

How Much Does a Hack Cost?

AUGUST 16, 2006 | It might be the most elusive figure in the security industry. Vendors want it so they can show the value of their products. Security pros want it so they can cost-justify new purchases. Attackers want it so they can measure the effectiveness of their exploits.

But after an industry-wide hunt, let us tell you: There is no single, definitive figure on the cost of security incidents.

Oh, there are data points. The problem is that they don't agree. Heck, they aren't even in the same ballpark. Check 'em out:

- In a study of Department of Justice data scheduled to be published Aug. 28, Phoenix Technologies and law enforcement agencies found that, in cases where stolen IDs and passwords were used, the average loss per incident was \$1.5 million. Some attacks caused as much as \$10 million in damages.
- According to the annual report by the Computer Security Institute and the FBI, the average loss per company due to security breaches in 2005 was about \$167,000, down from more than \$200,000 the year before. About half of the respondents reported between one and five incidents during the year.
- In a study conducted by Ponemon Institute and distributed by PGP Corp. last year, companies lost an average of \$14 million per breach per incident when customer data losses were incurred. The high cost was as much as \$50 million.
- A recent survey by the Yankee Group indicates that more than half of companies rate their Internet downtime costs at more than \$1,000 per hour.
- In a study published in 2004, the Aberdeen Group found that the cost of Internet-based business disruptions is about \$2 million per incident.

So, pick your number. Some rules of thumb say that \$100,000 is a good starting point when measuring average loss per incident. Some say \$200,000. Some say \$1,000 per hour.

"Take all studies with a grain of salt," says Rob Enderle, principal analyst with the Enderle Group, an IT consultancy. "Before you use the results, understand where you can trust them."

"Business risk is highly context sensitive and depends on both the business in question and the technical defect," says Gary McGraw, CTO of Cigital, a security consulting firm. "The same kind of bug in two different programs can lead to very different impact estimations. Anyone who tries to stand way back and squint at the whole picture is a simpleton."

Even the organizations that do the studies concede that they are often unscientific.

"There's no uniform financial accounting for cybercrime losses," notes Robert Richardson, editorial director at the Computer Security Institute. "What respondents give to these sorts of surveys are estimates. I think their estimates are interesting, and I think it probably says something that their cumulative estimates [of losses due to breaches] have dropped over the past few years. But there are a lot of reasons why that might happen, so you have to supply your own interpretations."

It might be attractive to use a generally-accepted industry figure to benchmark the costs of a hack, experts say, but there aren't any figures that the entire industry agrees upon. And even if there were, such industry-oriented figures probably could not be plugged into the risk assessment of any single company, where the variables may be quite different than the average.

Cost-justifying security purchases means making a customized evaluation of the potential threat and the damages it might cause, experts say. While there are many outsourcing companies that will conduct such a risk assessment, such as Accenture or PricewaterhouseCoopers, most companies can handle it inhouse.

"You list the likely risks and then calculate the cost of doing nothing," says Enderle. "You then have a baseline to measure the different security solutions against, both physical and electronic. You then prioritize them based on the positive financial impact that each has on the cost of doing nothing. Those that provide a reasonable return are viable."

In simple terms, you can calculate risk by estimating the cost of an incident and multiplying it by the probability that the incident will occur, experts say. There are many factors that can be included in the damage costs, including the cost of employee downtime, the cost of repairing the problem, and the cost of any lost business. Some companies add soft costs, such as damage to the brand that may occur as a result of a public breach or data theft.

Such calculations cannot be made using industry data, experts say. "A random study, unless it is well performed, is not something you want to base the protection of millions or billions of dollars on," says Ira Winkler, author of *The Spies Among Us*. "You need to see trends in attacks, and figure out where you are vulnerable. Study numbers are irrelevant compared to basic risk management."

Despite the consensus that enterprises should conduct their own risk analysis, most experts expect IT and security departments to continue to use more convenient industry numbers to justify their purchases. "Industry studies will continue to be actually used in decision making, no matter how bad they are," Enderle says. "[IT people] want an answer and, regardless of how good the answer is, they will gravitate to those who give them one."

— Tim Wilson, Site Editor, [*Dark Reading*](#)