



Cybercrime against Businesses, 2005 Findings from the National Computer Security Survey

Ramona R. Rantala
Bureau of Justice Statistics
September, 2008

Directives and Legislation

- The National Strategy to Secure Cyberspace, Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program:

“DOJ and other appropriate agencies will develop and implement efforts to reduce cyber attacks and cyber threats through . . . developing better data about victims of cybercrime and intrusions in order to understand the scope of the problem and to be able to track changes over time.” (A/R 2-1)
- Cyber Security Research and Development Act, P.L. 107-305



Partnerships

- DHS
 - National Cyber Security Division
 - U.S. Secret Service
- DOJ
 - Computer Crime and Intellectual Property
 - FBI Cyber Security Squad
- Other supporters
 - www.ojp.usdoj.gov/bjs/survey/ncss/ncss.htm
- Data collection agents
 - RAND Corporation
 - Market Strategies, Inc.



National Computer Security Survey

- Measure nature and prevalence of cybercrime
- Quantify losses
- Reveal vulnerabilities
- Identify best security practices
- Inform resource allocation
- Reduce cyber threats

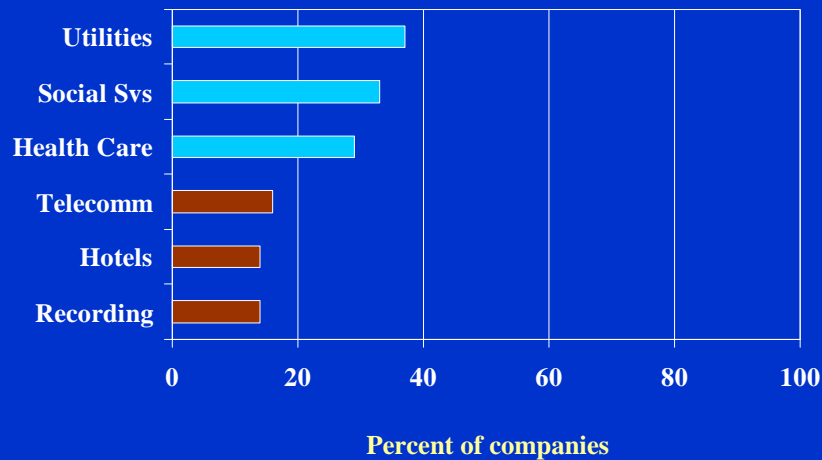


NCSS Universe, Sample, and Response

NCSS Universe, Sample, and Response, by Company Size, 2005

Number of employees	Number of businesses			Response
	Universe	Sample	Response	Rate
All businesses	7,278,109	35,596	8,079	23 %
2 to 24	6,771,026	11,479	2,056	18
25 to 99	396,355	5,601	1,236	22
100 to 999	98,585	11,472	2,894	25
1,000 or more	12,143	7,044	1,893	27

Highest and Lowest Response Rates



NCSS Data

- Represents more than 8,000 businesses
- Covers 36 economic sectors
- Is the most comprehensive data available on—
 - Nature of computer security incidents
 - Prevalence by industry and type of incident
 - Monetary losses
 - Downtime
 - Types of offenders
 - Reporting incidents to authorities
 - Vulnerabilities leading to breaches



The Nature of Cybercrime

- Cyber attacks
 - All or part of the computer system is the target
- Cyber theft
 - A computer was used to illegally obtain money, goods, or services
- Other computer security incidents
 - Spyware, adware, other malware
 - Phishing, spoofing
 - Hacking
 - Pinging, scanning, sniffing
 - Theft of other information



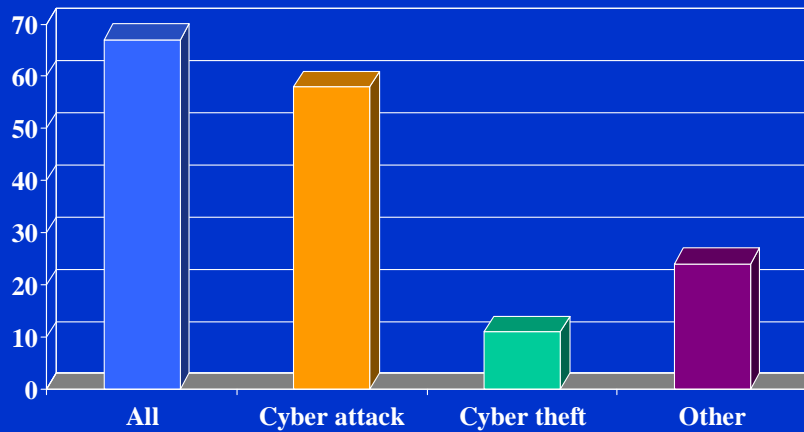
Prevalence of Cybercrime

Prevalence of computer security incidents among businesses, by type of incident, 2005

