)

None	29.5%
1-9	25.3%
10-49	19.8%
50-99	5.1%
100-249	9.0%
250 or more	11.1%
Mean	136
Median	5

3) How many of these electronic crimes or network, system or data intrusions are suspected to have been caused by:

Outsiders (non-employees or contractors)

(Base: 342 – respondents whose organization experienced any electronic crime)

None	7.0%
1-9	31.6%
10-49	14.0%
50-99	4.0%
100-249	5.8%
250 or more	8.1%
Mean	125
Median	5
Don't know	29.5%

Insiders (current or former employees or contractors)

(Base: 342 – respondents whose organization experienced any electronic crime)

None	29.5%
1-9	22.2%

10-49	11.4%
50-99	3.8%
100-249	2.0%
250 or more	1.6%
Mean	20
Median	1
Don't know	29.5%

3a) Average percent of e-Crimes or intrusions caused by outsiders vs. insiders
(Base: 342 – respondents whose organization experienced any electronic crime)

Outsiders	71.4%
Insiders	28.6%

4) Which of the following electronic crimes were committed against your organization in 2003?
(Check all that apply)
(Base: 342 – respondents whose organization experienced any electronic crime)

Virus or other malicious attack	77.2%
Denial of service attack	43.6 %
Illegal generation of SPAM email	38.3%
Unauthorized access by an <u>insider</u>	35.7%
Phishing	31.0%
Unauthorized access by an <u>outsider</u>	27.2%
Fraud	21.9%
Theft of intellectual property	20.5%
Theft of other proprietary info	16.4%
Employee identity theft	12.0%
Sabotage by an <u>insider</u>	10.8%
Sabotage by an <u>outsider</u>	10.8%
Extortion by an <u>outsider</u>	3.2%
Extortion by an <u>insider</u>	2.6%
Other	11.1%
Don't know	7.9%

5) Does your organization have a formal process in place for tracking e-crime attempts?
(Base: 500)

Yes	51.0%
No	37.2%
Not sure	11.8%

6) Does your organization have a formalized plan outlining policies and procedures for reporting and responding to e-crimes committed against your organization? (Base: 500)

Yes	49.8%
No, planning to implement plan within the next 12 months	23.4%
No plans for formalized plan at this time	17.2%
Don't know	9.6%

7) Does your organization have an incident response team? (Base: 500)

Yes	67.4%
No	27.0%
Don't know	5.6%

7a) Which of the following groups or departments are represented on your organization's incident response team? (Base: 337 – respondents with incident response team)

MIS, IT, IS, computer or networking	83.1%
Information security	73.9%
Senior management	59.9%
Physical or corporate security	54.3%
Legal or contracts	45.4%
Human resources	37.7%
Public relations	28.5%
Accounting, finance or purchasing	16.3%
Executive committee	13.9%
General administration	8.9%
Manufacturing, production or operations	7.4%
Board of directors	5.0%
Other	9.5%
Don't know	6.2%

8) Which of the following groups posed the greatest cyber security threat to your organization in 2003? (Base: 500)

Hackers	40.4%
Current employees	22.2%
Former employees	5.6%
Current service providers/contractors/consultants	3.2%
Customers	2.4%
Foreign entities	2.4%
Competitors	2.0%
Terrorists	1.0%
Former service providers/contractors/consultants	0.8%
Suppliers/Business Partners	0.2%
Information Brokers	0.2%
Don't know	19.6%

9) How effective do you consider each of the following technologies in place at your organization in detecting and/or countering misuse or abuse of computer systems and networks?

Technologies in use (Base: 500)

Firewalls	98.2%
Physical security systems	94.2%
Manual patch management	91.0%
Encryption of critical data in transit	85.4%
Role-Based access control	85.4%
Intrusion detection systems monitored by person	81.0%
Information assurance technologies	76.4%
Automated patch management	74.4%
Intrusion detection systems monitored by automated systems w/ built-in alarms	74.0%
Encryption of critical data in storage	70.8%
Anti-Fraud technologies working with ERP/account payable/billing systems	63.0%
Two factor authentication	56.2%
Wireless monitoring	53.6%
Keystroke monitoring of individual users	39.4%

Top 5 most effective technologies (rated extremely or very effective)

(Base: respondents using that particular technology at organization)

1. Firewalls	71.3%
2. Encryption of critical data in transit	63.0%
3. Encryption of critical data in storage	55.9%
Two-factor authentication	55.5%
4. Intrusion detection systems monitored by automated systems w/built in alarms	51.4%
5. Physical security systems	47.8%

