Proactive Credential Monitoring as a Method of Fraud Prevention and Risk Mitigation

By Marc Ostryniec, vice president, CSID

The increase in volume, severity, publicity and fallout of recent data breaches and cyber attacks has taken the topics of cyber-security, data protection and breach mitigation to new heights. While consumers who have had their personal information compromised in data breaches now have numerous options to monitor their identities and guard against becoming victims of fraud, can the same thing be said for businesses?

Billions of dollars are spent each year protecting businesses from security breaches, viruses, malware and hacking attempts. While companies have been increasing their security protocols and data breach mitigation plans to safeguard their data, an emerging topic addresses vulnerabilities and potential attack vectors that businesses may face resulting from situations completely out of their control and that are virtually impossible to detect – user credentials exposed outside of their own enterprise. Even if an enterprise's infrastructure is secure, often times the biggest risk lurks outside of the walls of an organization in the form of data trails left by employees and customers.

The inherent problem with data security is human fallibility. An enterprise may have the most sophisticated security systems in place, however if there is a human component to that system, there will be vulnerabilities. Simply put, employees and customers are the weakest link in the data security process. They share information on social networks, at business events and when shopping online. They inadvertently click on phishing links that download malware or viruses to company systems.

Business security systems have not evolved enough to account for human fallibility. Take, for example, last year's RSA SecurID breach. The breach started as a phishing email that was sent to numerous low-level employees at RSA. One employee clicked on an attachment in the email that downloaded a Trojan to the user's PC. Hackers then exploited the Trojan to secure credentials for individuals from the IT department and other employees until they worked their way up to a level that allowed them to access and transfer the SecurID information. RSA's security systems were in place and working fine. It was one unwitting employee that downloaded a Trojan that exposed the company's networks.

Human fallibility doesn't stop at downloading a virus or clicking on the wrong link. An email or password compromised from one company's data breach can open up vulnerabilities across a multitude of completely unrelated websites such as banking, financial, online retailers and the like. Free software programs available in black market chatrooms, where stolen information is frequently bought and sold, let hackers quickly test email and password combinations against high-value web sites

with the explicit goal of exposing other sites to fraud and misuse. A compromised email address is one of the most insidious credentials because it can easily be used to reset and retrieve passwords to gain access and take control of additional accounts.

Security firm Trusteer conducted a study of more than four million online banking users and found that 73 percent use their online banking password at other websites, and more than 50 percent use the same exact user name across multiple sites.[1]

The severity of this problem is further compounded when you consider that these compromised credentials could provide a direct route through the front door of a company – similar to what happened to RSA during the SecurID breach. If an email and password for an executive or IT employee is stolen, a hacker no longer has to worry about beating the company's security systems and evading anti-intrusion technology. They simply have to login and start stealing and destroying. It takes only one compromised email account to impair an organization with key loggers and other malware that may lead to further exposure that can cause far-reaching and potentially irreparable damage to the business.

These scenarios underlie a profitable, thriving cybercrime industry that does not show signs of slowing down or going away. According to Symantec's Norton CyberCrime report for 2011, business is good for data thieves. The report estimates that in the last year, 431 million adults, worldwide, were victims of cybercrime, with the total cost of those crimes coming to around $114 billion dollars.[2] According to a March 2011 Ponemon research report, *2010 Annual Study: U.S. Cost of a Data Breach,* negligence accounted for 41 percent of reported breaches.[3]

Proactive Credential Monitoring

The profitability of the cybercrime industry illustrates the rise and severity cyber attacks can have on businesses. Instead of merely trusting that firewalls and intrusion-detection technologies will do the job, businesses now must factor in the human component to their security systems and figure out how to protect valuable company, employee and customer data.

The most apparent way to limit the impact of human error on a security system is education - ensuring that employees and customers know how to handle sensitive data, how to detect emails that may contain malware or phishing schemes, how to identify websites and links that will infect a system with a virus and other general knowledge such as not leaving sensitive information unencrypted on a laptop. Security education is an ongoing process, a long process and doesn't address the immediate and increasing need for mitigating the human component of data security.

A second method of mitigating fraud exposure and risk to an organization is to proactively monitor for customer or employee information on black market chatrooms, message boards and websites where stolen information is commonly bought and sold. The challenge is doing this monitoring consistently, on a global scale. With data being sourced from CSID's CyberAgent® 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. CyberAgent can provide this information in real-time so companies can address exposure quickly and effectively.

