Global Information Assurance Certification Paper

Compliant but not Secure: Why PCI-Certified Companies Are Being Breached

GIAC GSLC Gold Certification

Author: Christian J. Moldes
E-mail: christian.moldes@hotmail.com
Advisor: Manuel Humberto Santander Pelaez

Accepted: December 7, 2015

Abstract

The Payment Card Industry published the Data Security Standard 11 years ago; however, criminals are still breaching companies and getting access to cardholder data. The number of security breaches in the past two years has increased considerable, even among the companies for which assessors deemed compliant. In this paper, the author conducts a detailed analysis of why this is still occurring and proposes changes companies should adopt to avoid a security breach.

1. Introduction

The Payment Card Industry Security Standards Council (PCI SSC) published the Data Security Standard (DSS) to provide a minimum set of required security controls to protect cardholder data 11 years ago (Search Security, 2013).

Although official statistics does not exist, the number of organizations that have successfully passed PCI DSS assessments have increased over the years. However, also increasing are the number of organizations that hit the news due to a security breach that affected cardholder data. A list of the most significant cardholder data security breaches within the past two years is included in Appendix A.

It is clear that even after so many years, there are still many misconceptions about PCI DSS compliance and its role in providing a reasonable level of security. Furthermore, some of these misconceptions have driven some organizations to allocate most of their resources into preventive controls disregarding detective controls. This resource allocation strategy results on organizations being unable to effectively handling security events and avoiding intrusions.

In this paper, we will not discuss companies that have been unable to achieve PCI DSS compliance. Criminals are breaching these organizations because they failed to implement the minimum set of required security controls. We focus on the organizations that QSAs (Qualified Security Assessors) deemed PCI DSS compliant instead as this calls into question whether the PCI DSS standard is effective to stop security breaches at all.

2. Compliant but not Secure

One of the biggest misconceptions about PCI DSS compliance is that PCI DSS-certified companies are secure, even more, hacker-proof as some vendors in the industry carelessly advertise. The payment card industry has widely discussed the difference between security and compliance in security and PCI compliance forums. If there were any doubts left, the past two years of security breaches demonstrates that no company is secure. Target, breached in 2013, was certified PCI DSS compliant weeks before criminals installed malware on the retailer's network (Bjorhus, 2014). Others such as Heartland Payment Systems suffered a major breach

Christian J. Moldes, Christian_moldes@hotmail.com

even though assessors have been deeming this company compliant for six consecutive years (Brenner, 2009).

Either the PCI DSS is ineffective to protect cardholder data or the way organizations are approaching PCI DSS compliance is flawed. If PCI DSS does not guarantee security, what is the benefit of complying with it? Besides possibly providing some legal safe harbor, complying with the PCI DSS reduces the probability of a security breach. However, compliance does not eliminate this probability.

PCI DSS includes security controls to deal with the most common risk scenarios and attack vectors identified by the PCI SSC. Even though, PCI SSC has updated the PCI DSS over the years, PCI DSS does not cover every possible attack scenario and vectors. While PCI SSC can improve the PCI SSC in future versions as they have been doing with every release, ultimately, cardholder data security, and not just compliance is the responsibility of each organization.

3. Why Are PCI-Certified Organizations Being Breached?

Verizon in its whitepaper "Verizon 2015 PCI Compliance Report" states: "Of all the companies investigated by our forensics team over the last 10 years following a breach, not one was found to have been fully PCI DSS compliant at the time of the breach" (Verizon, 2015). Therefore, we can conclude that based on the statistical information collected by Verizon from real security breaches, organizations are mistakenly deemed PCI DSS compliant. There are multiple probable reasons why this is occurring, and we can group these reasons into two major categories: reasons attributable to the organization and reasons attributable to the QSAs that are certifying these organizations.

