2010 CyberSecurity Watch Survey – Survey Results
Conducted by *CSO* magazine in cooperation with the U.S. Secret Service,
Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte

---

OVERALL RESULTS

CyberSecurity Watch Survey.....2010
Field Dates .....July – August 2009
Total completed surveys.....523
Margin of Error .....+/- 4%

NOTE TO EDITOR

Complete results attached below. Any references to the data from the 2010 CyberSecurity Watch survey must be sourced as originating from the following: *CSO* magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University, and Deloitte.

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.

4. **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 (August 2008 – July 2009).

SECTION ONE: RESPONDENT PROFILE

1) Is your organization public or privately held?

	2010
Public sector (net)	31%
State, Local or Tribal	22%
Federal	9%
Private sector	69%

2) How would you classify your organization?

	2010
For Profit	86%
Non-profit	14%

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

	2010
Information and telecommunications	15%
Banking and finance	13%
education	7%
Health care	6%
Electronics/ technology	6%
Services	5%
State or county law enforcement/ security (non emergency services)	5%
Government	4%
Insurance	4%
Federal law enforcement/ security (non-emergency services)	3%
Retail, consumer products	3%
Construction/ real estate	2%
Emergency services	2%
Military	2%
Research/ development	2%
Transportation	2%
Agriculture	1%
Chemical	1%
Defense industrial base	1%
Electric power	1%
Food	1%
Gas & oil	1%
Retail, food/ drink	1%
Wholesale	1%
Pharmaceutical	<1%
Water	<1%
Hazardous materials	-
Natural resources/ mining	-
Other	15%

4) Please indicate the critical infrastructure sector and key resources (CIKR) sector, as defined by the Department of Homeland Security, to which your organization belongs:

	2010
Information technology	21%
Banking and finance	16%
Government facilities	7%
Healthcare and public health	6%
Emergency services	5%
Communications	4%
Commercial facilities	3%
Transportation systems	3%
Defense industrial base	2%
Energy	2%
Agriculture and food	1%
Chemical	1%
Critical manufacturing	1%
Water	1%
National monument and icon	<1%
Postal and shipping	<1%
Not applicable	26%

5) What is the total number of employees in your entire organization (please consider parent, subsidiaries, plants, divisions, branches and other organizations worldwide)?

	2010
100,000 or more	10%
50,000 - 99,999	5%
30,000 - 49,999	4%
20,000 - 29,999	3%
10,000 - 19,999	8%
7,500 - 9,999	3%
5,000 - 7,499	6%
2,500 - 4,999	8%
1,000 - 2,499	8%
500 - 999	7%
100 - 499	16%
Under 100	23%
Don't know	1%

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

	2010
Director/manager of IS/ IT/ communications/ networking	17%
Director/manager of Security	15%
Staff	13%
Consultant	8%
Corporate non-IT management (i.e., CEO, President, CFO, Treasurer, COO, general manager, managing director	8%
Chief Information Officer (CIO) or Chief Technology Officer (CTO)	7%
Chief Security Officer (CSO) or Chief Information Security Officer (CISO)	7%
Detective/ case agent	7%
EVP/SVP/VP of IS/ IT/ communications/ networking	4%
Director/manager of Non-IT or security-related function (i.e., finance/ accounting, operations)	4%
EVP/SVP/VP of security	3%
EVP/SVP/VP of Non-IT or security-related function (i.e., finance/ accounting, operations)	2%
Supervisor	2%
Command officer	1%
Prosecutor	1%
Deputy chief/ chief deputy/ 1st assistant	<1%
Chief/ sheriff/ director	<1%
Other	1%

7) 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.)

	2010
Over $250 Million	4%
$100 to $249.9 Million	2%
$50 to $99.9 Million	2%
$25 to $49.9 Million	2%
$10 to $24.9 Million	2%
$5 to $9.9 Million	4%
$1 to $4.9 Million	10%
$500,000 to $999,999	5%
$250,000 to $499,999	6%
$100,000 to $249,999	10%
$50,000 to $99,999	8%
Less than $50,000	25%
Don't know/ Not Applicable	20%

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.)

	2010
Over $250 Million	4%
$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	5%
$1 to $4.9 Million	7%
$500,000 to $999,999	6%
$250,000 to $499,999	5%
$100,000 to $249,999	7%
$50,000 to $99,999	6%
Less than $50,000	25%
Don't know/ Not Applicable	29%

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

	2010
Decisions regarding information security	71%
Decisions regarding handling of employee policy violations	50%
Decisions regarding referral of potential electronic crime to law enforcement	49%
Investigations or prosecution of cybercrimes	46%
Decisions regarding corporate/ physical security	45%
Audit reporting concerning fraud or cybercrimes	42%
None of the above	12%

SECTION TWO: SECURITY EVENTS

1) Please estimate the total number of cyber security events experienced by your organization during the last 12 months (August 2008 – July 2009). 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.

