SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Protecting Companies from Identity Theft

Organizations must think company-wide and across public/private barriers to prevent data breaches

Marleah Blades

Originally Published in Security InfoWatch.com
October 2008

Protecting Companies from Identity Theft

Organizations must think company-wide and across public/private barriers to prevent data breaches

A man walking down an empty residential street opens a mailbox and shoves its contents — including a credit card statement containing four convenience checks — into his jacket. A hacker breaks into a corporate database and downloads information on all the company's 1,200 employees. A group collects social security numbers from a phishing scam that asks e-mail recipients to update their personal information on a sham Web site.
Teenagers watch a retail employee throwing paper transaction logs into a trash bin behind a shopping center and dig them out once she's gone. An organized gang pays a hospital worker to hand over the medical or insurance information of patients in bulk.

The problem with identity theft is that it is all of these things, and its results include all types of fraud, from credit card and check fraud to medical and government benefits fraud, as well as blackmail. Because identity theft is such a broad and perhaps ill-defined crime category, it is often shrouded in misconceptions, and its potential as a damaging threat is often underestimated.

In most of the above scenarios, the consumer is the immediate intended victim who stands to lose from the information theft. Businesses and organizations — the corporation whose database is breached, the company whose logo is on the phishing e-mail, the retailer whose dumpster is searched, the hospital and the insurance companies that lose patient information — also stand to suffer significant long-term consequences.

A Rampant Problem

There is no way to accurately estimate the number of identity thefts that occur annually. Many companies and organizations track reported cases of various types of identity theft, but few can monitor every method, and since the crime may go undiscovered or unreported for a long time, it is possible that existing estimates are the tip of the iceberg. Several estimates place the number of incidents between 8 and 10 million each year. The Identity Theft Resource Center, which continually catalogues confirmed electronic and paper data breaches, reports 259 breaches in 2008 as of May 13, with nearly 12 million individual records exposed.

More than 4 million of those records are accounted for by a major security breach reported by Hannaford Brothers supermarkets in March. This immense theft of credit and debit card numbers has already led to at least 1,800 confirmed cases of fraud.

It is this type of breach that sends shivers up the spines of retailers, banks and other companies that handle financial data. Whereas other types of identity theft, like the recovery of paper records outside a store, generally impact a limited number of customers and may easily duck attention, the high-level financial data security breach quickly exposes millions of records, making for spectacular headline news.

Potential Costs in the Billions

Last year, Forrester Research released a study called “Calculating the Cost of a Security Breach” that estimated the business costs of data breach at anywhere from $90 to $305 per customer record, depending on the type of company and the profile of the breach. When millions of accounts are exposed, the final figure is staggering.

Impacted businesses must front the cost of notifying customers of the breach, satisfying applicable fines, paying legal fees, instituting new protections, and investigating complaints. And in theft of credit card data specifically, victimized consumers are generally not held responsible for fraudulent charges, so banks or businesses end up bearing the direct financial losses.

Reputational loss and the loss of future sales take a toll as well. An online survey conducted by the Business Software Alliance and Harris Interactive in 2006 found that 30 percent of adults said they felt compelled to shop online less or not at all during the 2005/2006 holiday season because of security fears. Also, when the data exposed in a breach is financial, it seems to elicit a stronger response from consumers than, say, the loss of social security numbers or birth dates, because the danger feels more immediate and hits them where it hurts: in their bank accounts.

The Finger Points at Security

Any damage to the company as a whole is damaging to security, because the bottom line impacts every business unit. But in the case of a network breach, security is directly in the line of fire. When senior management and the board come to find out how this could have happened, they will head straight for security’s door. Fortunately, it seems that security is not always the sacrificial lamb anymore. Security executives at companies that have suffered some of the biggest breaches in recent years still have their jobs. But if major breaches occur, the public may call for the ousting of security leaders, their reputation will suffer inside and outside of the company, and they likely won't escape public embarrassment, since news outlets will be scouring their records and actions to find the hole that allowed the compromise.

Protecting from the Inside

There are a number of things companies can do to protect themselves. The right defenses depend upon the type of company, its level of sophistication or experience in information protection, and how it stores and transmits different types of information. But all organizations should begin the hardening process with a comprehensive risk assessment that is regularly re-evaluated. If your organization does not have the expertise to do this in-house, hire a consultant to help you through the process. The risk assessment is the only way to identify the appropriate measures to shore up the holes in your organization's security program.

The risk assessment is also a requirement of nearly every law, guideline and regulation governing the protection of sensitive information. Most industries and sectors are now subject to their own information protection requirements, with heavy fines and penalties for noncompliance. (For a partial list of security-related guidelines and regulations, visit **https://www.securityexecutivecouncil.com/public/lrvc**.)

These guidelines and requirements should be viewed as a help to the security program, not a hindrance. They provide guidance on how to prevent common attacks in various industries, taking some of the guesswork out of the risk mitigation process. However, compliance with the applicable laws and standards still does not guarantee protection against data breach. Hannaford Brothers was compliant with the PCI Data Security Standards when its network was compromised.

"Compliance is helpful, but compliance does not equal security," says Tony Heredia, Director of Investigations and Assets Protection for Target Corp. According to Heredia, private industry must partner with the public sector to investigate and prevent data breaches if they hope to protect themselves from this threat.

Preventing Through Partnership

"There are two key reasons this problem needs to be addressed jointly," says Heredia. "First, the criminals who set out to breach networks are intent on beating any technological advances that are in place. They are spending all their time — 24 hours a day — figuring that out. So you can't prevent everything with technology.

"Second, when something does happen, businesses need to partner with law enforcement to investigate it and rely on the criminal justice system to bring these people to justice. Both those groups need to understand the threat from a private-sector perspective, and they need the cooperation and help of the business' investigative resources."

Target believes this strongly enough to put their money where their mouth is. The company has been funding analysts at the National Cyber-Forensics and Training Alliance (NCFTA), which brings together subject matter experts from industry, academia, and government to provide advanced training and forensic analysis to reduce cyber vulnerability. Target has also positioned a full-time investigator at the FBI's Internet Crime Complaint Center for the last few years.

Public/private partnerships are useful for prevention as well as for investigation and prosecution. Says Heredia: "The Secret Service works with the Carnegie Mellon CERT Institute every year to do a survey of the private sector to better understand the trends around network breaches, network intrusions and personal information theft, and the more aware law enforcement is of what's going on in those enterprises, the better equipped they will be to handle those kinds of investigations."

Shared information about how a company's networks are constructed, the kinds of things being seen in their intrusion detection system, and what the virus software is picking up can help crime labs and groups like the NCFTA develop better parameters to detect this activity before it causes damage and makes headlines.

***Special thanks to Dick Lefler, managing partner of the Business Security Advisory Group, former CSO of American Express and faculty emeritus of the Security Executive Council, for sharing his insights and resources for the development of this article.*

Marleah Blades is former Senior Editor for the Security Executive Council. Prior to joining the Security Executive Council she served for *six years as managing editor of Security Technology & Design magazine.*

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year “retained” services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com