Data Security: Data Breaches

Deborah Cooper
The University of West Florida
United States
dlc50@students.uwf.edu

ABSTRACT: *This paper focuses on recent data breaches of two differing entities, Target (2013) and the U.S. Office of Personnel Management (2015). The number of accounts and people, as well as the personally identifiable financial information (PIFI) and personally identifiable information (PII), affected are discussed. Additionally, the lessons learned from each incident and the proposed or updated security measures implemented will be addressed.*

Keywords: Data breach, cybersecurity, data information systems, personally identifiable information (PII), personally identifiable financial information (PIFI), Target, Office of Personnel Management (OPM)

Received: 2 July 2016, Revised 11 August 2016, Accepted 19 August 2016

1. Introduction

4.2 million. 21.5 million. 40 million. 70 million. These numbers represented the people in two widely publicized cases where information was compromised by third party attacks to gain either personally identifiable financial information (PIFI[8]) or sensitive personally identifiable information (PII[6]). In each case, the targeted entities' data information systems were breached.

2. The Breachfs

U.S. based Target, an international general merchandise retailer, and the U.S. Office of Personnel Management (OPM) were both victims of data breaches in 2013 and 2015, respectively. Target's data breach affected only their U.S. locations and included PIFI, with information related to credit and debit card transactions.[8] OPM's data breaches included PII, with wide ranges of sensitive PII being compromised as far back as the year 2000.[6]

2.1 Target

In December 2013, consumers were shocked to learn that the credit and debit card payment information of millions of customers

had been compromised through U.S. based Target during the busiest shopping season of the year. Target's secured databases had been successfully hacked and customer information stolen.

2.1.1 The Numbers

Initially, the retail giant estimated that between November 27, 2013 and December 15, 2013, 40 million credit, debit, and Target REDcard card numbers were compromised. Maggie McGrath of Forbes magazine4 reported "…information stolen included customer names, credit or debit card number, the card's expiration date and CVV (card verification value)." The initial estimate was revised after further investigation to reflect as many as 70 million customers, including card numbers, were actually compromised and additional customer information was potentially compromised as well: "…the stolen customer information includes names, mailing addresses, phone numbers and email addresses"[4].

2.2 U.S. Office of Personnel Management (OPM)

Just this year, the U.S. Office of Personnel Management (OPM) made headlines for two separate data breaches. OPM6 reported on their web site that these breaches were "two separate but related cybersecurity incidents" and that these penetrations "have impacted the data of Federal government employees, contractors, and others." The "others" affected include anyone who has had a Federal background check, and, in some instances, their family members.

2.2.1 The Numbers

OPM[6] communicated that the April 2015 discovery of the 4.2 million Federal government employees' personnel data compromised included both current and former employees. The stolen PII includes "information such as full name, birth date, home address and Social Security Numbers." OPM[6] further disclosed that while they were investigating the initial personnel data breach, it was discovered that additional sensitive PII had been compromised, "including background investigation records of current, former, and prospective Federal employees and contractors" dating as far back as the year 2000, with 21.5 million Social Security Numbers (SSNs) also having been stolen. Of these 21.5 million SSNs, "1.8 million non-applicants, primarily spouses or co-habitants of applicants" were also compromised.

3. Lessons Learned

These large-scale attacks provoked the question, "How did this happen?" As these data breaches took all by surprise, there were lessons learned through the investigations.

3.1 Target

Target's investigation revealed two breaches into their systems: one through a trusted vendor and one through their point-of-sale devices in their retail stores. Their online customers were not affected.[8]

3.1.1 How Did This Happen?

Reporter Brian Krebs of Krebsonsecurity.com[2] recounted that in January 2014, Target reported their data breach was through a third party HVAC vendor. Concerns formed around why a third party's external network would have access to a retailer's main network, including their payment system network. The reporter further cited a contact as saying:

> "…it is common for a large retail operations to have a team that routinely monitors energy consumption and temperatures in stores…vendors need to be able to remote into the system in order to do maintenance…or troubleshoot…it is sometimes beneficial to allow a vendor to support versus train or hire extra people" [2].

In addition to the breach through the vendor, the intruders targeted the point-of-sale systems at various Target locations. They uploaded "their card-stealing malicious software" to Target's point-of-sale devices, allowing the thieves to gain access to real-time transaction information. This is how approximately 40 million credit and debit card accounts were compromised.[2]

3.2 OPM

OPM's investigations revealed not only an ongoing attack, but that the department had been aware of lack of proper security for months before the large data breach was disclosed to the public.

3.2.1 How Did This Happen?

Reporter Sean Gallagher of Arstechnica.com reported on the OPM breaches. The initial ongoing attack was "uncovered using

the Department of Homeland Security's (DHS) Einstein – the multi-billion dollar intrusion detection and prevention system that stands guard over much of the federal government's Internet traffic"[1]. Gallagher[1] stated that once baseline criminal attacks and network espionage tactics have been executed, Einstein may view the traffic analysis as normal network traffic. He further reported that while Einstein is working, it is detecting intrusions already in progress, not preventing them from happening.

The faults in the OPM date breaches are multiple and many layered. The Office of the Inspector General provided a report in November 2014 noting the agency's deficiencies in the OPM department's IT security. This report comes after other breaches had been noted, but before third-party vendors got hacked, like KeyPoint, Anthem, and Premera Blue Cross – all with ties to the OPM.[3]

Jacob Olcott, in an interview with Tom Field of Information Security Media Group[5], pointed out "that there are a series of organizations that have been involved with the breach outside of the Office of Personnel Management." He continued, "there is a connection between some of these third-party contractors and the security that they may have had in place, but also the Department of Interior, from a third-party perspective, was providing that data storage for OPM"[5].