Type of incident	All companies	Companies detecting incidents	
		Number	Percent
All incidents	7,636	5,081	67 %
Cyber attack	7,626	4,398	58 %
Computer virus	7,538	3,937	52
Denial of service	7,517	1,215	16
Vandalism	7,500	350	5
Cyber theft	7,561	839	11 %
Other	7,492	1,792	24 %

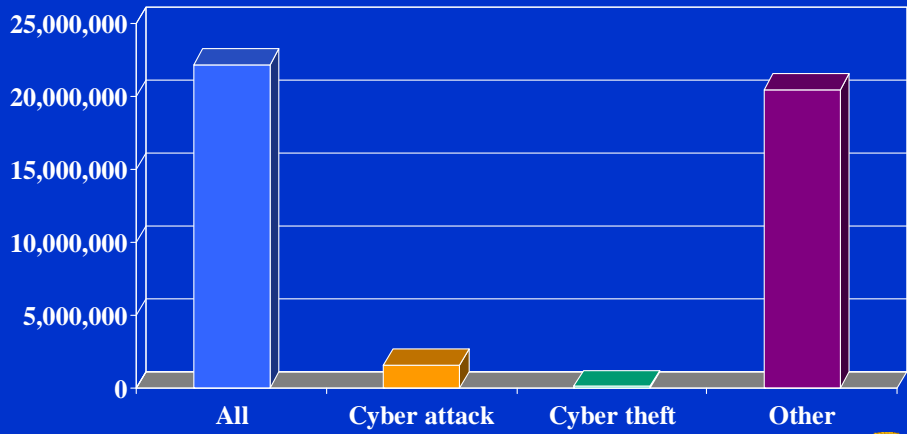
Prevalence of Cybercrime

Percent of companies



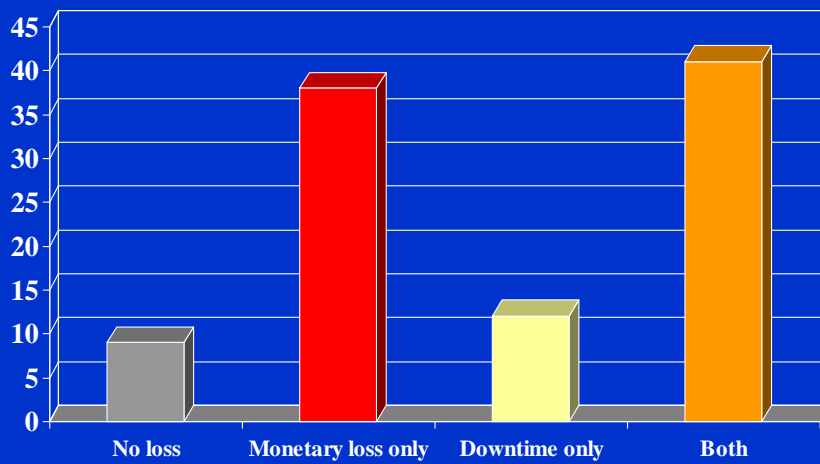
