INFOARMOR
DETECTION IS THE NEW PREVENTION

How to Protect Sensitive Corporate Data against Security Vulnerabilities of Your Vendors

July 2014

Executive Summary

Data breaches cost organizations millions and sometimes even billions of dollars in legal and remediation costs, loss of stock value, customer loss, reputation impact, and brand damage. The vendors that provide a variety of services to these organizations are now often the weakest link in the security chain. As a result, standard one-time or even periodic due diligence to screen and monitor the security profile of these third-party vendors is no longer sufficient. This white paper describes this challenge and a leading-practice solution that provides 1) comprehensive historical records on the data incidents of vendors to inform the vetting process upfront, and 2) continuous real-time monitoring of the security profile of vendors to aid ongoing incident avoidance and remediation.

Table of Contents

Your Company's Vendors Pose the Greatest Risk for Data Breaches

Third-party vendors are a growing source of risk to data breaches for organizations. In a recent study on the risks that vendors pose, Shared Assessments and Protiviti point out that "As the volume of outsourced products and services has surged in recent years, so, too, have the risks associated with vendors and third-party providers." [1] In the first quarter of 2014 alone, Risk Based Security tracked 669 incidents that exposed 176 million records – and 86 percent of these incidents involved outside the organization activity [2].

This means that third-party vendors have become the weak link in the security chain – either via digital threats or through physical access to vendor systems that hackers leverage. And when one vendor's data is compromised, a domino effect may occur in which dozens of companies that use the compromised vendor's services may be affected.

Over time, the number of data incidents is staggering. Risk Based Security alone has tracked 12,100 incidents that have exposed a total of 2.6 billion records. As the incidence of security breaches grows, organizations are being held accountable by customers, investors, and employees for the actions of their vendors. Few industries are immune, as incidents and breaches[1] have affected organizations in business (see sidebar), government, medical, and education [2]. InfoArmor tracks both compromised credentials (e.g., email addresses/usernames and passwords) and data incidents; the company currently identifies the compromise of 100,000-500,000 credentials daily.

Retailers under Fire in 2013

While the Target data breach has received much press due to the sheer magnitude of the breach (70 million shoppers' data was potentially compromised), other retailers also suffered from very large data breaches in 2013, making it the "year of the retailer breach," according to a Verizon report [3]. For the record, the Target breach occurred because one of its vendors – heating and air conditioning company Fazio Mechanical Services of Sharpsburg, Pennsylvania – was breached [4]. Retailer Neiman Marcus was the victim of a hack of about 350,000 credit cards from July to October 2013 [5]. Retail chain Michael's revealed in April 2014 that 2.6 million credit and debit cards may have been compromised from May to December 2013 [6]. These events are a reminder of the risks that companies with large, interconnected networks face in everyday dealings with suppliers.

The consequences of data breaches on organizations of all types are significant. In addition to the cost of remediating the breach, adverse impacts can include legal compliance and lawsuits, loss of stock value, reputation impact, customer loss, resignation of high-level executives, and brand damage. For example, the estimated cost of reissuing 21.8 million cards (less than a third of the number stolen in the Target breach) is $240 million [7]. Both the CEO and CIO of Target were forced to resign in the wake of the breach [8]. The ultimate cost of the breach may reach $1-$2 billion [9].

[1] A data "breach" is a breach of security with stolen data; a data "incident" is an event that exposes or is likely to expose data.

