2005 E-Crime Watch Survey – Survey Results

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

OVERALL RESULTS

E-Crime Watch Survey:	2005
Field Dates:	3/3/05 – 3/14/05
Total completed surveys:	819
Margin of Error:	+/- 3.4%

NOTE TO EDITOR

For the purpose of this survey, electronic crime, intrusion, insider and outsider are defined as follows:

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

The results comprised within this document represent an overview of findings. The survey was conducted online and designed to skip questions that were not relevant or to ask follow-up questions based on previous responses. Please note that prompts were provided to remind respondents of previous answers. Please do not assume questions as laid out in this document are presented exactly as respondents viewed them online.

SECTION ONE: RESPONDENT PROFILE

1) In which category does your organization fall?

Private sector	62%
Government	23%
Law enforcement/Prosecutor	14%

2) Are you, your organization or another individual at your organization currently a member of a United States Secret Service Electronic Crimes Task Force (ECTF) or Working Group (ECWG)?

Yes	33%
No	52%
Don't know/not sure	15%

3) To which of the following Electronic Crimes Task Force (ECTF) or Working Group (ECWG) do you belong to? (Base: 267 – ECTF or ECWG members only)

San Francisco	18%
Chicago	13%
New York	13%
Los Angeles	11%
Boston	6%
Charlotte	6%
Dallas	6%
Washington DC	6%
Birmingham	5%
Cleveland	5%
Las Vegas	4%
Miami	3%
Orlando	3%
Oklahoma City Tulsa	2%
Philadelphia	1%
Houston	<1%
Minneapolis	<1%

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

Government	25%
Information & Telecommunications	18%
Banking & Finance	14%
Public Health	5%
Defense Industrial Base	4%
Emergency Services	4%
Transportation	3%
Energy	2%
Food	2%
Chemical Industry and Hazardous Materials	1%
Postal & Shipping	1%
Agriculture	<1%
Water	<1%
Not applicable	20%

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

Law enforcement/security (non-emergency services)	15%
Information & telecommunications	12%
Banking & Finance	11%
Government	8%
Education	7%
Electronics/Technology	5%
Health Care	5%
Military	4%
Services	4%
Insurance	3%
Retail, consumer products	3%
Defense Industrial Base	2%
Emergency Services	2%
Research/Development	2%
Transportation	2%
Agriculture	1%
Chemical	1%
Construction/Real Estate	1%
Electric Power	1%
Food	1%
Gas & Oil	1%
Pharmaceutical	1%
Postal and Shipping	1%
Retail, food/drink	1%
Wholesale	1%
Hazardous Materials	<1%
Natural Resources/Mining	<1%
Water	<1%
Other	9%

6) 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	8%
10,000 – 99,999	24%
1,000 – 9,999	31%
500-999	8%
100-499	13%
Under 100	15%
Don't know	1%

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

IS/IT/networking management	29%
Security management	29%
Non-IT management	11%
Law enforcement	17%
Other	14%

8) What was your organization's approximate annual budget for information and corporate/physical security products, systems, services and/or staff in 2004? Please break out for:

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

Over $100 Million	4%
$10 Million - $99.9 Million	5%
$ 1 Million - $9.9 Million	15%
$500,000 - $999,999	4%
$250,000 - $499,999	5%
$100,000 - $249,999	10%
$50,000 - $99,999	9%
Less than $50,000	18%
Don't know	30%

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 $100 Million	3%
$10 Million - $99.9 Million	7%
$ 1 Million - $9.9 Million	12%
$500,000 - $999,999	4%
$250,000 - $499,999	5%
$100,000 - $249,999	7%
$50,000 - $99,999	8%
Less than $50,000	18%
Don't know	36%

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

Over $100 Million	2%
$10 Million - $99.9 Million	5%
$ 1 Million - $9.9 Million	12%
$500,000 - $999,999	4%
$250,000 - $499,999	4%
$100,000 - $249,999	6%
$50,000 - $99,999	7%
Less than $50,000	18%
Don't know	42%

9) What is the number of staff assigned to cyber crime investigations or forensics within your organization?

Full-time (Base = 142 – law enforcement/prosecutor sector/job title only)

None	26%
1	20%
2	18%
3	6%
4	6%
5 or more	24%
Mean	7
Median	2

Percents calculated on total respondent base of 819 unless otherwise specified.
Percent may not sum to 100 due to rounding.