For example, if an online retailer discovers that a customer's information has been compromised, even if it had nothing to do with that online retailers' website, that retailer can take action such as requiring a second form of authentication or forcing a reset of the customer's password before the user can access the system or make a purchase. Similarly, if a business finds that an employee's email address, password or system login information has been compromised, they can proactively reset the employee's credentials, thereby reducing the risk of a hacker accessing the businesses systems via the employee's login information. This new method of proactive monitoring can produce a clear business case through which minimal costs result in a direct and measureable reduction in corporate risk and fraud loss. Additionally, proactive monitoring can have a positive impact on customer retention and churn by reducing the instances of negative consumer experiences due to fraudulent transactions.

While there is great appeal in proactively monitoring customer and employee credentials, this approach also opens up interesting ethical and security questions of its own including discussion for customer and employee privacy rights and whether or not online entities have the right to be monitoring for this information without the customer or employee's explicit knowledge or permission. While the harvested information is technically sourced from the public domain – the online black market - and is completely within the rights of a corporation to take action for their credentials, questions are surfacing about whether companies should inform their customers why they are taking extra steps to reset passwords and to what level an employer should be informed about what their employees do online.

Privacy is a growing concern for online users, who are increasingly trusting more personal information to online services, mobile apps and the cloud. This year, the White House announced it is working on a framework for protecting consumer online privacy. This framework will call upon businesses to be more open with what information they collect from and for users, what they do with it, how they store it and give consumers the option to opt out of information tracking. Although it is not clear what this framework will look like in its final iteration, or if it will be voluntary or made law, it does denote a trend towards more transparent notification of what customer and employee information businesses track and collect.

While the above-mentioned safeguards are being put into place for mostly marketing and tracking purposes, it stands to reason they could apply to monitoring for customer and employee information for security purposes as well. An employee may not want their employer to know they have a certain credit card. Similarly, an online retailer shouldn't have access to a customer's date of birth or social security number if the customer hasn't volunteered that information. Even more alarming is the scenario of a business potentially being given the compromised credentials of a competitor. While clearly unethical, it provides a simple mechanism that one business could then use those credentials to access a competitor's system and do what the hackers did during the RSA SecurID breach.

The answer lies somewhere in the middle. All of this information could, conceivably be found by anyone with the knowledge and aptitude and there are simple ways to minimize the exposure and propagation of certain forms of personally identifiable information such as social security numbers, dates of birth, and bank accounts. In spite of these ethical questions, it is increasingly imperative that businesses take the necessary steps to protect themselves and their customers from cyber attacks and human fallibility. Proactively monitoring for compromised credentials presents an inexpensive, immediate and effective way to address one of the most fundamental challenges in security and access control. Doing nothing is simply not an option.

References

[1] *Trusteer Finds That Two Thirds of Internet Users Reuse Their Online Banking Credentials on Other Websites*. Trusteer, 10 Feb. 2012. Web. 27 Feb. 2012. <http://www.trusteer.com/company/press/trusteer-finds-two-thirds-internet-users-reuse-their-online-banking-credentials-other->.

[2] *Norton CyberCrime Report for 2011.* Norton by Symantec. 8 Sept. 2011. Web. 27 Feb. 2012. <http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/>.

[3]Ponemon Institute. 3 *2010 Annual Study: U.S. Cost of a Data Breach.* Symantec. March 2011. Web. 27. Feb. 2012 <http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf>.

About CSID

CSID is the leading provider of global, enterprise-level identity protection and fraud detection technologies and solutions to the world's top companies and government organizations. With CSID's advanced enterprise-level solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world. Products go beyond credit monitoring and include full-service identity theft protection; insurance and restoration; identity authentication and voice biometrics; and proactive breach preparation from discovery to resolution. CSID is the leading provider of global, enterprise-level identity protection and fraud detection

technologies and solutions. The company's technologies power more than 70 percent of the retail identity protection industry.

About CyberAgent

- CSID's CyberAgent scours chat rooms, blogs, websites, peer-to-peer networks and other file sharing sources to identify the illegal trading and selling of personal identities. Cyber Agent has discovered millions of credit cards, compromised email addresses, and personal credentials including Social Security Numbers, phone numbers, and medical IDs.

Using a variety of data gathering techniques, such as chat room monitoring, spidering/crawler/scraping capabilities and forum extraction, CyberAgent locates large volumes of compromised credentials.