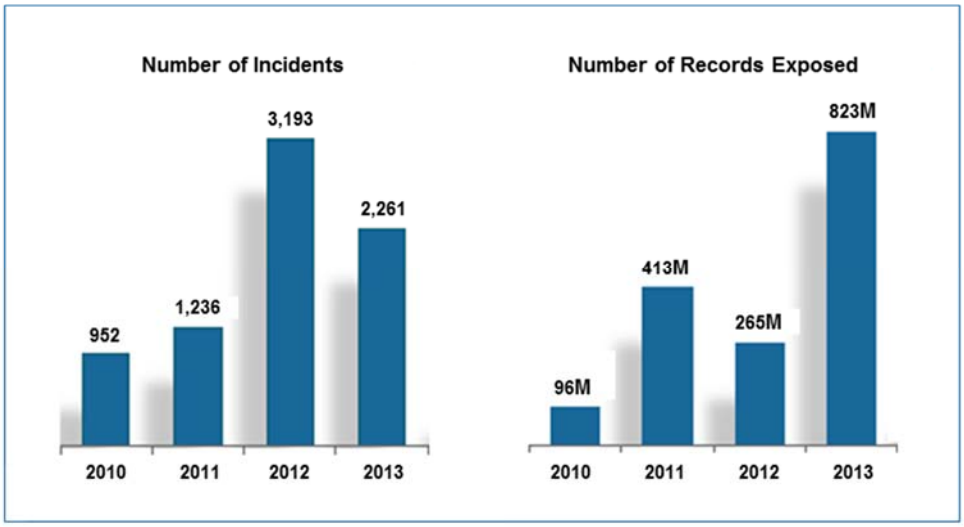

Figure 1. The number of data incidents and records exposed is increasing [2].

Increasing regulatory involvement in the management of third-party vendor risk is originating in the financial services sector and is likely to expand to other sectors. "The concern is not just breaches of customer information, but also compromise of intellectual property, which is obviously a concern of any company. So this is a widespread concern across industries, and particularly for quite some time in financial services."

"Due to the growing interconnectedness between companies and their supply chains, everyone is paying a lot of attention to vendor risk."

– **Marshall Toburen, GRC Strategist of RSA**

Regulatory guidelines and oversight are causing a paradigm shift in how organizations first vet and then monitor the risks posed by their third-party vendors. For example, the January 2014 version of the Federal Deposit Insurance Corporation (FDIC) Compliance Manual explains that the executive team of an insured institution is "ultimately responsible for managing the activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution." [10] In its December 2013 "Guidance on Managing Outsourcing Risk," The Federal Reserve issued "guidance to financial institutions to highlight the potential risks arising from the use of service providers and to describe the elements of an appropriate service provider risk management program." [11] The Shared Assessments/Protiviti report points out that other "standards and regulations with third-party risk implications" includes "Consumer Financial Protection Bureau (CFPB) regulations, ISO 27001/2, the Payment Card Industry (PCI) Security Standards Council's data security standards, Office of the Comptroller of the Currency (OCC) Third-Party Risk Guidance, and the National Institute of Standards and Technology (NIST's) Cybersecurity Framework." [1]

Today, There is No Way to Independently and Continually Monitor Vendor Security Posture

Existing practices for vetting third-party vendors provide no continuous monitoring of vendor data incidents and breaches. A vendor data security solution is needed that is continuous, objective, and easy to use within existing vendor management processes.

To vet and integrate new vendors, organizations typically conduct a process of due diligence in which they ask their potential new vendors to fill out questionnaires to assess technology and security risks. These questionnaires and risk management surveys are basically self-assessments, in which vendors check various boxes to indicate their procedures and involvement in past data breaches or incidents. Because most data incidents are discovered by third parties [3], these vendors may not even be aware of their involvement in, or responsibility for, data incidents. The responses to these questionnaires are often not independently verified. What's more, these surveys only provide a static snapshot of the vendor's security profile at the time of vetting. Even in the cases in which these self-assessments are systematically updated, the updates only reflect an unverified, static view of the vendor's security. When vendors do discover that they have been hacked, they may not reveal this for weeks or even months after the fact, which means that access to the data of the organization that hired the vendor may be comprised for a significant period without the organization's knowledge. Existing vendor security evaluation measures provide no ongoing, real-time way to monitor the security risks that these vendors may pose.

The potential consequences of data breaches in an organization due to third-party vendor risks indicates the need to extend beyond simple due diligence in today's environment.

Related approaches to vendor vetting provide little additional information to assess ongoing risks of working with vendors. Vendor credit monitoring, for example, does not offer visibility into data incidents. Traditional security processes in place at the organization or the vendor – such as antivirus software, firewalls, intrusion detection, and others – are not sufficient. In fact, they foster a false sense of security; they may seem to offer protection, but in fact, the number of recent data breaches and incidents have shown that these measures alone are ineffective. These trends call for an approach that complements existing measures.