Part-time (Base = 142 – law enforcement/prosecutor sector/job title only)

None	58%
1	19%
2	8%
3	3%
4	4%
5 or more	8%
Mean	3
Median	-

10) What is the average time period between when a case is initiated to its referral for prosecution? (Base = 142 – law enforcement/prosecutor sector/job title only)

Less than 5 weeks	13%
5 weeks – 12 weeks	46%
13 weeks – 30 weeks	21%
31 weeks – 52 weeks	16%
Over 52 weeks	4%

11) Which of the following factors contribute to significant time lags from the initiation of a case to its referral for prosecution? (Base = 142 – law enforcement/prosecutor sector/job title only. Check all that apply.)

Volume of cases compared to trained investigators	68%
Forensic processing backlogs	56%
Dependencies on other investigative agencies	41%
Other	16%

12) Considering your electronic crime related caseload only, in which five (5) areas would you say the majority of your agency's time is spent? (Base = 142 – law enforcement/prosecutor sector/job title only. Check all that apply.)

Fraud	87%
Identity theft	80%
Child exploitation	62%
Email threats	44%
Network intrusion	26%
Intellectual property crimes	24%
Phishing	24%
Narcotics	20%
Unauthorized information disclosure	16%
Spam email	11%
Denial of service	11%
Online extortion	7%
Other	16%

13) Considering your electronic crime related caseload only, in which ONE area would you say the MOST amount of your agency's time is spent? (Base = 142 – law enforcement/prosecutor sector/job title only)

Fraud	30%
Child exploitation	28%
Identity theft	18%
Network Intrusion	3%
Narcotics	3%
Intellectual property crimes	2%
Spam email	2%
Email threats	2%
Unauthorized information disclosure	1%
Phishing	1%
Online extortion	1%
Other	8%

14) Are you personally involved in any of the following at your organization? (Check all that apply)

Decisions regarding information security	73%
Decisions regarding referral of potential electronic crime to law enforcement	55%
Investigations or prosecution of electronic crime	55%
Decisions regarding corporate/physical security	49%
Audit reporting concerning fraud or electronic crimes	46%
None of the above	6%

15) How knowledgeable do you consider yourself in understanding laws surrounding computer crimes?

(Scale: Extremely knowledgeable, Very knowledgeable, Somewhat knowledgeable, Not knowledgeable, Don't know/not sure)

Extremely or Very Knowledgeable

In your state	37%
In the United States	31%
Worldwide	7%

Not Knowledgeable

In your state	11%
In the United States	12%
Worldwide	46%

SECTION TWO: ELECTRONIC CRIMES

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

Increased	35%
Decreased	13%
No Change	30%
Don't know/not sure	22%

2) Please estimate the total number of electronic crimes or network, system or data intrusions experienced by your organization in 2004. (Base: 816 – those responding only)

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

None	32%
1-9	32%
10-49	18%
50-99	5%
100-24	6%
250 or more	7%
Mean	86
Median	3

3) You indicated that your organization experienced X intrusions in 2004. How many of these electronic crimes or network, system or data intrusions are known or suspected to have been caused by:

Outsiders (Base: 554 – those experiencing 1+ electronic crimes or intrusions only)

None	4%
1-9	42%
10-49	19%
50-99	5%
100-249	4%
250 or more	7%
Mean	102
Median	5
Don't know	19%

Insiders (Base: 554 – those experiencing 1+ electronic crimes or intrusions only)

None	43%
1-9	24%
10-49	10%
50-99	2%
100-249	2%
250 or more	-
Mean	10
Median	-
Don't know	19%

4) Mean Percent of E-Crimes Caused by Outsiders vs. Insiders: (Base: 554 – those experiencing 1+ electronic crimes or intrusions only)

Outsiders	80%
Insiders	20%
Don't know	19%

5) Which of the following electronic crimes were committed against your organization in 2004? (Base: 554 – those experiencing 1+ electronic crimes or intrusions only. Check all that apply)

Virus or other malicious code	82%
Spyware	61%
Phishing	57%
Illegal generation of spam email	48%
Unauthorized access to information, systems or networks	43%
Denial of service attacks	32%
Rogue wireless access point	21%
Exposure of private or sensitive information	19%
Fraud	19%
(2004: Employee) Identity theft	17%
Password sniffing	16%
Theft of intellectual property	14%
Zombie machines on organization's network	13%
Theft of other (proprietary) info	12%
Sabotage	11%
Web site defacement	9%
Extortion	2%
Other	4%
Don't know/not sure	3%

6) You indicated the following types of electronic crimes were committed against your organization last year. Please indicate the source of these crimes, if known: (Check all that apply)