4. Proposed Security Measures

In light of the "how's" of the data breaches, both Target and OPM have taken action to ensure higher levels of security to protect their sensitive data.

4.1 Target

Target dedicated a page on their web site to address the questions and concerns of anyone who is believed to have been compromised.[8] In this dedicated section, Target apologized to its customers, reminded them that they, as consumers, had zero liability, advised that they watch their accounts, and even offered one year of free credit monitoring - if accepted by a certain date.

4.1.1 Proposed Resolutions Offered

People wanted answers. The dedicated site page stated that the issue (breach) had been resolved, "Yes. We closed the access point that the criminals used when we discovered the breach on Dec. 15, 2013" and with regards to certain customer information being taken as well, "This theft is not a new breach. This development was uncovered in the course of the ongoing investigation…we moved swiftly to close the access point…and removed the malware they left behind".[8]

However, Target's breach was not completely fixed before a statement was issued to the public. This was reported by John Mulligan, Target's Chief Financial Officer, to a Senate panel, "three days after the company announced last month it had solved the breach by removing the malicious software from its systems, transaction data were being stolen from another 25 checkout machines" and less than 150 customers were affected by this delay.[7]

In addition to having removed the malware, Target announced its intention to move forward six months ahead of schedule with EMV (Europay, MasterCard, and VISA) chip cards for their Target REDcards.[8] The installation of the card readers for their Target REDcards will have put the retailer ahead of the schedule for being prepared to accept MasterCard and VISA credit and debit cards with the EMV chips when the issuance of these more secure cards becomes mandatory in the fall/winter of 2015.

4.2 OPM

Like Target, OPM dedicated a page on their web site to address the questions and concerns of anyone who is believed to have been compromised.[6] The government agency offered no apology to those affected by these breaches; they instead addressed four areas: what happened, how someone may have been affected, what an affected person can do, and what the agency has done to help.

4.2.1 Proposed Resolutions Offered

OPM mentioned that in addition to current and former Federal employees, the breach may have also affected those who have undergone a background investigation as far back as the year 2000 to present and even specified the forms used for the background checks. They further detailed each specific group and how their information was compromised, stating that dependent upon the type of breach an individual's PII may have been involved in, the OPM will "be providing you with a suite of comprehensive services in the coming weeks… at no cost for at least three years" and recommended proactive steps for

individuals to take as well.[6]

Olcott[5] reminded his interviewer that it is difficult to establish and implement a sound security protocol and identify best practices when the problem itself has not truly been identified. "But what we do know is that, certainly this was an issue that starts with the top and the organization's ability to set security expectations," and prompted that third-party access is not forgotten in the cybersecurity reviews, "I think the first thing that we all have to ask ourselves is what were our expectations for security, and did that match what we contracted for. As a government investigator over the years…the first thing that you turn to is the contract…what did we actually contract for and was it being performed adequately."

OPM took ownership and addressed what how moving forward, they are focused on a more secure network:

> "OPM continues to take aggressive action to strengthen its broader cyber defenses and information technology (IT) systems. … Outlined in the Cybersecurity Action Report, OPM has identified 15 new steps to improve security and modernize its systems, including: Completing deployments of two-factor Strong Authentication for all users, expanding continuous monitoring of its systems, and hiring a new cybersecurity advisor".[6]

5. Conclusion

The occurrences of data breaches have continued to rise. Every organization, from the mom-and-pop gas station around the corner to a multi-billion dollar company and even the Federal Government are being targeted. Cyberterrorists are actively attacking data bases in an attempt to gain information that can be turned for a profit. Each organization must be pro-active and think one step-ahead to keep from data breaches from occurring.

References

[1] Gallagher, S. (2015). *Security: Why the "biggest government hack ever" got past the feds*. Retrieved from Arstechnica.com: http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/

[2] Krebs, B. (2014). *Target hackers broke in via HVAC company*. February 05. Retrieved from Krebsonsecurity.com: http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[3] Krebs, B. (2015). *Catching up on the OPM breach*. Retrieved from Krebsonsecurity.com, , June 15: http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/

[4] McGrath, M. (2014). *Investing: Target data breach spilled info on as many as 70 million customers.* , January 10. Retrieved from Forbes.com: http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/

[5] Olcott, J. (2015). Lessons from the OPM breach. (T. Field, Interviewer) July 14. Information Security Media Group. Retrieved from http://www.bankinfosecurity.com/interviews.php?interviewID=2793&user_email=kolade@penair.org&rf=2015-07-22#

[6] OPM. (2015). *Office of personnel management: Information about OPM cybersecurity incidents*. , July 17. Retrieved from OPM.gov: https://www.opm.gov/cybersecurity/

[7] Riddell, K. (2014,). *The washington times: Target data breach went on after fix statement, executive says.* February 4. Retrieved from The Washington Times Web site: http://www.washingtontimes.com/news/2014/feb/4/senate-panel-target-data-breach-occurred-longer-th/

[8] Target. (2014). *About us: Shopping experience: Payment card issue FAQ*. Retrieved from Corporate.Target.com: https://corporate.target.com/about/shopping-experience/payment-card-issue-faq