YOUR DATA IS SHOWING: WHAT'S NEXT IN IDENTITY PROTECTION

By Bryan Hjelm, Vice President of Product and Marketing

CSID®
A part of Experian

APRIL 2013

INTRODUCTION

When it comes to stealing identities, criminals will follow the money. Ten years ago, this meant stealing credit and debit card information to make unauthorized purchases and using stolen Social Security numbers to create new identities and open lines of credit. Today, the information that is valuable to an identity thief is shifting to seemingly harmless details like email addresses and passwords, mothers' maiden names and dates of birth, even high school mascots and pet names. As we share more online, from personal information on social media sites, to business information in the cloud, it becomes exponentially more difficult for businesses and consumers to protect themselves from identity theft and the repercussions of sharing too much information online.

The problem is, when it comes to protecting the personal information of employees and customers, businesses aren't making the shift with the identity thieves. 2011 saw more than 174 million records compromised in data breaches, costing businesses $5.5 million per breach in monetary damages—not including brand damages. With 2012 numbers expected to come in high and 2013 on track to be equally as disastrous, the questions that become increasingly urgent are how do we fix this? What can business do to protect employees and customer credentials? What can be done to mitigate the billions of dollars worth of damages that stolen credentials are inflicting on businesses?

WHAT'S NEXT

Monitoring Breach Data to Reduce Risk

When a breach occurs, the stolen information is often posted on a site like PasteBin that is considered public domain. As a business, you can monitor this information for consumer credentials, and then take proactive measures like asking the consumer to change his/her password for potential compromised accounts.

Proactive monitoring is done in real-time, which means a business can learn that an employee email address or password of customer database has been compromised the instant it is posted on a chat room, website or message board. This gives businesses the opportunity to react to the compromised information and subsequently mitigate the impact and risk of that stolen credential. With data being sourced from the CSID, a part of Experian, Enterprise Threat Intelligence (ETI) technology, companies can discover when a customer's email address, password or other personal information is found to be compromised—even if that exposure had nothing to do with the company doing the monitoring.

The second, and new, component to proactive monitoring is identifying company devices with compromised IP addresses. Most compromised credentials are stolen via malware. Most malware does two things: collects information from the compromised device and sends out spam to infect additional computers. Via proactive monitoring, businesses are able to identify the IP addresses of devices that are sending spam emails. A business can then evaluate the situation, identify what data may have been compromised and fix the device so it is no longer infected. CSID's ETI technology identifies nearly eight million compromised IP addresses every 14 days.

Behavioral Monitoring

Some companies assume all credentials are bad—that all passwords have been compromised. Rather than spend time protecting the credential, these companies focus on early detection and responding quickly to abnormal behaviors. For example, if a consumer has never used their bank account to transfer money, but all of a sudden tries to transfer a large amount to an unknown account, the bank can raise a red flag and prohibit or limit the transaction without some sort of additional verification. In a more business-oriented example, behavioral monitoring could involve monitoring an employee's current behavior against his historic use of a system. So if an employee suddenly tries to download an entire database of customer email addresses, when historically he has never needed access that information, an alert can be raised and company IT can act quickly to mitigate any damage in the event of a breach.

With the increasing popularity of big data and cloud computing, businesses have access to more complete profiles of user behavior. One example of behavioral monitoring that we could see in the near future is the use of smartphones to verify identity. Carriers can pinpoint where a smartphone is at any given time. If a business can tap into this information, it can use it, along with historical information of the places you normally work—the office, home, a near-by coffee shop—to determine if a user is accessing data from a common location or not. The system can then ask for additional verification if information is being accessed from a unique location.

Behavioral monitoring is an emerging way to both get ahead of and mitigate the impact of data breaches. Breaches and system misuse can be identified in real time and measures can be taken to stop it.

Two-Factor Authentication

Authentication factors include something the user knows (a password or PIN), something the user has (an ATM card, mobile device or smart card) and something the user is (a biometric characteristic, such as a voiceprint or fingerprint). A business needs to have a least two of these authentication methods in place for good security from an identity standpoint.

Passwords alone are not secure, but they are easy to use for consumers and employees. The problem is, they are easy to crack for the criminals as well. You can make passwords more secure by supplementing them with a second authentication

WHAT'S NEXT

method, and businesses are starting to do so. Traditional two-factor authentication methods have included tokens, smartcards and one-time SMS passwords. Two-factor authentication methods are evolving to include biometrics and pervasive computing. One such example is software being developed by security firm, Scout Analytics. Their software works with a user's keyboard to measure cadence and rhythm and determine if the correct user is logging in to a system. The user doesn't have to do anything extra aside from entering their login – the software works with the keyboard to implement the second authentication method. Systems like Scout Analytics' keyboard software have not reached the reliability level needed for widespread implementation, but they are getting there. It's only a matter of time until users are using their voices, fingerprints or other inherent traits to log into some systems.

Social Media Monitoring

According to Pew Internet Project, 67 percent of adults use a social networking site . With social media now an integral part of our lives, it makes it easier for criminals to find out personal information that was once much more elusive, information like date of birth, mother's maiden name and even seemingly trivial facts like a pet's name or a high school mascot that are often used as security questions on financial websites. This opens the door for those with bad intentions to steal credentials, identities and more.

Going beyond identity theft, what individuals share online can also harm their reputation. Employers are now checking social media sites as they vet applicants. College admissions officers check Facebook and Twitter to see if a potential student's online persona matches their admissions application.