<u>Outsider</u>

Phishing (Base: 316)	92%
Web site defacement (Base: 50)	92%
Spyware (Base: 338)	89%
Illegal generation of spam email (Base: 266)	89%
Denial of service attacks (Base: 179)	88%
Virus or other malicious code (Base: 453)	85%
Identity theft (Base: 95)	81%
Fraud (Base: 105)	80%
Zombie machines on organization's network (Base: 73)	77%
Password sniffing (Base: 86)	74%
Extortion (Base: 10)	60%
Sabotage (Base: 61)	59%
Unauthorized access to information, systems or networks (Base: 237)	58%
Theft of other (proprietary) info (Base: 65)	54%
Exposure of private or sensitive info (Base: 106)	47%
Theft of intellectual property (Base: 75)	33%
Rogue wireless access point (Base: 117)	29%

Insider
Rogue wireless access point (Base: 117) 72%
Theft of intellectual property (Base: 75) 64%
Exposure of private or sensitive info (Base: 106) 56%
Theft of other (proprietary) info (Base: 65) 55%
Unauthorized access to information, systems or networks (Base: 237) 54%
Sabotage (Base: 61) 44%
Fraud (Base: 105) 35%
Password sniffing (Base: 86) 34%
Extortion (Base: 10) 30%
Identity theft (Base: 95) 23%
Zombie machines on organization's network (Base: 73) 20%
Spyware (Base: 338) 11%
Illegal generation of spam email (Base: 266) 11%
Denial of service attacks (Base: 179) 11%
Web site defacement (Base: 50) 6%
Phishing (Base: 316) 2%
Virus or other malicious code (Base: 453) 14%

Unknown
Theft of intellectual property (Base: 75) 16%
Identity theft (Base: 95) 12%
Virus or other malicious code (Base: 453) 10%
Extortion (Base: 10) 10%
Zombie machines on organization's network (Base: 73) 10%
Exposure of private or sensitive info (Base: 106) 9%
Theft of other (proprietary) info (Base: 65) 9%
Illegal generation of spam email (Base: 266) 8%
Denial of service attacks (Base: 179) 8%
Rogue wireless access point (Base: 117) 8%
Sabotage (Base: 61) 8%
Unauthorized access to information, systems or networks (Base: 237) 8%
Spyware (Base: 338) 7%
Phishing (Base: 316) 7%
Web site defacement (Base: 50) 6%
Fraud (Base: 105) 5%
Password sniffing (Base: 86) 4%

7) You indicated your organization experienced X intrusions in 2004. How many of these intrusions were handled:

Internally without involving legal action or law enforcement
None 6%
1 ..... 6%
2 ..... 9%
3-5 ..... 19%
6-9 ..... 7%
10-24 ..... 16%
25 or more 22%
Mean 84
Median 6
Don't know 16%

Internally with legal action

None	69%
1	4%
2	4%
3-5	3%
6-9	1%
10-24	2%
25 or more	3%
Mean	5
Median	-
Don't know	16%

With the help of law enforcement

None	65%
1	7%
2	2%
3-5	4%
6-9	1%
10-24	3%
25 or more	2%
Mean	5
Median	-
Don't know	16%

Externally by filing a civil action

None	80%
1	4%
2	1%
3-5	1%
6-9	-
10-24	-
25 or more	1%
Mean	<1
Median	-
Don't know	16%

8) If any intrusions were not referred for legal action, please indicate the reason(s) not referred: (Base: 554 – those experiencing 1+ electronic crimes or intrusions only. Check all that apply)

Damage level insufficient to warrant prosecution	59%
Lack of evidence/not enough info to prosecute	50%
Concerns about negative publicity	15%
Concerns that competitors would use to advantage	7%
Unaware we could report these crimes	6%
Prior negative response from law enforcement	6%
Other	14%
Don't know	7%

9) Which of the following types of losses did your organization experience in 2004? (Base: 554 – those experiencing 1+ electronic crimes or intrusions only. Check all that apply)

Non-critical operational losses	50%
Non-critical financial losses	26%
Harm to reputation	12%
Critical operational losses	11%
Critical financial loss	2%
Loss of life	1%
Other	6%
Not applicable – no losses experienced	17%
Don't know/not sure	17%

10) Please estimate the total monetary value of losses your organization sustained due to electronic crimes or system intrusions in 2004: (Base: 777 – those answering only)

$10 million or more	1%
$1 million - $9.9 million	2%
$500,000 - $999,999	1%
$100,000 - $499,999	4%
Less than $100,000	31%
Mean	$506,670
Median	-
Sum	$150,000,000
Don't know/not sure	62%

11) In 2004, did monetary losses to your organization from electronic crime increase, decrease or remain the same compared to 2003? (Base: 723 – those answering only)

Increase	22%
Decrease	10%
Remain the same	21%
Not sure	47%

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

Increase	26%
Decrease	13%
Remain the same	27%
Not sure	34%

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

Increase	88%
Decrease	1%
Remain the same	4%
Not sure	7%

14) Which of the following groups posed the greatest cyber security threat to your organization in 2004?

