

Estimating the Cost of a Security Breach

23 Feb 2008

By Andrew Wong

The Challenges

As the number of companies that conduct their businesses electronically grows continuously, information security becomes one of major concerns for senior management. Moreover, as mobile and remote users become more commonplace and previously impenetrable network perimeters dissolve, companies must provide more than simply perimeter security. Damage can occur from the inside out, and companies must protect sensitive data within the enterprise boundaries. In addition, companies are tasked with not only minimizing the cost of security events but also predicting and preventing them.

Calculating the cost of a security breach has never been easy. It is a task than most security practitioner must grapple with, especially when fighting for the additional dollar to invest in information security technologies and processes.

Yet over the past few years, the frequency and gravity of security breaches have increased. Just take a look at TJX. In December 2006, the US retailing giant detected a hacker intrusion against its credit card transaction processing system. Hackers stole information from 45.7 million customer credit and debit cards. It is estimated that the breach will cost TJX US\$1.7 billion, in addition to a number of ongoing legal claims/class suits from affected customers and shareholders.

But how does this apply to my company? The estimated costs were fuzzy. For example, a 2005 CSI/FBI survey estimated the cost to be US\$167,000. Meanwhile, Ponemon Institute survey conducted in 2006 suggested the cost to be US\$4.8 million per breach. Yet another U.S. Department of Justice survey in August 2006 determined the average loss per incident was US\$1.5 million.

In reality, there are many different factors – having taken into account both the tangibles and intangibles - in a security breach cost calculation. At a basic level, the most obvious cost component is human labour. The fuzz is the loss of reputation or the damage control costs required to earn back the consumer's trust. We now have to spend time on public relations efforts, as well as assuring both customers and auditors (including the country regulators) that new processes are in place to guard against such breaches in the future.

This article will attempt to explore some of the considerations when contemplating the cost of a systems breach. It is quite easy to come out with a reasonably estimate. Predictably, I will advocate by saying that it pays to invest upfront in IT security, be it technology, training, policy initiatives or prevention mechanisms. In fact, we might even be able to prove the costs.

Key Cost Components

For a start, we have to move away from the old adage that when a company faces a data breach, all it takes is to have a response team to fix the problem and test the mitigation, and then the company would resume normal business activities. It may be true for some minor hiccups here and there, but definitely not for the major, well-publicized breaches.

To get a better understanding of the magnitude, the costs are broken down in different categories.

1. Clean-up Costs

Lost employee productivity is perhaps the significant part of the total cost. The fact that these 'investigators', assuming they are employees, will be taken away from their normal work activities. Time will be spent analysing what has happened, re-installing operating systems, restoring installed programs and data files, reviewing log files, writing incident reports, interfacing with vendors or suppliers etc.

The estimates can be based on:

- Labour and material costs associated with the detection, containment, repair and reconstitution of the breached resources.
- Labour costs and legal costs associated with the collection of evidence and prosecution of an attacker.
- Lost of productivity for non-IT staff, who have to work in a degraded mode, whilst containment and recovery from the breach is in progress

In fact, according to a Ponemon Institute survey, the cost of diverting employees from every day tasks to managing a data breach increased 100 percent last year, from \$15 per record in 2005 to \$30 a record.

2. Damage Control

Loss of reputation is probably contentious, and in most high-profile breaches, it is more likely be the one to break the camel's back. Perhaps, one of the worst things a company can lose to a hacker is its hard-earned reputation. Rebuilding a brand can cost millions in public relations consulting fees, customer outreach efforts, advertising campaigns and discounted product offers.

Estimates can be based on:

- Public relations consulting costs, to prepare statements for the press, and answer customer questions.
- Call Centres to take additional calls.
- Discounted product offers, gifts, etc.

3. Opportunity Cost

Companies typically experience customer losses after a breach. Forrester estimates that 10 to 20% of your potential customers will be scared away by a security breach in a given year. Most organisations have a good idea of how much each customer is worth and can therefore extrapolate the total opportunity cost.

Estimates can be based on:

- Lost business, due to unavailability of the breached information resources.
- Lost business that can be traced directly to accounts fleeing to a safer environment.
- Failure to win new accounts due to bad press associated with the breach.

4. Indirect Costs

a. Restitution costs

In some foreign jurisdiction (or countries), the company may be required to establish a \$x million consumer restitution fund for the n records that were breached. Forrester estimates it to around \$30 per record.