	2010
None	40%
ANY (NET)	60%
Mean (excluding 0)	2,704
Median (excluding 0)	5

2) Has the number of cyber security events experienced by your organization in the past 12 months increase, decrease or remain the same, when compared to the prior 12 months?
(Base: experienced a cyber security event during the past 12 months)

	2010
Increased	37%
Decreased	14%
No Change	34%
Don't know/ not sure	16%

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

OUTSIDERS (Non-employees or Non-contractors, currently or previously) (Base: experienced a cyber security event during the past 12 months)

	2010
Mean	50%
Median	50%

INSIDERS: Current employees or contractors) (Base: experienced a cyber security event during the past 12 months)

	2010
Mean	26%
Median	1%

UNKNOWN (Base: experienced a cyber security event during the past 12 months)

	2010
Mean	24%
Median	-

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?

	2010
Mean	28%
Median	15%

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?

	2010
Mean	72%
Median	85%

SECTION THREE: CYBERCRIME

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

	2010
None	14%
ANY (NET)	51%
100%	15%
No Answer	35%

2) Please indicate all of the cybercrimes committed against your organization during the past 12 months, along with the sources of these cybercrimes to the best of your knowledge. (Base: Experienced a cyber security event during the past 12 months)

2010	Committed (net)	Insider	Outsider	Source Unknown	Not Applicable	Don't Know
Virus, worms or other malicious code	53%	14%	41%	19%	13%	15%
Unauthorized access to/ use of information, systems or networks	35%	23%	13%	6%	36%	23%
Illegal generation of spam email	32%	7%	26%	9%	37%	21%
Spyware (not including adware)	41%	15%	28%	13%	23%	23%
Denial of service attacks	27%	5%	23%	11%	41%	21%
Financial Fraud (credit card fraud, etc.)	26%	11%	16%	4%	46%	24%
Phishing (someone posing as your company online in an attempt to gain personal data from your customers or employees)	38%	5%	33%	11%	31%	21%
Theft of other (proprietary) info including customer records, financial records, etc.	21%	15%	5%	4%	51%	25%
Theft of Intellectual Property	22%	16%	6%	4%	48%	26%
Intentional exposure of private or sensitive information	16%	11%	6%	4%	56%	23%
Sabotage: deliberate disruption, deletion or destruction of information, systems or networks	19%	10%	10%	5%	55%	21%
Zombie machines on organization's network/ bots/use of network by BotNets	22%	7%	17%	8%	47%	23%
Web site defacement	14%	2%	12%	3%	61%	22%
Extortion	5%	1%	3%	1%	72%	23%
Other	4%	2%	2%	2%	56%	39%
None of the Above		5%				
Theft of Personally Identifiable Information (PII)	20%	10%	11%	4%	51%	26%
Unintentional exposure of private or sensitive information	34%	29%	3%	5%	40%	22%

3) How these intrusions were handled based upon source:

	Insider
	Experienced a Cyber Security Event committed by Insider
	2010
Handled internally without involving legal action or law enforcement	72%
Handled internally with legal action	13%
Handled externally by notifying law enforcement	10%
Handled externally by filing a civil action	5%

4) Please indicate all mechanisms used by insiders in committing electronic crimes against your organization in the past 12 months (Base: Experienced cyber security event during the past 12 months by an insider):

	2010
Laptops	44%
Copied information to mobile device (USB drive, iPod, etc.)	42%
Downloaded information to home computer	38%
Stole information by sending it out via email	34%
Shared account (e.g. system administrator, DBA, etc.)	33%
Used their own account	33%
Stole hardcopy information	30%
Compromised an account	28%
Remote access	25%
Used authorized system administrator access	25%
Stole information by downloading it to another computer	25%
Escalated privileges	22%
Blackberry or other mobile handheld device	20%
Social engineering	17%
Password crackers or sniffers	16%
Backdoors	13%
Rootkit or Hacking Tools	9%
Malicious code inserted as part of the software development process	5%
Logic bomb	2%
Other	8%
Don't know	11%

5) If any cyber security events were not referred for legal action, please indicate the reason(s) not referred: (Base: experienced a cyber security event during the past 12 months)

	2010
Damage level insufficient to warrant prosecution	37%
Lack of evidence/ not enough information to prosecute	35%
Could not identify the individual/ individuals responsible for committing the eCrime	29%
Concerns about negative publicity	15%
Concerns about liability	7%
Prior negative response from law enforcement	7%
Concerns that competitors would use incident to their advantage	5%
Unaware that we could report these crimes	5%
Other	5%
Don't know	14%
Not applicable	24%

6) Which of the following types of losses did your organization experience during the past 12 months as a result of cybercrime?