3.1. Reasons Attributable to the Organization

3.1.1. Compliance program

Some organizations mistakenly assume that PCI DSS compliance is simply passing their annual assessment and obtaining a certification. These organizations place all their compliance efforts into this point-in-a-time event and fail to maintain compliance

between one assessment and the next one. It is not surprising that these organizations end up being breached primarily because of their lack of a mature compliance program. This type of organizations usually fail to:

- Identify all locations where cardholder data is stored and define their compliance scope accordingly
- Gain visibility and control of their payment channels that could result in unknown new cardholder data flows and repositories
- Monitor security controls and compliance periodically
- Provide adequate security awareness to all the organization's stakeholders to ensure PCI DSS required security controls are understood and applied to all the system components in scope
- Filling out compliance self-assessment questionnaires without validating security controls

For example, Sally Beauty's sysadmins were using VB scripts containing the username and password of a network administrator at the company (Krebs, 2015a). This insecure practice is in clear violation of PCI DSS requirement 8.2.1 which demands all credentials be rendered unreadable during transmission and storage on all system components (PCI SSC, 2015).

3.1.2. Unrealistic expectations

Organizations may have unrealistic expectations for their QSAs. For example, they expect their QSAs to:

- Understand the organization's business processes and applications better than the organization's staff
- Uncover all gaps and vulnerabilities
- Uncover all locations where the organization stores cardholder data

While there are QSAs that may be familiar with some industries and their business processes, it is very difficult for every QSA to be a subject-matter expert in all industries.

Even properly scoped assessments are limited by time and resources, and as such, in most cases QSAs can only review a sample of systems components. Making it impossible for a QSA to uncover all gaps and vulnerabilities. It is also common for an organization that has previously been deemed PCI-compliant to have to remediate newly discovered gaps during an assessment cycle.

An experienced QSA may be familiar with typical locations where organization usually store cardholder data and may be able to find data that has been stored outside the official data repositories. However, unless organizations use automated tools, it will be impossible for a QSA to find all locations where cardholder data may be stored.

For example, after their security breach, Forever 21 blamed their QSA for failing to uncover undisclosed files containing cardholder data (Schuman, 2008). Unless this QSA was hired to conduct a data discovery process, blaming their QSA for this undisclosed data repositories is unfair.

In summary, some organizations are breached because their security assurance rests on unrealistic expectations and because of their lack of due diligence in their compliance efforts.

3.1.3. Human error

As it is widely known in information security, humans are the weakest link in the information security chain. Organizations should expect that people are going to fail. Someone could forget to apply a security patch, misconfigure a security setting, not follow the security policies and procedures, or click on a malicious link. Regardless of all security controls in place, criminals breach some organizations simply because of human errors.

For example, a district manager that kept his credentials taped to a laptop may have contributed to Sally Beauty's security breach (Krebs, 2015a). Raising questions about the

effectiveness of Sally Beauty's security awareness program and its compliance with PCI DSS.

3.1.4. Focus on preventive controls only

Some organizations spend their entire efforts on preventing security breaches from ever happening and forget about the need to allocate resources to identifying and investigating security events thoroughly.

If criminals succeed on compromising cardholder data, it is likely that the organization was unable to detect the intrusion, and preventive security controls, regardless of the number deployed, have been ineffective to either stop the intrusion or generate appropriate alerts.

It is also embarrassing that several breached organizations actually received alerts and notifications from the security controls they implemented as the breach was occurring; however, the organization performed little or no action at all to investigate these alerts and notifications.

For example, Target confirmed that the hack attack against the retailer's point-of-sale (POS) systems triggered alarms, which its information security team evaluated and chose to ignore (Schwartz, 2014). Sally Beauty's Tripwire solution fired warnings when the intruders planted malware on their point of sale systems. Either nobody was monitoring those alerts or the alerts were plainly dismissed (Krebs, 2015a). In a similar case, SecurePay's web application firewall, a PCI DSS optional requirement, triggered alerts as the attack was occurring. The application firewall raised an alert so the network team could block the IP address involved in the alert. (Krebs, 2014a). It is clear that the network team did not conduct a thorough investigation or that they did not take any action resulting in criminals extracting cardholder data anyway.