- A good estimate is the increase in insurance premiums, arising from a breach.
- b. Additional security and audit requirements
Most breaches inevitably would lead to a higher level of security and audit requirements. An audit from a qualified, independent, third-party professional may be required to assure that its security program meets the standards that include administrative, technical and physical safeguards.
- c. Other liabilities
For credit card breaches, the issuing banks incur significant costs to replace the credit cards and compensating the fraud victims. Forrester estimates the total replacement cost ranges from US\$10 to US\$35 per card.

Data Breach Impact Calculator

How much does a data breach impact your business? This calculator, based on the Privacy Management Toolkit by Rebecca Harold, provides an example of the items an organisation should consider when estimating the potential impacts of a data breach.

A. Total Personnel Hours = $1+2+3+4+5+6$

1. Personnel time to determine a breach has occurred
2. Discussion time with legal counsel and executives about the situation
3. Personnel time to determine all the individuals (customers) impacted
4. Personnel time to collect contact information for impacted customers
5. Personnel time to write and mail letters
6. Additional personnel time (others)

B. Total Incident Costs = $1+2+3+4+5$

1. Call centres to take additional calls
2. Public and investor relations
3. Cost of positive advertising to protect company brand
4. Forensics and criminal investigations
5. Cost to change or repair system where breach occurred

C. Total Monitor Cost = $1 * 2 * 3$

1. Total number of individuals within the compromised database(s)
2. Cost per individual for monitoring reports
3. Number of months or years to monitors

D. Total Legal Fines, Fees and Awards = $1 + (2 * 3)$

1. Fines and fees for applicable laws or service penalties
2. Number bringing civil suit
3. Award per individual

E. Total Loss Customer Value = $1 * 2$

1. Number of lost customers
2. Value per customer

Total Estimated Impact Cost = $A + B + C + D + E$

Stock Market Reaction

While the toolkit provides an estimate of the potential cost impact from a security data breach, it did not take into account the market reaction of information security breaches announced publicly. A scan of the internet shows that there are only a small number of researches on this area. Most of these studies were centred on a single event-based methodology on the assumption that capital markets are efficient to evaluate the impact of the events on expected future cash flows of the companies.

A summary of some of these studies are outlined below:

- Campbell et al. [1] found a highly significant negative stock market reaction when breaches are related to unauthorized access to confidential data while other breaches did not have significant market reaction.
- Garg et al. [2] estimated that security incidents can cost breached companies 0.5 to 1 percent of annual sales on average. However, spill over effects from the study shows that share price of security vendors associated with the company increase between 1 to 3 percent and insurance companies experienced 1 to 2 percent increase in a share price.
- Two separate studies by Garg et al. [2] and Cavusoglu et al. [3] found that the security breach announcements on average caused the breached companies losing 2.1 percent of their market value within two days following the public announcement. On the other hand, the security developers realized an average abnormal return of 1.36 percent during this period.

Interesting, a study conducted in 2006 by Myung Ko and Carlos Dorantes suggests that information security breaches have minimal long term economic impact on the impacted companies. One possible explanation is that the breached companies respond to the breach incident by making additional security investment to prevent from any future breaches. This can lead to either help reduce the negative reputation of the companies caused by the breach or even have a positive long-term economic impact on the firm. Another explanation is that as the time passes, people forget about what happened earlier and the impact of the breach on financial performance phases out over the long-term.

Conclusion

Quantifying the costs from security breaches is challenging since the choices are to either predict the unknown, or wait until a security incident occurs and evaluate the damage. However, companies can evaluate their current assets, assess the risks associated with those assets, identify the probability of a security incident, and estimate the associated financial impact. These predicted expenses can help justify the security initiatives necessary to protect an enterprise's assets, mitigating the risk of downtime and increasing productivity and business cost savings.

Furthermore, although prevention is the best policy, creating a detailed response plan will help any enterprise deal more effectively with downtime if it does occur, assuming a quicker recovery, minimized costs, and shorter duration. Finally, companies must be prepared to invest in IT security, staff training, developing security policy initiatives and working out prevention mechanisms.

The writer heads the Information Security department at a Singapore bank. He has more than 20 years experiences in developing security policies, solutions and have implemented numerous security measures for major e-channels and internet banking systems. This article is contributed in his personal capacity.

References

- [1] Campbell, K., Gordon, L., Loeb, M. and Zhou, L. "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *Journal of Computer Security*, Vol. 11, Number 2003, pp. 431-448.
- [2] Garg, A., Curtis, J. and Halper, H. "The financial impact of IT security breaches: what do investors think?," *Information Systems Security*, Vol. 12, Number 1, 2003, pp. 22-33.
- [3] Cavusoglu, H., Mishra, B. and Raghunathan, S. "The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers," *International Journal of Electronic Commerce*, Vol. 9, Number 1, 2004, pp. 69-104.