Top 5 least effective technologies (rated not very or not at all effective)

(Base: respondents using that particular technology at organization)

1. Manual patch management	23.1%
2. Wireless monitoring	19.8%
3. Keystroke monitoring of individual users	15.7%
4. Automated patch management	13.7%
5. Information assurance technologies	13.4%

10) In your opinion, how effective is each of the following security policies and procedures in preventing or reducing electronic crime at your organization? (Top 5)

Policies and procedures in use

(Base: 500)

(NET) Internal monitoring of employees*	94.6%
Written “inappropriate use” policy	94.0%
Require employees/contractors to sign acceptable use policies	89.8%
Monitor Internet connections	89.6%
Require internal reporting to management of misuse/abuse by insiders	89.2%
Employee education and awareness programs	88.6%
Corporate security policy	88.4%
New employee security training	88.4%
Periodic risk assessments	87.8%
Conduct regular security audits	87.6%
Employee/contractor background examinations	87.4%
Regular security communication from management	86.2%
Periodic systems penetration testing	84.6%
Use of an incident response team	78.2%
Include security in contract negotiations with vendors/suppliers	74.8%
Hired a Chief Security Officer (CSO)/ Chief Information Security Officer (CISO)	54.2%
Use of “white hat” hackers	53.8%
Government security clearances	51.6%
Polygraph examinations	31.0%

* (NET) Internal monitoring of employees includes: Monitor Internet connections, Employee monitoring, Storage & review of e-mail, Storage & review of computer files; Storage & review of voice mail; Record or review employee phone conversations.

Top 5 most effective policies/procedures (rated extremely or very effective)

Base: (500) respondents using that particular policy/procedure at organization

1. Conduct regular security audits	51.1%
2. Hire CSO or CISO	49.4%
3. Periodic systems penetration testing	48.5%
4. Monitor internet connections	46.0%
5. Periodic risk assessments	45.1%

Top 5 least effective policies/procedures (rated not very or not at all effective)

Base: (500) respondents using that particular policy/procedure at organization

1. Record or review employee phone conversations	25.6%
2. Storage and review of voice mail	25.0%
3. Polygraph exams	19.4%
Storage and review of computer files	19.0%
4. Require employees/contractors to sign acceptable use polices	18.3%
5. Written “inappropriate use” policy	17.2%
Regular security communication from management	17.2%

11) In your opinion have any of the following security policies and procedures led to the:

- a) Deterrence of a potential criminal?
- b) Detection of an e-criminal?
- c) Termination of an employee or contractor?
- d) Prosecution (civil or criminal) of an alleged criminal?

Disposition of policies/procedures (<i>Base: among those with policy/procedure in place</i>)	Deterrence	Detection	Termination	Prosecution	None	Don't know
Corporate security policy	61%	21%	16%	7%	11%	19%
New employee security training	61%	9%	4%	<1%	14%	22%
Employee education & awareness programs	60%	19%	12%	4%	12%	18%
Regular security communication from management	58%	10%	4%	1%	14%	23%
Require employees/contractors to sign acceptable use policies	55%	11%	14%	4%	11%	25%
Written "inappropriate use" policy	55%	15%	32%	5%	8%	16%
(NET) Internal monitoring of employees*	52%	50%	36%	11%	9%	15%
Include security in contract negotiations with vendors/suppliers	51%	16%	5%	2%	15%	26%
Hired a Chief Security Officer (CSO) or Chief Information Security Officer (CISO)	45%	25%	11%	8%	19%	30%
Require internal reporting to management of misuse or abuse by employees & contractors	44%	24%	20%	3%	12%	24%
Employee/contractor background examinations	43%	24%	10%	2%	14%	28%
Monitor Internet connections	41%	41%	25%	5%	12%	18%
Conduct regular security audits	40%	46%	10%	2%	11%	21%
Periodic risk assessments	38%	38%	3%	<1%	15%	23%
Employee monitoring	36%	32%	27%	8%	16%	22%
Storage & review of e-mail	36%	30%	22%	5%	16%	25%
Government security clearances	34%	16%	4%	2%	19%	37%
Use of "white hat" hackers	34%	23%	2%	1%	16%	36%
Storage & review of computer files	32%	36%	18%	6%	16%	25%
Periodic systems penetration testing	29%	42%	3%	<1%	16%	25%
Use of an incident response team	29%	35%	11%	8%	18%	25%
Storage & review of voice mail	24%	17%	5%	2%	23%	38%
Record or review employee phone conversations	20%	19%	8%	3%	23%	42%
Polygraph examinations	18%	14%	3%	3%	25%	46%

* (NET) Internal monitoring of employees includes: Monitor Internet connections, Employee monitoring, Storage & review of e-mail, Storage & review of computer files; Storage & review of voice mail; Record or review employee phone conversations.