Solution of Leading Practices for Real-Time Vendor Monitoring

InfoArmor now offers a first-in-class, software-as-a- service (SaaS) solution called Vendor Security Monitoring (VSM). This solution provides historical information on data incidents, breaches, and compromised credentials at vendors, as well ongoing monitoring of data incidents and breaches that occur at vendors. VSM enables organizations to enhance their security posture, protect their digital assets, and minimize their risk of data breaches by more thoroughly vetting new potential vendors upfront and by continuously monitoring vendors for security incidents, breaches, and compromised credentials.

The critical need for VSM is based on the premise that timely detection and remediation is the new prevention. All incidents and breaches in an organization's vendor ecosystem cannot be

prevented. However, if any data incident by any of an organization's vendors in their dealings with any organization is identified immediately, remedial action can be taken to contain the exposure, potentially eliminate or minimize the scope of a data breach, and identify ways to avoid further such incidents from occurring. The key is early detection and prompt action.

Only a system like VSM that monitors all data incidents in real-time can facilitate such a process. This approach can help organizations when they are vetting potential new vendors by examining historical records of data incidents, breaches, and compromised credentials. By examining the scope, severity, frequency, and other attributes of the incident history, the organization can make an informed decision as to whether the risks of working with this vendor are manageable. After a vendor becomes part of an organization's ecosystem, VSM continues to provide value by monitoring and immediately reporting any data incidents or breaches by the vendor. This enables organizations to monitor their vendor ecosystem in real-time in a proactive way.

The solution is powered by the PwnedList (pronounced "owned" list), a proprietary collection of security incidents and compromised credentials that has been meticulously collected for over a decade. To create this database, a team of highly skilled security professionals acts as the eyes and ears of its clients. They apply ethical, comprehensive practices to monitor data incidents and breaches, resulting the capture and categorization of more than 270 million compromised credentials in 17,800 data incidents to date. The information is obtained from hacker forums, web crawlers, data loss databases, hacker communities, the dark net, deep web, file sharing portals, key logger dumps, and malware logs. The team employs daily scanning and harvesting of data from these sources, and compiles and organizes this data into useful information. The result is a compendium of forensic data incident reports.

VSM Capabilities

Figure 2 shows an example of the sort of data that VSM provides to organizations on vendors. Organizations can first input a vendor name or domain, and VSM identifies all related domains, aliases, and affiliated companies to provide a comprehensive security posture of the vendor. Figure 2 shows a summary line for each of 13 different vendors for a particular organization. It indicates the date of the most recent incident, the number of incidents in the database, and the number of compromised credentials in the database.

By selecting any single vendor, Figure 3 shows more information on the data incidents that involved that vendor. This table provides a description of the incident, the date of the incident, and the type of incident.

To learn more about a particular incident or breach, users can select the incident and view more information (see Figure 4). In addition to displaying an indication of the severity of the breach, this screen also provides relevant links to media references to learn more about the breach.

