What Does a Computer Security Breach Really Cost?

Submitted by

Anita D. D'Amico, Ph.D.
Secure Decision, a Division of Applied Visions, Inc.
AnitaD@avi.com

September 7, 2000

Objective

Many CEOs and CIOs are slow to invest in computer security because they do not know how to measure their Return on Investment (ROI). No one has shown them the actual costs associated with *not* investing in computer security. The objective of this paper is to provide the information security officer with objective data about the actual cost of computer security breaches to commercial companies. The information presented herein can be used as input into the ROI analyses to support security procurements.

How Cost Is Measured

In the commercial world, the cost of a cyber security breach is measured by both "tangibles" and "intangibles." The tangibles can be calculated based on estimates of:

- Lost business, due to unavailability of the breached information resources
- Lost business, that can be traced directly to accounts fleeing to a "safer" environment
- Lost productivity of the non-IT staff, who have to work in a degraded mode, or not work at all, while the IT staff tries to contain and repair the breach
- Labor and material costs associated with the IT staff's detection, containment, repair and reconstitution of the breached resources
- Labor costs of the IT staff and legal costs associated with the collection of forensic evidence and the prosecution of an attacker
- Public relations consulting costs, to prepare statements for the press, and answer customer questions
- Increases in insurance premiums
- Costs of defending the company in any liability suits resulting from the breached company's failure to deliver assured information and services.

Not all of these tangible costs will occur with each breach; some will only occur with major, well-publicized breaches.

The intangibles refer to costs that are difficult to calculate because they are not directly measurable, but are nevertheless very important for business. Many of these intangibles

are related to a "loss of competitive advantage" that results from the breach. For example, a breach can affect an organization's competitive edge through:

- Customers' loss of trust in the organization
- Failure to win new accounts due to bad press associated with the breach
- Competitor's access to confidential or proprietary information.

While the focus of this paper is the commercial world, I'd like to note that the military environment has similar cost issues. In the military, the tangible costs are measured in human lives, replacement costs of equipment, and prolonged military operations. The intangibles would include loss of tactical advantage, loss of international prestige, and impaired negotiating positions.

In the next several sections, we will look at how people in various organizations have calculated the cost of breaches in both hypothetical and real world situations.

Hypothetical Examples of the Cost Impact of Security Breaches

Forrester Research[1] estimated the tangible and intangible costs of computer security breaches in three hypothetical situations. Their analysis indicated that, if thieves were to illegally wire $1 million from an on-line bank, the cost impact to the bank would be $106 million. They also estimated that, in the hypothetical situation that cyber techniques are used to divert a week's worth of tires from an auto manufacturer, the auto manufacturer would sustain losses of $21 million. Finally, they estimated that if a law firm were to lose significant confidential information, the impact would be almost $35 million.

Does this sound unrealistic? Remember, that Forrester used both tangibles and intangibles in their estimates, including the loss of confidential information and reputation. The sections below present the results of analyses of real world cost impacts of cyber events, using largely tangible costs as the means of estimating impact.

Real World Examples of Cost Impacts

Cost Impacts On Individual Companies

In December, 1998 Ingram Micro, a PC wholesaler, had to shut down its main data center in Tucson, Arizona due to an electrical short. While the reason for the shut down was not a security breach, the loss of Ingram's Internet business and electronic transactions from 8:00 AM to 4:00 PM mimicked what could happen with a Distributed Denial of Service (DDOS) attack or a major intrusion. As a result of its one day of lost sales and system repairs, Ingram estimates that it lost a staggering $3.2 million.[2] This figure is comparable

[1] Howe, Carl; McCarthy, John C.; Buss, Tom; and Davis, Ashley. "The Forrester Report: Economics of Security", February, 1998

[2] Salkeyer, Alex. "Who Pays When a Business Is Hacked?" Business Week Online: Daily Briefing, May 23, 2000. URL: http://www.businessweek.com/bwdaily/dnflash/dnfarch.htm

to Forrester's projection of a $21 million loss for an auto manufacturer who is unable to get tires for a week.