Hackers	37%
Current employees	18%
Foreign entities	6%
Former employees	5%
Information brokers	3%
Current service providers/consultants/contractors	2%
Terrorists	2%
Customers	2%
Suppliers/business partners	1%
Competitors	1%
Former service providers/consultants/contractors	1%
Don't know/not sure	21%

15) Does your organization have a formal process or system in place for tracking e-crime attempts?

Yes	52%
No	31%
Don't know/not sure	18%

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

1 year or less	21%
More than 1 year to 2 years	13%
More than 2 years to 5 years	16%
5 years or longer	9%
Don't know	31%
Not applicable/Does not track	10%

17) Does your organization have a formalized plan outlining policies and procedures for reporting and responding to e-crimes committed against your organization?

Yes	46%
No, planning to implement next 12 months	18%
No plans at this time	21%
Don't know/not sure	15%

18) 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? (Check all that apply)

(Scale: Extremely effective, Very effective, Somewhat effective, Not very effective, Not at all effective, Don't know, Not applicable/Do not use)

Technologies in Use

Firewalls	99%
Automated virus scanning	99%
Physical security systems (Electronic access control systems, badging systems, CCTV, etc.)	94%
Spyware/adware detection software	93%
Intrusion detection systems	91%
Manual patch management	90%
Network traffic monitoring/ network based forensic tools	88%
Encryption	87%
Automated patch management	86%
Configuration management/periodic checks for non-baseline files to detect Trojan horses, logic bombs, etc.	86%
Technologies tracking access & use of corporate data/Information assurance technologies	83%
Role-based access control	83%
Anti-fraud technologies working with ERP/accounts payable & billing systems	68%
Wireless monitoring	66%
Two-factor authentication (using biometrics, smart cards, etc.)	63%
Keystroke monitoring of individual users	53%

Most Effective (Extremely or Very Effective) Technologies in Use (Base: respondents with technology in use)

Firewalls (Base: 810)	68%
Automated virus scanning (Base: 810)	66%
Encryption (Base: 715)	58%
Two-factor authentication (using biometrics, smart cards, etc.) (Base: 517)	56%
Intrusion detection systems (Base: 743)	50%
Physical security systems (Electronic access control systems, badging systems, CCTV, etc.) (Base: 771)	49%
Network traffic monitoring/ network based forensic tools (Base: 722)	46%
Spyware/adware detection software (Base: 758)	43%
Role-based access control (Base: 677)	42%
Automated patch management (Base: 704)	40%
Configuration mgmt/periodic checks for non-baseline files to detect Trojan horses, logic bombs, etc. (Base: 704)	39%
Technologies tracking access & use of corporate data/Info assurance technologies (Base: 682)	35%
Anti-fraud technologies working with ERP/accounts payable & billing systems (Base: 560)	28%
Wireless monitoring (Base: 544)	26%
Keystroke monitoring of individual users (Base: 434)	22%
Manual patch management (Base: 741)	21%

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

Manual patch management (Base: 741) 26%
Keystroke monitoring of individual users (Base: 434) 22%
Wireless monitoring (Base: 544) 15%
Spyware/adware detection software (Base: 758) 12%
Technologies tracking access & use of corporate data/Info assurance technologies (Base: 682) 12%
Physical security systems (Electronic access control systems, badging systems, CCTV, etc.) (Base: 771) 8%
Automated patch management (Base: 704) 7%
Anti-fraud technologies working with ERP/accounts payable & billing systems (Base: 560) 6%
Configuration mgmt/periodic checks for non-baseline files to detect Trojan horses, logic bombs, etc. (Base: 704) 6%
Network traffic monitoring/ network based forensic tools (Base: 722) 6%
Two-factor authentication (using biometrics, smart cards, etc.) (Base: 517) 6%
Intrusion detection systems (Base: 743) 5%
Role-based access control (Base: 677) 5%
Encryption (Base: 715) 4%
Automated virus scanning (Base: 810) 3%
Firewalls (Base: 810) 2%