In summary, criminals are breaching some organizations because organizations are not allocating sufficient resources to investigate security events and alerts, and stop attacks once detective controls identify a potential intrusion.

3.2. Reasons Attributable to the QSAs

There are several reasons attributable to the QSA companies as well. Mistakenly, they may certify non-compliant organizations due to poor methodologies and unqualified consultants. Even in these cases, it is important to understand that the role of a QSA in a PCI DSS assessment is not to conduct a complete discovery of all non-compliant issues. The QSA's role is to provide an opinion on the compliance status of an organization based on the time allocated to interview the organization's staff, review a sampling of system components, and analyze evidence provided by the organization.

3.2.1. QSA methodology

The methodology to conduct PCI DSS assessments used by some QSAs may lead to certifying non-compliant organizations. Jennifer Bjorhus interviewed several industry members who described the work conducted by the largest QSA company as "lax", not accurate, "glaring with errors", and poor quality (Bjorhus, 2014).

The following list illustrates cases where a poor methodology may lead to a flawed assessment:

- QSAs who rely mostly on their interviewees' statements to validate compliance
  - Some QSAs may accept their interviewee's statements at face value. They do not realize that sometimes interviewees are not necessarily the most authoritative person to speak on a subject or that they may just assume that security controls are in place, and that sometimes interviewees may rely on what their staff has told them without validating those assertions themselves.
- QSAs who solely rely on evidence provided by the organization
  - QSAs have to keep in mind that the organization may provide evidence of only selected system components that currently comply with PCI DSS. QSAs may miss the opportunity to uncover compliance deviations and issues if they only rely on screenshots or partial configuration reviews provided at the organization's discretion.
- QSAs who spend little to no time onsite

    - With little time to conduct an onsite review, it is very unlikely that the QSA would conduct a thorough analysis and detect not so evident gaps. News media identified at least one QSA company of performing assessments in a third or quarter of the time compared to other QSA companies (Grundvig, 2013).
- QSAs who don't take a representative sampling of system components
    - QSAs who do not take appropriate sampling sets may fail to identify gaps in the security management processes and patterns that contribute to security operations inconsistency.
- QSAs who are validating positives instead of negatives
    - QSAs who validate positives would focus on finding evidence of compliance. QSAs who validate negatives focus on finding evidence of non-compliance. It is very easy to validate positives, as a small sampling would be sufficient to believe that an organization is PCI DSS compliant. On the contrary, validating negatives requires spending more time to ensure no instances of non-compliance exists. This latter approach would obviously take more time and most QSAs do not usually practice it.

3.2.2. QSA individual expertise

The QSA expertise can also be a factor that allows non-compliant organizations to pass assessments, for example:

- QSAs who fail to identify the right compliance scope for an organization
    - QSAs may incorrectly advise their clients to leave critical components out of the compliance scope. These components, if compromised, could be used by an attacker to gain access to the cardholder data environment.
- QSAs who are not experts on specific areas or technologies
    - QSAs who are not experts on the technologies under review may fail to identify critical vulnerabilities or misconfigurations. An intruder may exploit these vulnerabilities to escalate privileges and gain access to cardholder data.

- QSAs who are not familiar with hacking techniques or attack vectors that hackers use to breach organizations
    - A QSA who is not familiar with hacking techniques or attack vectors may fail to identify how the lack of specific security controls could put the cardholder environment at risk. Robert Carr, Heartland's CEO, blamed his QSA for being unable to identify a common attack vector criminals use against other companies (Brenner, 2009).

4. Improving PCI DSS Compliance and Security

Given that there are multiple reasons why organizations can be compliant but not secure, organizations should strive to improve their PCI DSS compliance program and security.