12) How many electronic crimes committed against your organization in 2003 were uncovered by accident, as opposed to as a result of systems and/or policies that you have in place? (Base: 500)

Zero	25.2%
Less than 10%	16.8%
10-24%	9.0%
25-49%	6.8%
50-74%	7.2%
75-99%	2.8%
100%	5.0%
Don't know	27.2%

13) How knowledgeable do you consider yourself in understanding laws surrounding computer crimes? (Base: 500)

Knowledge level regarding laws surrounding computer crimes	Very or extremely knowledgeable (NET)	Somewhat knowledgeable	Not knowledgeable	Somewhat or not knowledgeable (NET)	Don't know
In your state	38.8%	45.6%	13.4%	59.0%	2.2%
In the United States	33.4%	50.2%	14.2%	64.4%	2.2%
Worldwide	8.4%	40.2%	41.6%	81.8%	9.8%

14) What is the total monetary value of losses your organization sustained due to electronic crimes or system intrusions in 2003?

We do not track monetary losses due to electronic or related crimes (Base: 500) 32.4%

(Base: 338)

\$100 million or more	0.3%
\$10 million to \$99.9 million	2.4%
\$1 million to \$9.9 million	5.0%
\$500,000 to \$999,999	5.0%
\$100,000 to \$499,999	11.2%
Less than \$100,000	26.3%
Don't know/not sure	49.7%

Mean	\$3,920,000
Median	\$100,000
Sum*	\$666,000,000

*Sum figure calculated using midpoints within each range.

15) Which of the following types of losses has your organization experienced in 2003?

No losses experienced in 2003 (Base: 500)	17.0%
(Base: 415)	
(NET) Operational losses	56.4%
Non-critical operational losses	50.4%
Critical operational losses	14.9%
(NET) Financial losses	24.6%
Non-critical financial losses	22.7%
Critical financial losses	2.9 %
Other	11.8%
Don't know	31.8%

16) How far back does your organization keep records on or otherwise track of network, data and system intrusions? (Base: 500)

1 year or less	17.8%
More than 1 year to 2 years	12.8%
More than 2 years to 5 years	13.0%
5 years or longer	10.8 %
Don't know	25.6%
Not applicable-does not track	20.5%

Section 3: Insider Threats

1) Please indicate all sources of insider intrusions in 2003 (Check all that apply)

(Base: 140 – respondents whose organization has experienced intrusions from insiders)

Current employees not in management positions at the time of the intrusion	72.9%
Current employees in management positions at the time of the intrusion	37.9%
Current contractors/temporary employees at the time of the intrusion	32.9%
Former employees previously employed in non-management positions	30.7%
Former contractors/temporary employees	15.0%
Former employees previously employed in management positions	13.6%
Don't know/Not sure	8.6 %

2) Average percentage of internal intrusions

(Base: 140 – respondents whose organization has experienced intrusions from insiders)

Handled internally without involving legal action or law enforcement?	71.7%
NET (handled with help of law enforcement or other legal action)	49.3%
Handled internally with legal action?	17.9%
Handled with the help of law enforcement?	13.0%
Handled externally by filing a civil action?	1.6%
Don't know	4.3%

3) For insider intrusions not referred for any legal action please indicate the reason why?
(Check all that apply)

(Base: 140 – respondents whose organization has experienced intrusions from insiders)

Damage level insufficient to warrant prosecution	57.9%
Lack of evidence/not enough information to prosecute	36.4%
Concerns about negative publicity	27.1%
Concerns that competitors would use incident to their advantage	11.4%
Prior negative response from law enforcement	7.1%
Unaware that we could report these crimes	0.7%
Other	16.4%
Don't know	7.1%

4) Does your organization monitor its computer systems and networks for misuse or abuse by employees or contractors? (Base: 500)

Yes	80.4%
Yes, systems only	4.8%
Yes, networks only	8.4%
Yes, both	67.2%
No	13.4%
Don't know	6.2%

5) Does your organization require internal reporting of misuse or abuse of computer access by employees or contractors? (Base: 500)

Yes	71.8%
No	18.0%
Don't know	10.2%

6) Does your organization have a written “inappropriate use” security policy for use of networks, data, and systems? (Base: 500)