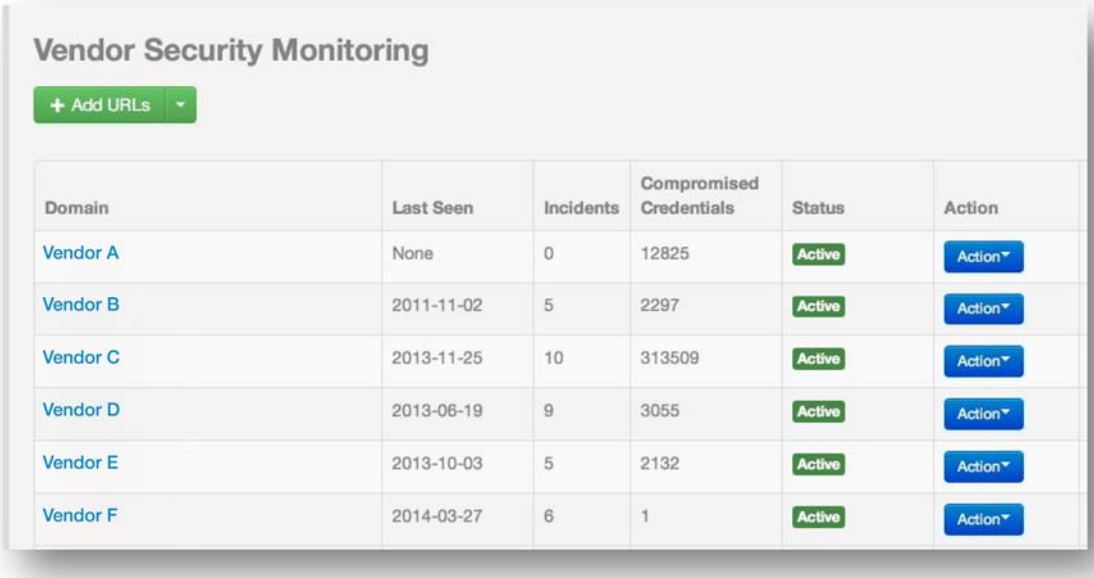

Figure 2. Vendor Security Monitoring: Summary List of Vendors

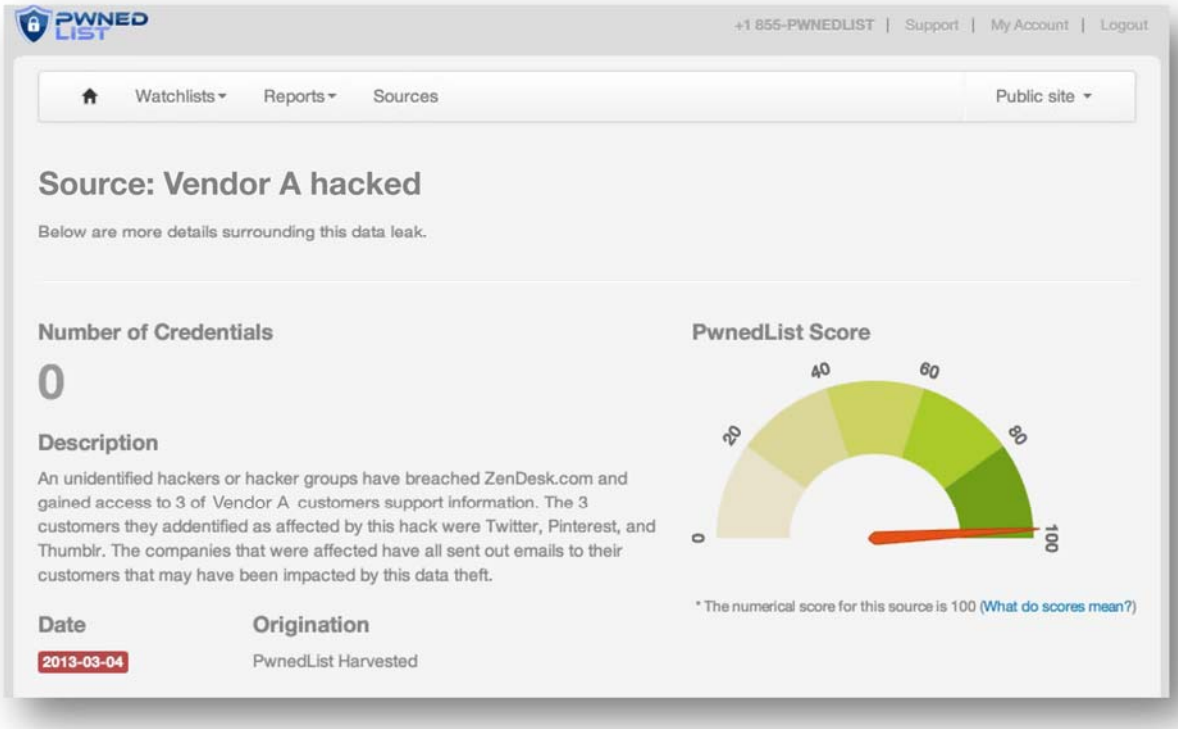

Figure 3. Vendor Security Monitoring: Detailed Information on a Particular Data Breach

The data is completely available and transparent to users. This enables users to conduct searches on a geographical basis, or by a particular group of cyber criminals (for example, if one group is targeting a specific organization or vendor), hashtag, and by other search criteria.