19) Which of the following security policies and procedures does your organization use to attempt to prevent or reduce electronic crime? (Check all that apply)

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

20) Have any security policies and procedures at your organization supported or played a role in the deterrence, detection, termination or prosecution of an individual? (Base: 751 – among those organizations using 1+ policy/procedure to prevent/reduce electronic crime only)

Yes 61%
No 15%
Don't know/not sure 24%

21) In your opinion, have any of the following security policies and procedures at your organization supported or played a role in the…(Check all that apply per row)

Deterrence of a potential e-criminal? (Base: respondents with policy/procedure in place)

New employee security training (Base: 379) 80%
Regular security communication from management (Base: 272)..... 80%
Employee education & awareness programs (Base: 550) 78%
Require employees/contractors to sign acceptable use policies (Base: 486) 74%
Segregation of duties (Base: 355) 73%
Account/password management policies (Base: 609)..... 72%
Include security in contract negotiations with vendors/suppliers (Base: 274) 72%
Formal "inappropriate use" policy (Base: 584)..... 70%
Corporate security policy (Base: 504)..... 69%
Hired a CSO or CISO (Base: 194)..... 67%
Mandatory internal reporting to management of misuse or abuse by employees & contractors (Base: 285).... 66%
Random security audits (Base: 331)..... 61%
Employee/contractor background examinations (Base: 397) 60%
Government security clearances (Base: 182)..... 58%
Employee monitoring (Base: 344) 57%
Storage & review of e-mail or computer files (Base: 244) 56%
Monitor Internet connections (Base: 536)..... 52%
Conduct regular security audits (Base: 466) 51%
Periodic risk assessments (Base: 448) 51%
Periodic systems penetration testing (Base: 364) 48%
Use of "white hat" hackers (Base: 119) 46%
Use of incident response team (Base: 274)..... 42%

Detection of an e-criminal? (Base: respondents with policy/procedure in place)

Use of "white hat" hackers (Base: 119) 59%
Monitor Internet connections (Base: 536)..... 56%
Random security audits (Base: 331)..... 52%
Conduct regular security audits (Base: 466)..... 51%
Periodic systems penetration testing (Base: 364) 50%
Employee monitoring (Base: 344) 50%
Use of incident response team (Base: 274)..... 49%
Storage & review of e-mail or computer files (Base: 244) 48%
Periodic risk assessments (Base: 448)..... 43%
Mandatory internal reporting to management of misuse or abuse by employees & contractors (Base: 285).... 39%
Hired a CSO or CISO (Base: 194)..... 38%
Employee/contractor background examinations (Base: 397) 30%
Segregation of duties (Base: 355) 28%
Account/password management policies (Base: 609)..... 27%
Corporate security policy (Base: 504)..... 20%
Government security clearances (Base: 182)..... 20%
Formal "inappropriate use" policy (Base: 584)..... 19%
Employee education & awareness programs (Base: 550) 17%
Include security in contract negotiations with vendors/suppliers (Base: 274) 17%
Require employees/contractors to sign acceptable use policies (Base: 486) 14%
Regular security communication from management (Base: 272)..... 11%
New employee security training (Base: 379) 9%

Termination of an employee or contractor? (Base: respondents with policy/procedure in place)

Employee monitoring (Base: 344) 37%
Storage & review of e-mail or computer files (Base: 244) 34%
Formal "inappropriate use" policy (Base: 584) 32%
Mandatory internal reporting to management of misuse or abuse by employees & contractors (Base: 285) ... 32%
Monitor Internet connections (Base: 536) 31%
Corporate security policy (Base: 504) 27%
Require employees/contractors to sign acceptable use policies (Base: 486) 24%
Use of incident response team (Base: 274) 22%
Conduct regular security audits (Base: 466) 17%
Employee/contractor background examinations (Base: 397) 16%
Hired a CSO or CISO (Base: 194) 16%
Random security audits (Base: 331) 14%
Include security in contract negotiations with vendors/suppliers (Base: 274) 11%
New employee security training (Base: 379) 9%
Government security clearances (Base: 182) 8%
Employee education & awareness programs (Base: 550) 7%
Segregation of duties (Base: 355) 7%
Account/password management policies (Base: 609) 6%
Periodic risk assessments (Base: 448) 5%
Periodic systems penetration testing (Base: 364) 5%
Use of "white hat" hackers (Base: 119) 3%
Regular security communication from management (Base: 272) 2%