Total Incidents

Number of incidents



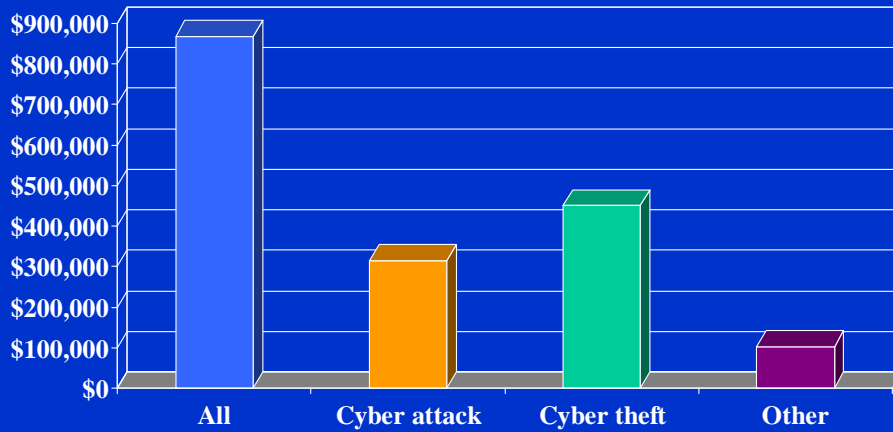
Types of Loss

Percent of companies



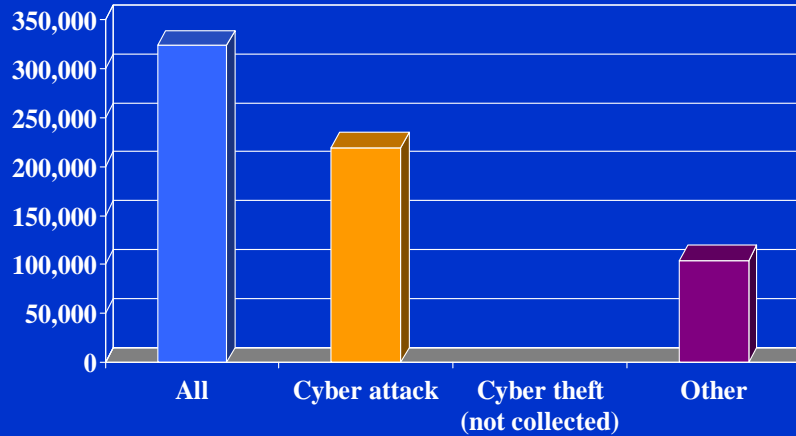
Total Monetary Loss

Monetary Loss
(in thousands of dollars)



Total System Downtime

System downtime
(in hours)



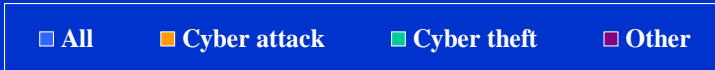
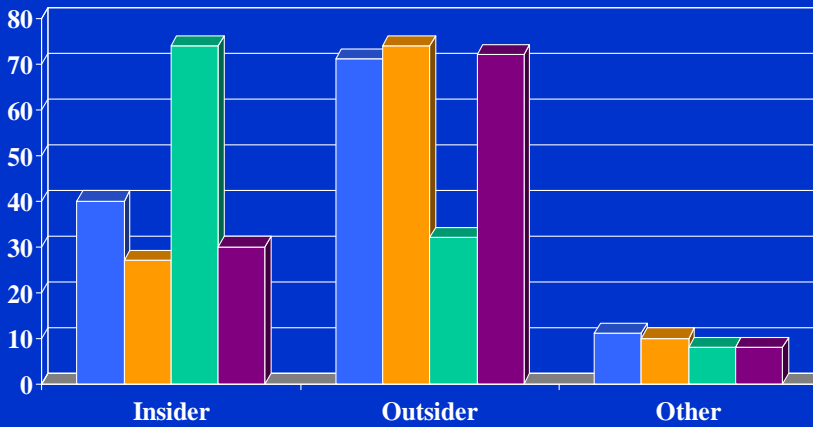
Unknown Cyber Offenders