Yes, policy currently in place	82.0%
No	6.6%
Policy pending	7.4%
Don't know	4.0%

7) Are employees required to review and accept the written inappropriate use policy on any periodic Bases? (Check all that apply)

(Base: 410 – those with written inappropriate use policy in place)

No	12.2%
Yes, upon employment	54.9%

Yes, upon accessing data	11.2%
Yes, every six months	1.2%
Yes, annually	27.6%
Yes, periodically	13.4%
Don't know	2.9%

8) How does your organization communicate the inappropriate use policy to its employees and contactors? (Check all that apply)

(Base: 410 – those with written inappropriate use policy in place)

Hardcopy distribution	57.3 %
Electronic mail	48.3 %
Web reference	43.7%
Direct communications from managers	34.6%
Training materials	32.4%
Training classes	26.8%
Other	4.6%
Don't know	3.7%

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

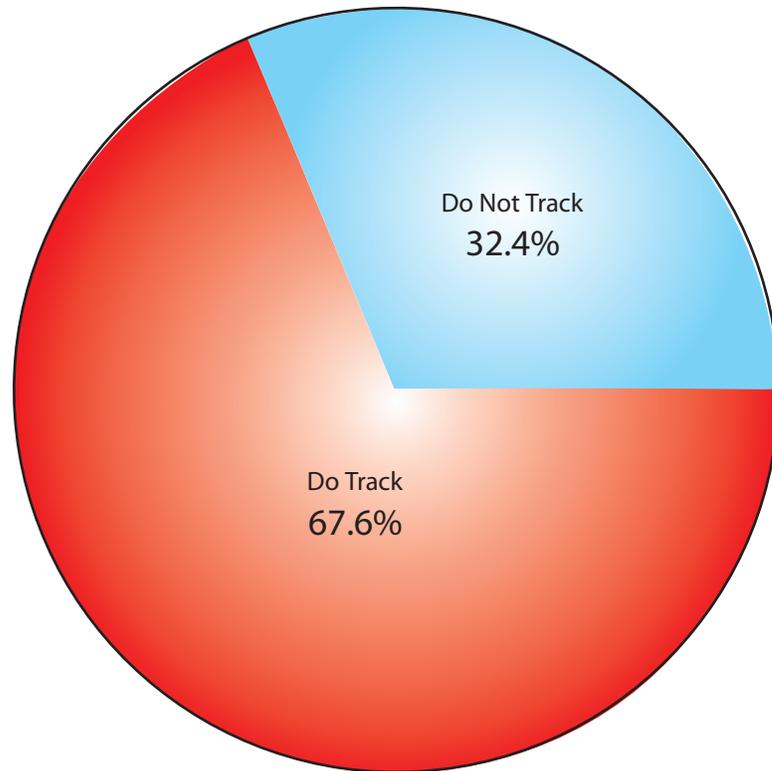
(Base: 480 – total with policy)

Monthly	2.1%
Every 6 months	7.1%
Annually	24.2%
As needed	47.5%
Other	2.9%
Don't know	16.3%

10) With respect to your organization, what is the most adverse consequence that has ever occurred from an insider network, data, or system intrusion? (Base: 500)

Critical disruption to organization only	24.6%
Harm to organization's reputation	15.2%
Loss of current or future revenue	7.0%
Critical system disruption affecting customers & business partners	7.0%
Loss of customers	3.0%
Critical system disruption, affecting the larger critical infrastructure	1.8%
Personal injury	0.4%
No impact	41.0%

