BUSINESS **SOLUTIONS**

Calculating the cost of a security breach

Last Updated: 01/17/08

Executive Summary

Security breaches are costly and fast becoming more costly. The fines and the public relations problems aren't the only penalties, and companies that hold financial or health information are not the only ones that can be victimized.

Breach of Security, Breach of Trust Can Carry Big Costs

Security breaches happen all the time, to computer networks everywhere. However, some breaches are much more costly than others: those where personal information is exposed for possible use in criminal activities. Security breaches involving private records are also breaches of trust, and companies are learning that these carry stiff penalties.

For example, the U.S. Federal Trade Commission assessed ChoicePoint Corporation, a provider of identification and credential verification services, $15 million in fines and penalties for a data breach where fraudulent companies were able to access the personal information of 163,000 customers. But even worse can happen.

CardSystems, a credit card processor, closed its doors and had its assets purchased by another firm following a breach that exposed the names, account numbers and expiration dates of as many as 40 million credit card holders. The company had violated the terms of its contracts with Visa, American Express and others by not encrypting the information and by storing credit card verification numbers.

The business cost of breaches involving private data is high and getting higher. Ponemon Institute, an organization dedicated to advancing responsible information and privacy management, which has been surveying data-breach costs since 2005, released a study in November 2007 showing that the average cost of a security breach has gone up almost 90 percent in just two years since the first study.

The cost of a single breach is now $6.3 million. Companies spent an average of $197 for each lost record – investigating the breach, notifying customers, restoring security infrastructures and recovering lost business. Forrester Research, in a survey of 28 companies, found a range of cost from $99 to $305 per lost record.

And the problem isn't going away. Privacy Rights Clearinghouse (privacyrights.org), an organization that offers information on how to protect personal privacy, reported 312 recorded security breaches involving personal data from January 1 through December 6, 2007.

Since January 2005, when the organization began compiling its list, security breaches have exposed more than 216 million data records of U.S. residents. The list includes organizations of all sizes: financial services companies, insurance companies, healthcare companies, colleges and universities, government agencies and more.

The number of records compromised in each incident ranges from a dozen to tens of millions. All these incidents have at least two things in common: they all involve real costs, and they are all visible to the public.

Your company is probably at risk, too

Almost every company network — and almost certainly including yours — contains some kind of sensitive business or personal-identity information like banking and payroll. Your company is responsible for the security of that kind of information. And with regulatory agencies and industry groups focusing on the problem, all sizes of companies may face penalties for security breaches.

A compromised system, a lost backup tape, a stolen notebook computer or a disgruntled or careless employee can expose your company to a wide range of unfortunate consequences if you allow unencrypted private data to be exposed. It doesn't matter whether data thieves penetrated your security to steal the information or whether one of your employees mishandled it. It doesn't even matter whether the lost information is actually used to commit fraud.

Besides personal information, there's likely a lot of other types of sensitive data on your network: trade secrets, customer information, intellectual property and more. It's difficult to put a monetary value on the exposure or loss of this kind of information. But it could be substantial, and it is certainly more than the cost of protecting it.

How many ways does a security breach cost?

The big fines make the news, but a security breach carries many other costs. Here's a quick list of all the expenses that your company might face in the event of a serious security breach – in case you need more support to persuade management to increase funding for network security.

By the way, Darwin Professional Underwriters, a specialty liability insurance products provider, has an online Data Loss Calculator that makes it easy to estimate the total cost of a security breach, based on the number of records affected and the various costs your company might incur. The calculator is at www.Tech-404.com/calculator.html.

- *Customer Notification and Follow-Up.* You'll have to contact every person whose information has been put at risk, which means letters, envelopes, postage, a call center or hotline and any special promotions aimed at regaining customer trust. In some cases, organizations responsible for breaches (e.g. LexisNexis and Fidelity Investments) are paying for credit monitoring services to help customers track and protect their credit records.

- *Lost Customers.* Depending on the business you are in, customer migration could be severe. And the cost and time needed for replacing customers is significant. Because data theft is frequently in the news, more and more people are acutely aware of the risks of data theft, and they are growing less likely to be forgiving.

- *Legal Costs.* You will need outside attorneys to guide you through the aftermath of a breach, especially if you violated any government regulations. You might even need them to defend you against civil actions, even though so far courts have not awarded any damages where actual losses could not be proved.

- *Customer Restitution.* ChoicePoint was the first, and so far the only company that has had to pay restitution costs to affected individuals. The company established a $5 million fund for that purpose, so a precedent has been set, and restitution is likely to become more common.

- *Damage to Brand and Company Image.* This is difficult to quantify, but think about all the effort and money your company has spent building its image or brand in the marketplace. Then imagine how much of that spending has been sacrificed and how much it will cost to rebuild your reputation.

- *Regulatory Fines and Penalties.* If your company is subject to government regulations like Sarbanes-Oxley, HIPAA (Health Insurance Portability and Accountability Act) and the Gramm-Leach-Bliley Act, or to industry guidelines like the Payment Card Industry (PCI) data security standards, you will likely face fines or penalties, which can be substantial. As noted above, the FTC fined ChoicePoint $15 million. In addition, following in California's footsteps, many states have passed or are working on data-security laws that will carry significant penalties.

- *Increased Security and Audit Requirements.* You won't be able to return to business as usual following a breach. Count on having to upgrade your security program and perhaps having to comply with elevated security audit requirements.

- *Employee Downtime.* Employee productivity will likely suffer for some period following a breach, and not just in the IT department. In fact, a Forrester Research study found that lost employee productivity cost about $30 per lost record in 2006, about double what it was in 2005.

Let CDW help you protect your network data

The bottom line for your company is that you need to take steps to prevent costly security breaches. A good place to start is with your CDW account manager. He or she can put you together with CDW-trained security technology specialists to develop a custom security plan for your business. If you don't have an account manager yet, call (800) 985-4239.