To address this growing trend of sharing sensitive information online, businesses have started developing social monitoring products that send an alert to a subscriber when something they shared online could be potential harmful – both to their reputation and risk of identity theft. But it's difficult to get social monitoring right, and no business seems to have cracked the code just yet. Privacy and Terms of Use policies make it difficult for some products to scrape social sites without user credentials, and for parents trying to monitor their children, for example, these aren't always easy to obtain.

Child ID Theft

One additional area where new products and technologies are quickly emerging is child identity theft monitoring. According to a 2011 study conducted by Carnegie Mellon University's CyLab, children are 51 times more likely to have their identities stolen than adults. , Most children have unused social security numbers that an identity thief can pair with any name and birthdate and then use to open a line of credit or apply for a job. The probability of this theft is low because a child's credit files largely go unused or unnoticed until they are 18.

CSID recently conducted a study that revealed more than half of parents are aware that child identity theft is a growing issue, and more than three-fourths are concerned that their child's identity might be stolen. But, the results also revealed that despite these conclusions, more than half of parents are not currently taking active measures to prevent misuse of their child's personal information. The survey does demonstrate a willingness to take action and as a result, some identity protection and fraud detection businesses are taking child-monitoring products to market, or adding them to already existing product line-ups. These products monitor a child's social security number and credit report for fraud. Utah, Maryland and Rhode Island have also put legislation in place that gives free credit checks to minors via their parents and guardians, and other states, such as Florida, are close to following suit.

Public Web Monitoring

Online information aggregators and people finder sites collect publicly available information about individuals in one easily searchable website, often providing personal information as specific as street name, marital status, parent's names and occupation. The identity theft implications of services like this are obvious but the actions individuals can take to remove the sensitive information from online sources are limited and time-consuming.

New services are launching that do the heavy lifting involved with removing sensitive information from online sites. The company will

WHAT'S NEXT

contact data brokers and request information removal. In instances where an individual or business' action is required, the service will send specific instructions ensuring all private and personal information is removed from the web.

Small Business Protection

According to the 2013 Symantec Internet Security Threat Report, 50 percent of all targeted cyber attacks in 2012 were aimed at businesses with fewer than 2,500 employees. Thirty-one percent of attacks were aimed at businesses with fewer than 250 employees. These stats are telling. Small businesses are increasingly becoming a target for hackers.

There are numerous reasons for this. The first is small business owners normally don't have the time or resources to focus on security the way an enterprise business does. According to the National Cyber Security Alliance, 83 percent of small businesses have no formal cyber security plan, while 69 percent lack an informal one. Additionally, many small business owners feel like they aren't at risk. Why go after a mom-and-pop shop when the potential rewards are so much greater if a hacker goes after a larger company? The reason - small businesses often offer the path of least resistance when it comes to security, making them a desirable target.

An emerging trend in security monitoring for small businesses is proactive monitoring for compromised credentials – credentials that are both inside and outside of the business' ecosystem. For example, a stolen email or password can be used to delve deeper into a company's system and access sensitive and valuable data. This exact scenario happened in the state of South Carolina in 2012 when a hacker used the credentials of a South Carolina Department of Revenue employee to gain access to more than 3.6 million Social Security numbers, 387,000 encrypted credit and debit card numbers and the login credentials for an additional 250 employees. Over the course of the three-month breach, a hacker compromised 44 systems on 21 different state servers using 33 unique pieces of malware and four employee user accounts. This one breach cost the state more than $14 million to resolve.

The severity of this problem is further compounded when you consider that a compromised credential outside of a company's ecosystem could still pose a risk to the company. In a 2012 survey on consumer password habits, CSID found that 61 percent of people reuse the same password across multiple websites and 44 percent of consumers change their password once a year or less.

Yet 89 percent of consumers felt secure with their current password habits. Based off of these research findings, it stands to reason that employees use the same login credentials for both work and personal use and a credential stolen from a personal website can compromise the business.

Proactive monitoring services can keep tabs on a number of company credentials including employee passwords, email addresses and business credit statements, credit card and debit card numbers. The business can then secure the compromised device and quickly respond to any stolen information or credentials.

Proactive credential monitoring is going to become increasingly important for small businesses as hackers continue to increase their focus on these easy targets. When coupled with traditional security measures like anti-virus software and firewall protection, and supplemented by protective measures like identity theft insurance, proactive monitoring can provide small businesses a more complete defense against theft.

ABOUT CSID

CSID

CSID, a part of Experian, is a leading provider of global identity protection and fraud detection technologies for businesses, their employees, and consumers. With CSID's enterprise-level solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world. CSID's comprehensive identity protection services extend beyond credit monitoring to include a full suite of identity monitoring and fraud detection services; identity theft insurance provided under policies issued to CSID; full-service restoration services; and proactive data breach services.

Methodology

CSID and digital data collection firm Research Now teamed up to survey a demographically representative sample of 150 owners of small businesses in the U.S. with 1-10 employees from the Research Now Small Business Owners Panel. The sample framework is balanced based on industry, vertical, number of employees, annual revenue, years in business, legal entity type and personal service business types.

Contact Us

Join CSID on Facebook at facebook.com/CSID and on Twitter at @CSIdentity.

For more information, please contact Director of Marketing, Cody Gredler at cgredler@csid.com.

Sources: 2012 Data Breach Investigations Report, Verizon Enterprise) | 2011 Annual Study: U.S. Cost of a Data Breach | Pew Internet: Social Network, 2012 | Child Identity Theft: New Evidence Indicates Identity Thieves Target Children for Unused Social Security Numbers | Child Identity Theft: A Parenting Blind Spot, CSID, 2013 | New Law Aims at Child ID Theft, ABC, 2013

LEARN MORE AT

CSID.COM