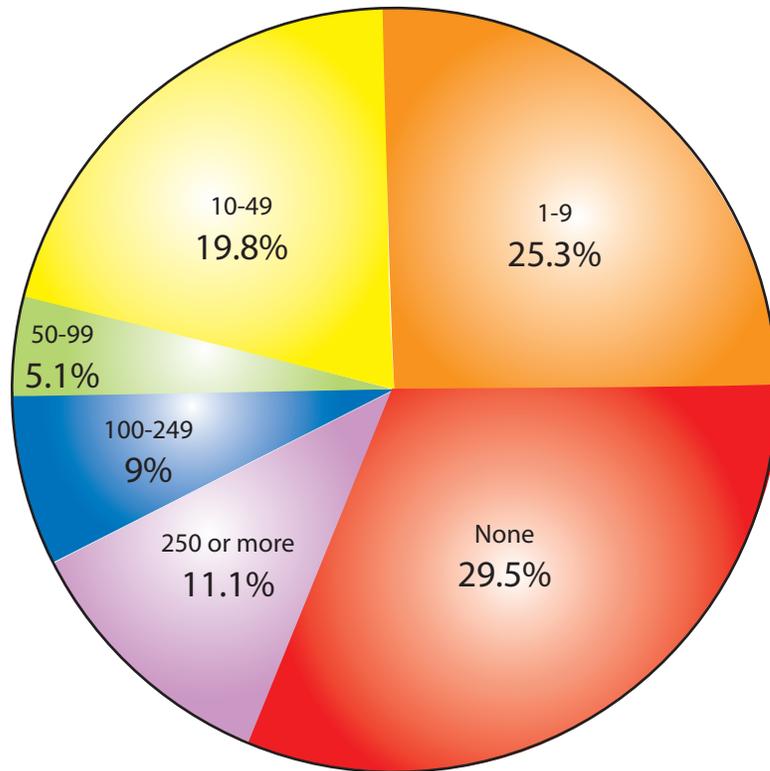
Percentage of Companies Tracking Monetary Loss Due to Electronic Crime or System Intrusion



Estimated E-crime Dollar Loss in 2003: \$666 million

Source: CSO Magazine/US Secret Service/CERT Coordination Center
Base: 500

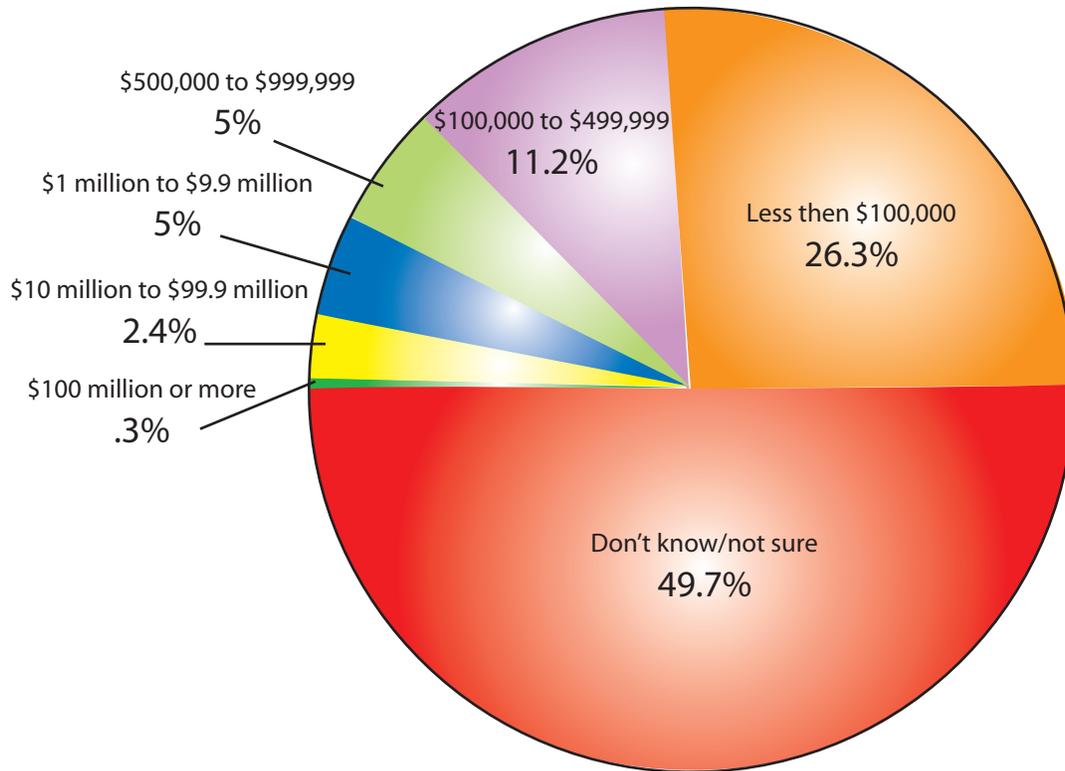
2003 Estimated Number of Electronic Crimes or Network, System or Data Intrusions Experienced by Organizations



Average Number of E-crimes or Intrusions: 136

Source: CSO Magazine/US Secret Service/CERT Coordination Center
Base: 485

2003 Dollar Loss Due to Electronic Crimes or System Intrusion



Estimated E-crime Dollar Loss in 2003: \$666 million

Source: CSO Magazine/US Secret Service/CERT Coordination Center
Base: 338