	2010
Operational losses	25%
Financial losses	13%
Harm to reputation	15%
Theft of sensitive data	16%
Exposure of confidential information such as PII	15%
Loss of intellectual property	12%
Other	5%
Not applicable- no losses experienced in past 12 months	31%
Don't know/ not sure	23%

7) Please estimate the total monetary value of losses your organization sustained due to cybercrime during the past 12 months. (Base: experienced a cyber security event during the past 12 months)

	2010
Mean	$394,700
Median	$10,000

8) During the past 12 months, did monetary losses to your organization from cyber security events increase, decrease, or remain the same compared to the prior 12 months (August 2008 – July 2009)? (Base: experienced a cyber security event during the past 12 months)

	2010
Increase	16%
Decrease	7%
Remain the same	35%
Not sure	42%

SECTION FOUR: EFFECTIVENESS OF SECURITY MEASURES

1) Does your organization have a formalized plan outlining policies and procedures for reporting and responding to security events committed against your organization? (Base: experienced a cyber security event during the past 12 months)

	2010
Yes	56%
No, but planning to implement formalized plan within next 12 months	19%
No plans at this time	18%
Don't know/ not sure	7%

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

	2010
1 year or less	10%
More than 1 year to 2 years	13%
More than 2 years to 5 years	21%
More than 5 years	19%
Don't know	26%
Not applicable - do not keep track of security events	12%

3) Which of the following security policies and procedures does your organization use in an attempt to prevent or reduce security events?

	2010
Account/ password management policies	80%
Acceptable use policy/ Formal “inappropriate use” policy	68%
Monitor Internet connections	64%
Employee/ contractor background check	61%
Non-disclosure agreement	61%
New employee security training	55%
Required internal reporting of misuse or abuse of computer access by employees or contractors	55%
Periodic risk assessments	54%
Employees required to review and accept the written inappropriate use policy on any periodic basis	53%
Incident response team	52%
Internet connection monitoring (external)	51%
Periodic security education and awareness programs	51%
Periodic systems penetration testing	49%
Employee Assistance Program	46%
Targeted Employee Monitoring in response to suspicious or concerning behavior	46%
Conduct regular security audits	45%
Include security in contract negotiations with vendors/ suppliers	45%
Regular account audits	43%
Employee monitoring	41%
Random security audits	40%
Intellectual property agreement	37%
Storage & review of e-mail or computer files	36%
Technically enforced segregation of duties	36%
Regular information audits	34%
Regular security communication from management	34%
Hired a Chief Security Officer (CSO) or Chief Information Security Officer (CISO)	31%
Monitor online actions of employees at increased risk for insider threat (e.g. employees who are disgruntled or have turned in resignation)	31%
Software code reviews	30%
Public Law Enforcement partnerships	26%
Use of “white hat” hackers	20%
Government security clearances	14%
None of the above/ Don’t have security policy in place	2%
Don't know	3%

4) How effective do you consider each of the following technologies in place at your organization in detecting and/ or countering security events?
(Scale: Very effective, Somewhat effective, Not very effective, Not at all effective, Don't know, Not applicable-don't use) (Base: experienced a cyber security event during the past 12 months)

Percent "Very" or "Somewhat" Effective	**2010**
Statefull firewalls	86%
Electronic access control systems	82%
Access controls	80%
Password complexity	79%
Encryption	76%
Heuristics-based SPAM filtering	74%
Application layer firewalls	71%
Host-based firewalls	68%
Network-based antivirus	68%
Identity management Systems	67%
Network IDS/IPS	66%
Policy-based network connections & enforcement	66%
RBL-based SPAM filtering	66%
Surveillance	66%
Wireless encryption/ protection	66%
Automated patch management	65%
Host-based antivirus	63%
Badging	62%
Change control/configuration management systems	62%
Network-based policy enforcement	62%
Rights management	62%
Multi-factor/strong authentication	61%
Network access control (NAC)	60%
Role-based authentication	57%
Host-based policy-enforcement	56%
Application configuration monitoring	53%
Host-based IDS/ IPS	53%
Manual patch management	53%
Host-based SPAM	51%
Network-based monitoring/forensics/ESM tool	51%
Software development tools (& processes)	50%
Host based anti-SPAM	47%
Data tracking	46%
Host base configuration management/change control	45%
Application monitoring & trending	44%
Digital signatures	43%
One-time passwords	43%
Wireless monitoring	41%
Data loss prevention (DLP) tools	39%
Application signing	38%
Automated integrity controls	38%
Anomaly detection system	32%
Biometrics	30%
Keystroke monitoring	24%