4.1.1. Develop a mature compliance program

Organizations should develop a mature compliance program by conducting the following tasks:

1) Designate an individual or group to manage and monitor PCI DSS compliance and empower them to have influence across the organization.
2) Conduct a data discovery process regularly to identify and maintain an inventory of data repositories and system components in scope. Define your PCI DSS scope based on this inventory.
3) Automate PCI DSS compliance to have a clear visibility of the compliance status of the organization at all times. Organizations can achieve this task by using GRC tools such as IBM OpenPages, RSA Archer or similar.
4) Provide appropriate security awareness training to ensure all stakeholders understand the need of PCI DSS compliance. This training has to be tailored to the specific needs of each organizational group.
5) Follow PCI SSC's best practices for implementing PCI DSS into business-as-usual processes.

4.1.2. Select the right QSA

Organizations should understand that PCI Compliance is the organization's responsibility, not the QSA's. However, not having the right QSA may affect the PCI DSS understanding, interpretation, and scope definition.

Price should not be the only factor to take into consideration when selecting a QSA. Consider the QSA methodology, assessment process, and internal training practices as well. Keep in mind that small consulting companies may lack the benefit of large QSA companies. There are strength in numbers and large QSA companies may benefit of having multiple consultants with diverse expertise, different opinions, and insight of multiple industries.

Interview your QSA consultant before committing to an assessment. Select your QSA consultants based on their expertise and knowledge of your industry, technologies in use, and information security. Keep in mind that QSA consultants cannot be experts on everything but at least some exposure to the business processes and technologies used by your organization is very important. A QSA consultant with some experience in penetration testing or computer forensics is highly desirable. These individuals would be able to identify vulnerabilities easily based on their insight of past security breaches and hacking techniques, and your organization would obtain the most value out of each assessment cycle.

It is important to rotate QSA consultants at least every couple of years. Your organization may benefit from having different perspectives, expertise, audit skills, and approaches to the PCI DSS assessment.

4.1.3. Strengthen your monitoring and investigation capabilities

In a time and age where APTs (Advanced Persistent Threats) are prevalent, no organization would ever be safe. Attackers can spend as much time as needed to perform reconnaissance, research the organization and technologies in use, and obtain information about the security controls in place if they are targeting a specific organization.

Researchers found that the malware used in the Target's security breach was custom-made for the Target intrusion and carefully crafted to avoid detection by all antivirus tools on the market (Krebs, 2014b). Given this, most organizations would not have been able to stop an intruder.

Organizations have to allocate more resources to strengthen their monitoring and investigation capabilities. Organizations have to document their assets and their locations, dataflows, network paths, attack vectors, and attack scenario. The staff assigned to monitoring activities should have a clear and deep understanding of how data flows, in what format, security controls in place, and possible attack vectors to extract this data.

Organizations with limited resources should at least adopt risk-based monitoring process. For example, system components could be classified according to criticality:

a) Group 1: All system components that store cardholder data
b) Group 2: All system components that process and transmit cardholder data but which do not store it even temporarily.
c) Group 3: All system components that provide security and authentication services
d) Group 4: All system components that provide access to the cardholder data environment
e) Group 5: All system components that are facing external networks such as the Internet, partners' networks, or wireless networks.
f) Group 6: Any other components in scope not included in previous groups.

Ideally, organizations should monitor and investigate all the security events and alerts; however, assuming that resources are limited, organizations could use the following strategy to monitor and investigate activities:

a) 50% of monitoring time assigned to group 1 and 2. The organization should investigate all the security events and alerts in this group.

b) 35% of monitoring time assigned to groups 3, 4 and 5. The organization should investigate all the critical events in this group and remaining events only if there is time left.
c) 15% of monitoring time assigned to group 6. The organization should sample security events and alerts in this group for additional research and investigation, and pick different types of events each day.

Organizations should learn from their own and other organizations' mistakes. Special attention should be paid to attack vectors successfully used during previous penetration tests and for the techniques and attack vectors used by criminals to breach other organizations.

5. Conclusion

There are multiple reasons why PCI DSS-certified organizations are being breached. This can be attributable to the organizations' approach to PCI DSS compliance and the use of unqualified assessors.