To estimate the cost impact of the types of breaches that happen daily to companies, one can turn the annual surveys of the Computer Security Institute (CSI) (www.gosci.com) and the FBI[3],[4]. For the past five years, the CSI-FBI "Computer Crime and Security Survey" has been a major source of information on the frequency and impact of computer security breaches, through their polling of commercial, non-profit, and government organizations. Their Year 2000 report was based on a survey of 643 information security professionals from organizations throughout the United States. Typically, the respondents represent organizations that have already made some commitment to computer security. In the 1999 survey, 91% of the respondents had firewalls, 42% had intrusion detection systems, and 34% were using digital certificates in their companies.

Of the 643 respondents in the year 2000, 90% had detected cyber attacks on their organizations; and 74% reported financial losses associated with those attacks. Of the total sample of respondents, 42% (273 people) were able to quantify their exact losses, which totaled $265,589,940, or **$972,857 cost impact per organization across all types of breaches**.

The highest impact came from theft of proprietary information, reported by 66 people. Their total losses came to $66,708,000 or **$1,010,727 cost impact per organization for theft of proprietary information.** While this may seem like a lot, the average cost impact of theft of proprietary information in their 1999 survey was $1,847,652. The **sabotage of data or networks was reported by 61 respondents, for a total loss of $27,148,000 or an average loss of $445,049 per organization**. This loss was significantly higher than the 1999 average loss of $163,740 associated with sabotage.

While these estimates are presumably based on tangible costs to the company, one can infer that the respondents are very aware of and sensitive to the intangible costs of a tarnished reputation that could result from media treatment of security breaches. I base this conclusion, on some interesting data in the 1999 survey. In 1999, 48% of those respondents who had been subjected to an intrusion did not report it. Among the most important reasons cited for their decision not to report those breaches were the fear of negative publicity and the use of the information by competitors.

Cost Impacts Across Industries

---

[3] "Cyber attacks rise from outside and inside corporations", Press Release from Computer Security Institute, March 5, 1999. URL: http://www.gocsi.com/prelea990301.htm

[4] "Ninety percent of survey respondents detect cyber attacks, 273 organization report $265,589,940 in financial losses", Press Release from Computer Security Institute, March 22, 2000, URL: http://www.gocsi.com/prelea_000321.htm

Some research and consulting firms such as Computer Economics (www.computereconomics.com) measure the impact of computer breaches across several companies or industries. Computer Economics[5] has estimated that in 1999 businesses around the globe spent $12.1 billion to combat the effect of computer viruses. Their estimate was based on tangibles such as lost productivity, network down time, and expenses incurred to get rid of the virus infections.

The ILOVEYOU and its copycats have also been studied for their financial impacts across industries. According to Computer Economics[6] the ILOVEYOU virus and its variants caused $6.7 billion in damage in the first five days.

The FBI, in their testimony before the Senate Subcommittee on Technology, Terrorism and Government Information[7], cites the Yankee Group's estimate that industries around the world lost $1.2 billion to the DDOS attacks on e-commerce in February 2000. Their estimate was based on lost capitalization, lost revenues and the costs of security upgrades.

The Cost of Piracy

A different form of security breach – software piracy – also has a cost impact across the software industry. International Planning and Research[8], an independent research firm, estimated that software vendors lost $12.2 billion 1999 due to software piracy. They estimate that one out of three pieces of software used by businesses around the world are pirated copies.

Conclusion

The financial impact of computer security breaches has been quantified by several sources. The best estimate of the impact of security breaches on a single organization can be found in the CSI-FBI survey of over 600 organizations. They concluded that the average cost impact of security breaches on each organization is over $972,000 per year.

---

[5] Noack, David. "Computer Viruses Cost $12 Billion in 1999", APB News, Jan. 20, 2000, URL: http://www.apbnews.com/newscenter/internetcrime/2000/01/20/virus0120_01.html

[6] "Love Bug Damage Costs Rise to $6.7 Billion" Press release by Computer Economics, May 9, 2000, URL: http://www.computereconomics.com/cei/press/2000/pr000509.html

[7] "Statement for the Record of Guadalupe Gonzalez, Special Agent in Charge, Phoenix Field Division, FBI on Cybercrime" before the Special Field Hearing, Senate Committee on Judiciary, Subcommittee on Technology, Terrorism, and Government Information, Washington, DC, April 21, 2999, URL: http://www.fbi.gov/pressrm/congress/congress00/gonza042100.htm

[8] Noack, David. "Businesses Use $12 Billion of Stolen Software" APB News, May 25, 2000, URL: http://www.apbnews.com/newscenter/internetcrime/2000/05/25/software0525_01.html