Percent of companies



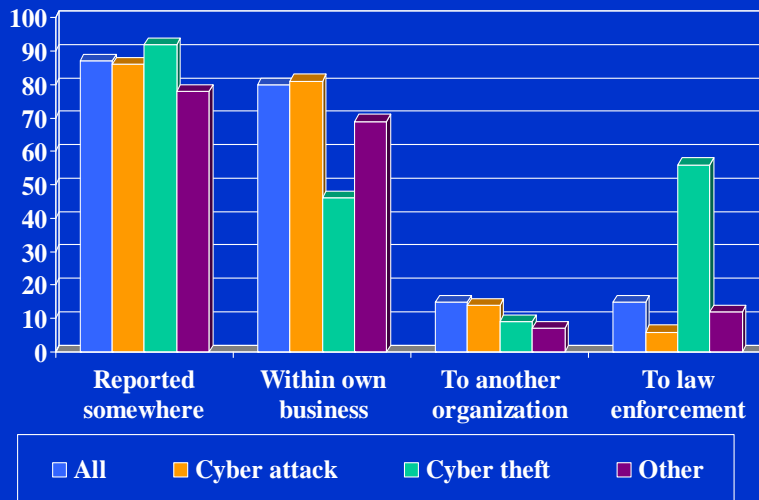
Suspected Cyber Offenders

Percent of companies



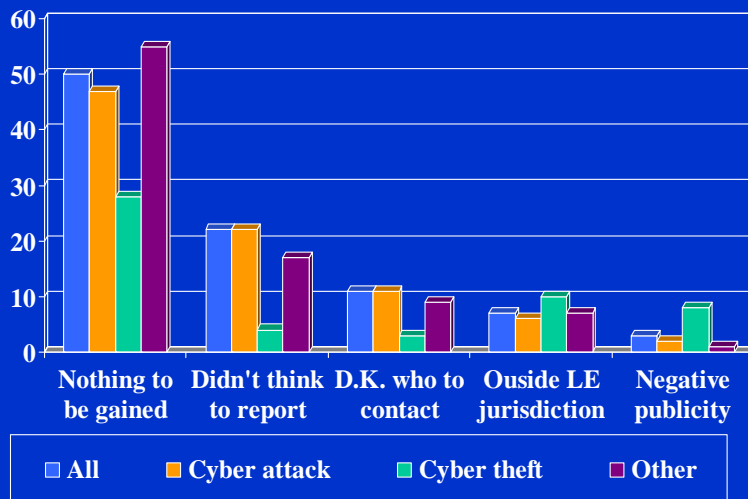
Reporting Incidents to Authorities

Percent of companies



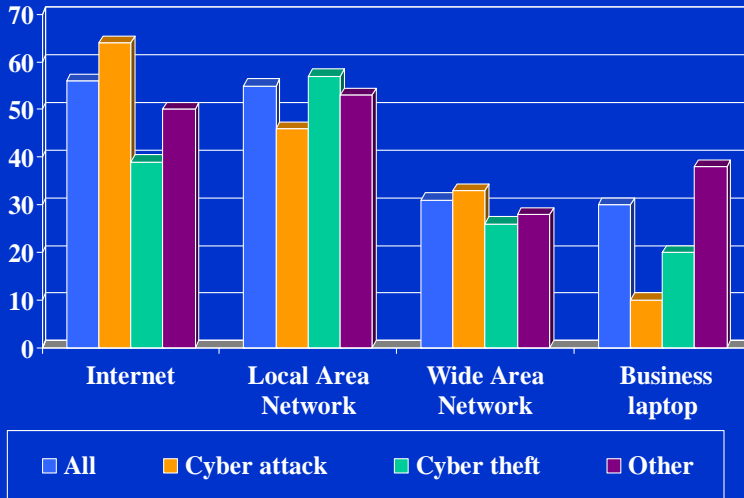
Reasons Incidents Were Not Reported

Percent of companies



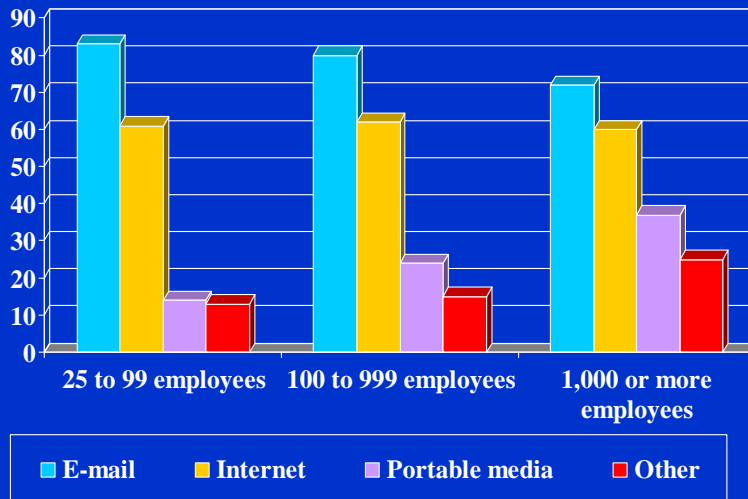
Networks Most Commonly Accessed

Percent of companies



Computer Virus Sources

Percent of companies



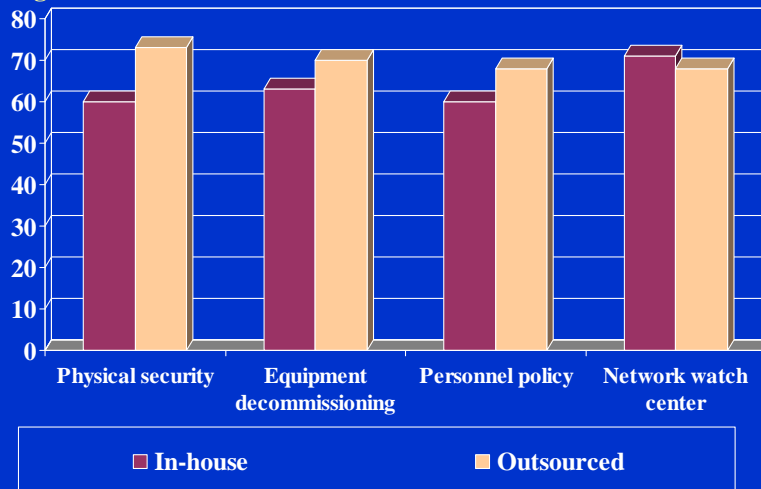
Most Common Computer Security—

- | <u>In House</u> | <u>Outsourced</u> |
|--|---|
| <ul style="list-style-type: none">• Disaster recovery plan• Corporate security policy• Physical security• Personnel policy• Business continuity plan | <ul style="list-style-type: none">• Intrusion testing• Vulnerability/risk assessment• Disaster recovery plan• Periodic audits• Network watch center |



In-House Versus Outsourced Security

Percent of companies detecting an incident



Future Plans

- Scale down questionnaire
- Survey a sample of industries each year
- Explore mandatory reporting requirements



Contact

Ramona Rantala
Statistician
Bureau of Justice Statistics
Department of Justice

(202) 307-6170
Ramona.Rantala@usdoj.gov



For Your Reference



Risk Levels

- Critical infrastructure
 - Agriculture
 - Chemical and drug mfg
 - Computer system design
 - Finance
 - Health care
 - Internet service providers
 - Petroleum mining and manufacturing
 - Publications and broadcasting
 - Real estate
 - Telecommunications
 - Transportation and pipelines
 - Utilities



Risk Levels (continued)

- High risk
 - Manufacturing, durable
 - Manufacturing, non-durable goods
 - Motion picture and sound recording
 - Retail
 - Scientific research and development
 - Wholesale
- Moderate risk
 - Accounting
 - Advertising
 - Architecture and engineering
 - Business and technical schools
 - Insurance
 - Legal services



Risk Levels (continued)

- Low risk