Given that is impossible to stop a committed attacker, organizations should improve how they approach PCI DSS compliance and information security. Their goal should be to implement a mature compliance program where the compliance state is the result of the organization's business-as-usual processes. Organizations will receive appropriate advice and value out of each assessment cycle if they select the right QSA.

Finally, in order to minimize the impact of a security breach, organizations must strengthen their monitoring and investigation capabilities by allocating more resources to monitoring and investigation of security alerts.

Christian J. Moldes, Christian_moldes@hotmail.com

6. Appendix A: Security Breaches

The following table contains the most significant security breaches occurred in the past two years. However, this is not a comprehensive list of all the security breaches over that period. Moreover, several entities reported investigating possible credit card breaches for which no additional information is publicly available.

Table 1 - Security Breaches Occurred in the previous two years

Organization	Industry	Date	Attack Vector	References
CVS	Drugstore Chain	July 17, 2015	In-store kiosks compromised by malicious software.	http://krebsonsecurity.com/2015/07/cvs-probes-card-breach-at-online-photo-unit/
Service Systems Associates	Service Provider	July 9, 2015	Payment terminals in the gift shops of several of our clients compromised by malicious software.	http://krebsonsecurity.com/2015/07/credit-card-breach-at-a-zoo-near-you/
Missing Link Networks Inc.	Credit Card Processor	May 27, 2015	Undisclosed attack vector.	http://krebsonsecurity.com/2015/06/breach-at-winery-card-processor-missing-link/
Harbortouch	POS Vendor	May 1, 2015	Payment terminals in restaurants and bars compromised by malicious software. Only some of Harbortouch's customers were affected.	http://krebsonsecurity.com/2015/05/harbortouch-is-latest-pos-vendor-breach/
Mandarin Oriental Hotel Group	Hotel Chain	March 4, 2015	Payment terminals compromised by malicious software. Undisclosed attack vector.	http://krebsonsecurity.com/2015/03/credit-card-breach-at-mandarian-oriental/
Natural Grocers	Grocery Chain	March 2, 2015	Database vulnerabilities were exploited to gain access to the network. Point of Sale Systems compromised by malicious software.	http://krebsonsecurity.com/2015/03/natural-grocers-investigating-card-breach/
Book2Park.com	Parking Services	February 2, 2015	Malware deployed on their E-commerce site. Specific attack vectors were not disclosed.	http://krebsonsecurity.com/2015/02/target-hackers-hit-third-parking-service/
OneStopParki	Parking	December	E-commerce site hacked via an unpatched vulnerability in	http://krebsonsecurity.com/2014/12/target-hackers-hit-

Organization	Industry	Date	Attack Vector	References
ng.com	Services	30, 2014	Jomla. Company put off applying security update because it broke portions of the site.	onestopparking-com/ http://krebsonsecurity.com/2015/01/park-n-fly-onestopparking-confirm-breaches/
Park-n-Fly	Parking Services	December 16, 2014	E-commerce site hacked. Undisclosed attack vector.	http://krebsonsecurity.com/2014/12/banks-park-n-fly-online-card-breach/
Bebe Stores	Retail	December 5, 2014	Retail stores compromised by malicious software.	http://krebsonsecurity.com/2014/12/bebe-stores-confirms-credit-card-breach/
Jimmy John's	Fast Food Chain	October 31, 2014	Payment terminals in retail stores compromised by malicious software. Credentials used to manage point-of-sale systems remotely were compromised to gain access to the payment terminals.	http://krebsonsecurity.com/2014/07/sandwich-chain-jimmy-johns-investigating-breach-claims/ http://krebsonsecurity.com/2014/09/signature-systems-breach-expands/
Staples, Inc.	Retail	October 20, 2014	Payment terminals in retail stores compromised by malicious software.	http://krebsonsecurity.com/2014/10/banks-credit-card-breach-at-staples-stores/ http://krebsonsecurity.com/2014/12/staples-6-month-breach-1-16-million-cards/ http://krebsonsecurity.com/2014/11/link-found-in-staples-michaels-breaches/
Kmart	Retail	October 10, 2014	Payment terminals in retail stores compromised by malicious software.	http://krebsonsecurity.com/2014/10/malware-based-credit-card-breach-at-kmart/
Dairy Queen	Fast Food Chain	October 10, 2014	Payment terminals in stores compromised by malicious software.	http://krebsonsecurity.com/2014/08/dq-breach-hq-says-no-but-would-it-know/ http://krebsonsecurity.com/2014/10/dairy-queen-confirms-breach-at-395-stores/
Jimmy Johns	Fast Food Chain	September 24, 2014	Intruder stole login credentials from the company's point-of-sale vendor and used these credentials to remotely access the point-of-sale systems at	http://krebsonsecurity.com/2014/07/sandwich-chain-jimmy-johns-investigating-breach-claims/