Prosecution of an alleged criminal? (Base: respondents with policy/procedure in place)

Use of incident response team (Base: 274) 15%
Hired a CSO or CISO (Base: 194) 13%
Storage & review of e-mail or computer files (Base: 244) 12%
Employee monitoring (Base: 344) 11%
Corporate security policy (Base: 504) 10%
Mandatory internal reporting to management of misuse or abuse by employees & contractors (Base: 285) ... 10%
Require employees/contractors to sign acceptable use policies (Base: 486) 7%
Conduct regular security audits (Base: 466) 7%
Use of "white hat" hackers (Base: 119) 7%
Formal "inappropriate use" policy (Base: 584) 6%
Monitor Internet connections (Base: 536) 6%
Random security audits (Base: 331) 5%
Include security in contract negotiations with vendors/suppliers (Base: 274) 5%
Account/password management policies (Base: 609) 4%
Government security clearances (Base: 182) 4%
Employee education & awareness programs (Base: 550) 3%
Employee/contractor background examinations (Base: 397) 3%
New employee security training (Base: 379) 3%
Segregation of duties (Base: 355) 3%
Periodic risk assessments (Base: 448) 2%
Periodic systems penetration testing (Base: 364) 2%
Regular security communication from management (Base: 272) 2%

Don't know (Base: respondents with policy/procedure in place)

Government security clearances (Base: 182) 29%
Employee/contractor background examinations (Base: 397) 24%
Hired a CSO or CISO (Base: 194) 24%
Periodic risk assessments (Base: 448) 22%
Periodic systems penetration testing (Base: 364) 20%
Include security in contract negotiations with vendors/suppliers (Base: 274) 20%
Require employees/contractors to sign acceptable use policies (Base: 486) 19%
Use of incident response team (Base: 274) 19%
Account/password management policies (Base: 609) 18%
Conduct regular security audits (Base: 466) 18%
Storage & review of e-mail or computer files (Base: 244) 18%
Corporate security policy (Base: 504) 17%
Segregation of duties (Base: 355) 17%
Employee education & awareness programs (Base: 550) 16%
New employee security training (Base: 379) 16%
Regular security communication from management (Base: 272) 16%
Monitor Internet connections (Base: 536) 15%
Use of "white hat" hackers (Base: 119) 15%
Random security audits (Base: 331) 14%
Mandatory internal reporting to management of misuse or abuse by employees & contractors (Base: 285) ... 14%
Formal "inappropriate use" policy (Base: 584) 13%
Employee monitoring (Base: 344) 12%

SECTION THREE: INSIDER THREATS

1) Does your organization monitor its computer systems and networks for misuse or abuse by employees or contractors?

Yes, systems only	5%
Yes, networks only	11%
Yes, both systems & networks	64%
No	12%
Don't know/not sure	7%

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

Yes	69%
No	20%
Don't know/not sure	11%

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

Yes	83%
No	6%
Policy pending	7%
Don't know/not sure	3%

4) Are employees required to review and accept the written inappropriate use policy on any periodic basis? (Base: 681 – those with inappropriate use policy in place only. Check all that apply)

Upon employment	54%
Upon accessing data	9%
Every six months	1%
Annually	27%
Periodically	14%
No	12%
Don't know/not sure	4%

5) How does your organization communicate the written inappropriate use policy to its employees and contractors? (Base: 681 – those with inappropriate use policy in place only. Check all that apply)

Hardcopy distribution	62%
Electronic mail	47%
Web reference	39%
Training materials	31%
Direct communication from managers	29%
Training classes	24%
Other	3%
Don't know	1%

6) How often does your organization review or update its security policy? (Base: 681 – those with inappropriate use policy in place only)

Every 6 months	5%
Annually	28%
As needed	46%
Other	2%
Don't know	19%

7) Please indicate all sources of insider intrusions in 2004 (Base: 214 – those experiencing insider intrusions. Check all that apply)

Current employees in non-managerial positions	52%
Current contractors or temporary employees	34%
Current employees in managerial positions	27%
Former employees in non-managerial positions	24%
Former employees in managerial positions	16%
Former contractors/temporary workers	13%
Don't know	22%

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

Critical system disruption to organization only	22%
Critical system disruption affecting customers and business partners	8%
Harm to organization's reputation	7%
Loss of current or future revenue	6%
Critical system disruption affecting the larger critical infrastructure sector	4%
Loss of customers	3%
Loss of business partners	<1%
Loss of life	<1%
Personal injury	<1%
No impact	50%

###