 - Accommodations
 - Administrative support
 - Arts & entertainment
 - Construction
 - Food services
 - Forestry, fishing, and hunting
 - Management of companies
 - Mining
 - Rental services
 - Social services
 - Other services
 - Warehousing



Highest Prevalence of Cybercrime

- Telecommunications (82%)
- Computer system design (79%)
- Manufacturing, durable goods (75%)
- Chemical and drug manufacturing (73%)
- Manufacturing, non-durable goods (72%)
- Business and technical schools (72%)
- Publications and broadcasting (71%)



Highest Prevalence of Cyber Attacks

- Telecommunications (74%)
- Computer system design (72%)
- Manufacturing, durable goods (68%)
- Chemical and drug manufacturing (66%)
- Publications and broadcasting (65%)
- Business and technical schools (64%)
- Manufacturing, non-durable goods (61%)



Highest Prevalence of Cyber Theft

- Finance (33%)
- Internet service providers (21%)
- Telecommunications (17%)
- Computer system design (15%)
- Manufacturing, durable goods (15%)
- Publications and broadcasting (14%)
- Accommodations (14%)



Highest Prevalence of Other Incidents

- Telecommunications (32%)
- Manufacturing, durable goods (32%)
- Architecture and engineering (31%)
- Chemical and drug manufacturing (27%)
- Wholesale (27%)
- Legal services (27%)



Lowest Prevalence of Cybercrime

- Forestry, fishing, and hunting (44%)
- Agriculture (51%)
- Food services (54%)
- Accounting (55%)
- Petroleum mining and manufacturing (56%)



Lowest Prevalence of Cyber Attacks

- Agriculture (40%)
- Forestry, fishing, and hunting (40%)
- Accounting (47%)
- Food services (48%)
- Finance (49%)



Lowest Prevalence of Cyber Theft

- Forestry, fishing, and hunting (3%)
- Warehousing (4%)
- Social services (5%)
- Agriculture (6%)
- Advertising (6%)
- Legal services (6%)



Lowest Prevalence of Other Incidents

- Food services (15%)
- Forestry, fishing, and hunting (16%)
- Accommodations (16%)
- Warehousing (16%)
- Agriculture (17%)