Organization	Industry	Date	Attack Vector	References
			some locations and deploy malicious software on the payment terminals.	http://krebsonsecurity.com/2014/09/jimmy-johns-confirms-breach-at-216-stores/
Home Depot	Retail	September 7, 2014	Self-checkout lanes in retail stores compromised by malicious software. Attackers used stolen credentials from a third-party vendor to enter the perimeter of Home Depot's network. Once in the network, the attackers exploited an unpatched vulnerability in Microsoft Windows.	http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/ http://krebsonsecurity.com/2014/09/in-home-depot-breach-investigation-focuses-on-self-checkout-lanes/
Goodwill Industries International Inc.	Non-profit Organization / Retail Thrift Stores	July 21, 2014	Payment terminals in retail stores compromised by malicious software. Third-party service provider hosting Point of Sale environment was compromised to deploy malicious software.	http://krebsonsecurity.com/2014/07/banks-card-breach-at-goodwill-industries/ http://krebsonsecurity.com/2014/09/breach-at-goodwill-vendor-lasted-18-months/
P.F. Chang's	Restaurant Chain	June 12, 2014	Payment terminals compromised by malicious software. Undisclosed attack vector.	http://krebsonsecurity.com/2014/06/p-f-changs-confirms-credit-card-breach/ http://krebsonsecurity.com/2014/06/p-f-changs-breach-likely-began-in-sept-2013/
Sally Beauty	Retail	March 05, 2014	Intruders gained access to the network through a Citrix remote access portal set up for use by employees who needed access to company systems while on the road. Credentials for remote access were taped to laptop of a district manager. Attackers scanned and mapped the network, used VB scripts to deploy malware and exfiltrated data via DNS traffic.	http://krebsonsecurity.com/2014/03/sally-beauty-hit-by-credit-card-breach/ http://krebsonsecurity.com/2014/03/sally-beauty-confirms-card-data-breach/ http://krebsonsecurity.com/2014/03/zip-codes-show-extent-of-sally-beauty-breach/ http://krebsonsecurity.com/2015/05/deconstructing-the-2014-sally-beauty-breach/
Smucker's	Online Retail	March 04, 2014	Web server compromised to steal form data as customers	http://krebsonsecurity.com/2014/03/thieves-jam-up-