5) Have any of the following security policies and procedures at your organization supported or played a role in the:
    a. Deterrence of a potential criminal
    b. Detection of a criminal
    c. Termination of an employee or contractor
    d. 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
	2010	2010	2010	2010
Periodic systems penetration testing *(base: 153)*	40%	10%	8%	1%
Periodic security education & awareness programs *(base: 159)*	38%	2%	7%	1%
Regular security communication from management *(base: 105)*	38%	6%	8%	2%
Use of "white hat" hackers *(base: 62)*	37%	11%	8%	3%
New employee security training *(base: 171)*	36%	4%	7%	-
Technically-enforced segregation of duties *(base: 113)*	36%	4%	12%	2%
Conduct regular security audits *(base: 139)*	35%	11%	25%	6%
Monitor Internet connections	35%	18%	37%	10%
Random security audits *(base: 125)*	35%	10%	22%	3%
Regular information audits *(base: 105)*	35%	9%	17%	5%
Hired a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) *(base: 97)*	34%	12%	10%	6%
Periodic risk assessments *(base: 168)*	34%	10%	9%	4%
Government security clearances *(base: 45)*	33%	9%	13%	2%
Internet connection monitoring (external) *(base: 160)*	33%	18%	31%	11%
Regular account audits *(base: 135)*	33%	12%	19%	4%
Employee/ contractor background check *(base: 189)*	32%	22%	23%	4%
Monitor online actions of employees at increased risk for insider threat (e.g. employees who are disgruntled or have turned in resignation) *(base: 96)*	32%	16%	43%	10%
Employees required to review and accept the written inappropriate use policy on any periodic basis *(base: 166)*	31%	5%	24%	4%
Employee monitoring *(base: 128)*	31%	18%	49%	9%

Security Policy	Deterrence of a potential criminal	Detection of a criminal	Termination of an Employee or Contractor	Prosecution of an Alleged Criminal
	2010	2010	2010	2010
Intellectual property agreement *(base: 115)*	31%	4%	18%	7%
Required internal reporting of misuse or abuse of computer access by employees or contractors *(base: 171)*	31%	15%	36%	9%
Include security in contract negotiations with vendors/ suppliers *(base: 139)*	30%	4%	14%	3%
Non-disclosure agreement *(base: 189)*	30%	2%	16%	5%
Storage & review of e-mail or computer files *(base: 111)*	30%	17%	23%	10%
Account/ password management policies *(base: 250)*	29%	7%	21%	3%
Incident response team *(base: 163)*	25%	23%	26%	14%
Software code reviews *(base: 93)*	25%	3%	7%	3%
Targeted employee monitoring in response to suspicious or concerning behavior *(base: 144)*	23%	17%	53%	11%
Public law enforcement partnerships *(base: 82)*	21%	15%	13%	16%
Acceptable use policy/ Formal "inappropriate use" policy *(base: 212)*	20%	7%	55%	9%
Employee Assistance Program *(base: 143)*	13%	1%	4%	1%

6) Are you more concerned or less concerned about cyber security threats posed to your organization during the past 12 months compared to the prior 12 months?

	2010
More concerned	55%
Less concerned	4%
Level of concern has not changed	41%

7) Is your organization more prepared or less prepared to deal with (prevent, detect, respond, recover) cyber security threats today compared to 12 months ago?

	2010
More prepared	58%
Less prepared	6%
Same level of preparedness	37%

Percents calculated on total respondent base of 523 unless otherwise specified. Percent may not sum to 100 due to rounding.

Contacts:

***CSO* Magazine**
Lynn Holmlund
508.935.4526
lholmlund@idgenterprise.com

Deloitte
Daniel Mucisko
973.602.4126
dmucisko@deloitte.com

CERT Program
Kelly Kimberland
412.268.4793
public-relations@sei.cmu.edu

U.S. Secret Service
Joseph Freyre
202.406.9330
joseph.freyre@usss.dhs.gov