VSM provides email notifications when an incident occurs. In the case of an incident, VSM also provides guidance for organizations to implement an appropriate business response. The type of response depends on the scope, frequency, and type of breach or incident. The response process usually involves three phases. In the first step, the organization informs the vendor of the incident because the vendor may not yet be aware of it. The second step is to obtain confirmation from the vendor of the incident. The third step is then to identify existing impacts, identify potential future impacts, discuss remediation steps that the vendor is implementing, discuss additional prudent remediation measures for the vendor to implement, and discuss what steps can be implemented to prevent an incident like this one from happening again. The key here is to adopt a businesslike approach with open lines of communication early in the process.

Conclusion

InfoArmor's Vendor Security Monitoring provides an end-to-end solution to protect the digital assets of organizations from the data incidents and breaches of their vendors. The SaaS system is easy to use and provides real-time objective and actionable intelligence – a necessity in today's vendor ecosystem management

For More Information

For more information, contact info: sales@infoarmor.com or (800) 789-2720.

About InfoArmor

InfoArmor offers businesses industry-leading identity, privacy and data security services to help fight emerging fraud. Since data theft and digital fraud are current realities, InfoArmor believes detection is the new prevention. InfoArmor offers security-conscious businesses fraud-fighting tools that combine big data with actionable alerts and personalized service. InfoArmor was established in Scottsdale, Ariz., in 2007 to help Washington Mutual protect the identities of its 10 million credit card holders. In August of 2013, InfoArmor acquired PwnedList to strengthen its position as a data innovator by adding compromised credential monitoring to its suite of solutions.

References

1. Shared Assessments and Protivity, “2014 Vendor Risk Management Benchmark Study,” 2014, http://www.protiviti.com/en-US/Documents/Surveys/2014-Vendor-Risk-Management-Benchmark-Study.pdf.
2. Risk Based Security, Inc., and Open Security Foundation, “Data Breach Intelligence Reporting,” April 2014.
3. Verizon, “2014 Data Breach Investigations Report,” http://www.verizonenterprise.com/DBIR/2014/?gclid=CP_t8sa3k78CFQiUfgodsmEALg.
4. Stephanie Mlot, *PC Magazine*, “HVAC Vendor Confirms Link to Target Data Breach,” February 7, 2014, http://www.pcmag.com/article2/0,2817,2430505,00.asp.
5. Ben Elgin, Dune Lawrence, and Michael Riley, *Bloomberg Businessweek Technology,* “Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data,” February 21, 2014, http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data.
6. Mathew J. Schwartz, *InformationWeek,* “Michaels Data Breach Response: 7 Facts,” April 22, 2014, http://www.darkreading.com/attacks-breaches/michaels-data-breach-response-7-facts/d/d-id/1204630.
7. Christine DiGangi, *Credit.com* blog, “The Target Data Breach has Cost Banks $240 million…So Far,” February 21, 2014, http://blog.credit.com/2014/02/target-data-breach-cost-banks-240-million-76636/.
8. Associated Press, “Target CEO Gregg Steinhafel resigns following last year’s security breach,” May 5, 2014, http://www.wjla.com/articles/2014/05/target-ceo-fired-following-last-year-s-security-breach-102788.html.
9. Kathleen Caulderwood, *International Business Times*, “Damage from Massive Target Data Breach is Tough but Temporary,” May 5, 2014, http://www.ibtimes.com/damage-massive-target-data-breach-tough-temporary-1580348.
10. Federal Deposit Insurance Corporation (FDIC) Compliance Examination Manual, Section VII-4.1 Third Party Risk, updated January 2014, https://www.fdic.gov/regulations/compliance/manual/.
11. The Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulation; Division of Consumer and Community Affairs, “Guidance on Managing Outsourcing Risk,” December 5, 2013, http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf.