Computer Security – Survey and Optimal Investment

CSI/FBI 2005
Outline

• Computer Crime and Security Survey
  – Respondents
  – Key findings

• How much should be spent to improve computer security?
Security Survey

• Respondents
  – CSI/FBI 2005
  – 700 computer security practitioners in US corporations, government agencies, financial institutions, medical institutions and universities.
Security Survey

Figure 1. Respondents by Industry Sector

- Financial: 17%
- High-tech: 15%
- Educational: 6%
- Medical: 7%
- Retail: 1%
- Transportation: 1%
- Telecommunications: 4%
- Legal: 1%
- Federal Government: 9%
- State Government: 5%
- Local Government: 2%
- Other: 19%
- Manufacturing: 9%
- Utility: 4%

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 699 Respondents
Figure 2. Respondents by Number of Employees
(Numbers do not total 100% due to rounding.)

- 50,000 or more: 11%
- 1-99: 20%
- 10,000-49,999: 16%
- 100-499: 14%
- 1,500-9,999: 23%
- 500-1,499: 15%

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 699 Respondents
Figure 3. Respondents by Revenue

- Over $1 billion: 37%
- Under $10 million: 25%
- $10 million to $99 million: 18%
- $100 million to $1 billion: 20%

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 549 Respondents
Security Survey

Figure 5. Percentage of IT Budget Spent on Security
(Numbers do not total 100% due to rounding.)

- More than 10%: 8%
- 8-10%: 11%
- 6-7%: 8%
- 3-5%: 24%
- 1-2%: 24%
- Less than 1%: 11%
- Unknown: 15%

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 690 Respondents
Figure 7. Average Reported Computer Security Expenditure per Employee
By Organization Revenue

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 405 Respondents
Figure 8. Average Reported Computer Security Expenditure/Investment per Employee
By Industry Sector

- State government
- Utility
- Transportation
- Telecommunications
- Manufacturing
- High-tech
- Financial
- Medical
- Retail
- Local government
- Educational
- Legal
- Federal government
- Other

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 405 Respondents
Security Survey

Figure 10. Percentage of Security Function Outsourced

(Numbers do not total 100% due to rounding.)

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 682 Respondents
Security Survey

- Key findings

Figure 13. Unauthorized Use of Computer Systems within the Last 12 Months

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
Figure 14. Types of Attacks or Misuse Detected in the Last 12 Months
By Percent of Respondents

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 700 Respondents
Figure 16. Dollar Amount Losses by Type

- Virus: $42,787,767
- Unauthorized access: $31,233,100
- Theft of proprietary info: $30,933,000
- Denial of service: $7,310,725
- Insider Net abuse: $6,856,450
- Laptop theft: $4,107,300
- Financial fraud: $2,565,000
- Misuse of public Web application: $2,227,500
- System penetration: $841,400
- Abuse of wireless network: $544,700
- Sabotage: $340,600
- Telecom fraud: $242,000
- Web site defacement: $115,000

Total Losses for 2005 were $130,104,542

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 639 Respondents
Figure 17. Security Technologies Used

- Firewalls: 97%
- Anti-virus software: 96%
- Intrusion Detection Systems: 72%
- Server-based access control lists: 70%
- Encryption for data in transit: 68%
- Reusable account/login passwords: 52%
- Encrypted files: 46%
- Smart cards/other one-time password tokens: 42%
- Public Key Infrastructure: 35%
- Intrusion Prevention Systems: 35%
- Biometrics: 15%

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 687 Respondents
Figure 19. Organization Invests the Appropriate Amount on Security Awareness Training

Mean Values Reported on a Seven-Point Scale

- High-tech
- Federal Government
- Other
- Transportation
- State Government
- Telecommunications
- Financial
- Medical
- Retail
- Manufacturing
- Educational
- Local Government
- Utility
- Legal

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 698 Respondents
Figure 21. Actions Taken After Computer Intrusion(s) in the Last 12 Months

- Patched holes
- Did not report
- Reported to law enforcement
- Reported to legal counsel

Source: Computer Security Institute
2005: 320 Respondents
Figure 22. Reason Organization Did Not Report the Intrusion to Law Enforcement

Percentage of Respondents Identifying as Important

- Negative publicity would hurt stock/image: 43%
- Competitors would use to their advantage: 33%
- Civil remedy seemed best course: 16%
- Unaware of law enforcement interest: 16%

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute
2005: 423 Respondents
How much should be spent?\textsuperscript{1}

- The Model (Gordon & Loeb 2002)
  - Invest $z$ to reduce $L$

Vulnerability: $v$

\[ s(0) = v \]

Attacks

Information System

Breach function: $s(z)$, $s(0) = v$

Loss

Threats
How much should be spent?  

- The Model

\[ EBIS(z) = [v - s(z,v)] \times L \]

\( v \) : probability a threat is realized

\( z \) : dollar invested in security

\( v \times L \), loss due to realized threat
How much should be spent? 

• Breach functions
How much should be spent? 

• For low or high vulnerability systems, no optimal investment
• For midrange vulnerability, about 37% of expected loss
• Different breach function may have different optimal investment