Organization	Industry	Date	Attack Vector	References
			were submitting the data during the online checkout process. Company was running an outdated, vulnerable version of ColdFusion, a Web application platform made by Adobe Systems Inc.	smuckers-card-processor/
SecurePay	Credit card processing company	March 04, 2014	Web server compromised to steal data as during the processing. Company was running an outdated, vulnerable version of ColdFusion, a Web application platform made by Adobe Systems Inc.	http://krebsonsecurity.com/2014/03/thieves-jam-up-smuckers-card-processor/
White Lodging	Hotel Franchisee	January 31, 2014 April 13, 2015	Malicious software installed on cash registers in food and beverage outlets	http://krebsonsecurity.com/2014/01/hotel-franchise-firm-white-lodging-investigates-breach/ http://krebsonsecurity.com/2015/02/banks-card-thieves-hit-white-lodging-again/ http://krebsonsecurity.com/2015/04/white-lodging-confirms-second-breach/
Michaels Stores, Inc. Aaron Brothers	Retail	January 25, 2014	Payment terminals in retail stores compromised by malicious software.	http://krebsonsecurity.com/2014/01/sources-card-breach-at-michaels-stores/ http://krebsonsecurity.com/2011/05/breach-at-michaels-stores-extends-nationwide/
Neiman Marcus	Retail	January 10, 2014	Undisclosed attack vector.	http://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus/
Target Brands Inc.	Retail	December 18, 2013	Payment terminals in retail stores compromised by malicious software. Malware-laced email phishing attack sent to employees at an HVAC firm. The credentials used by this service provider were compromised to gain access to the Target's network	http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/ http://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach/ http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Organization	Industry	Date	Attack Vector	References
			and deploy malicious software.	http://www.darkreading.com/attacks-and-breaches/target-ignored-data-breach-alarms/d/d-id/1127712 http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

7. References

Bjorhus, J. (2014). “Clean Reviews Preceded Target’s Data Breach, and Others”. Retrieved August 15, 2015 from www.govtech.com website: http://www.govtech.com/security/Clean-Reviews-Preceded-Targets-Data-Breach-and-Others.html

Brenner, B. (2009). “Heartland CEO on Data Breach: QSAs Let Us Down”. Retrieved August 15, 2015 from www.csoonline.com website: http://www.csoonline.com/article/2124260/privacy/heartland-ceo-on-data-breach--qsas-let-us-down.html

Grundvig, J. (2013). “Changing Your Password Won't Change Anything - You Will Still be Hacked”. Retrieved August 15, 2015 from www.huffingtonpost.com website: http://www.huffingtonpost.com/james-grundvig/changing-your-password-wo_b_4414149.html

Krebs, B. (2014a). “Thieves Jam Up Smucker’s, Card Processor”. Retrieved August 15, 2015 from krebsonsecurity.com website: http://krebsonsecurity.com/2014/03/thieves-jam-up-smuckers-card-processor/

Krebs, B. (2014b). “A Closer Look at the Target Malware, Part II”. Retrieved August 15, 2015 from krebsonsecurity.com website: http://krebsonsecurity.com/2014/01/a-closer-look-at-the-target-malware-part-ii/

Krebs, B. (2015a). “Deconstructing the 2014 Sally Beauty Breach”. Retrieved August 15, 2015 from krebsonsecurity.com website: http://krebsonsecurity.com/2015/05/deconstructing-the-2014-sally-beauty-breach/

PCI SSC (2015). “PCI DSS v.3.1”. Retrieved August 15, 2015 from www.pcisecuritystandards.org website: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

Schuman, E. (2008). “Breach Update: Forever 21 Stored 5-Year-Old Transaction Data”. Retrieved August 15, 2015 from archives.thecontentfirm.com website: http://archives.thecontentfirm.com/securityfraud/breach-update-forever-21-stored-5-year-old-transaction-data/

Schwartz, M. (2014). “Target Ignored Data Breach Alarms”. Retrieved August 15, 2015 from www.darkreading.com website: http://www.darkreading.com/attacks-and-breaches/target-ignored-data-breach-alarms/d/d-id/1127712

Search Security. (2013). “The history of the PCI DSS standard: A visual timeline”. Retrieved August 15, 2015 from searchsecurity.techtarget.com website: http://searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline

Verizon (2015) “Verizon 2015 PCI Compliance Report”. Retrieved September 3, 2015 from www.verizonenterprise.com website: http://www.verizonenterprise.com/pcireport/2015/

8. Acknowledgments

Special thanks to the following members of the IBM security services practice who graciously offered themselves to proofread this paper and suggested additional content.

- Michael Rodriguez
- Greg Tkaczyk
- Kenneth Mininger
- Cristian Bobadilla Cepeda
- Ron Black