Interested in learning more about security?

SANS Institute InfoSec Reading Room

PCI DSS and Security Breaches: Preparing for a Security Breach that Affects Cardholder Data

Organizations that transmit, process or store cardholder data are contractually obligated to comply with the Payment Card Industry Data Security Standard (PCI DSS). They may be tempted to assume that once they are certified compliant, they are immune to security breaches, and as a result, may be inadequately prepared when such events occur. Regardless of their compliance status, organizations that fail to prepare could face long investigations, expensive forensic services, staff terminations, and loss of business and r...

PCI DSS and Security Breaches: Preparing for a Security Breach that Affects Cardholder Data

GIAC GCCC Gold Certification

Author: Christian J. Moldes
E-mail: Christian_moldes@hotmail.com

Advisor: Sally Vandeven

Accepted: February 28, 2018

Abstract

Organizations that transmit, process or store cardholder data are contractually obligated to comply with the Payment Card Industry Data Security Standard (PCI DSS). They may be tempted to assume that once they are certified compliant, they are immune to security breaches, and as a result, may be inadequately prepared when such events occur.

Regardless of their compliance status, organizations that fail to prepare could face long investigations, expensive forensic services, staff terminations, and loss of business and reputation.

This research/paper provides detailed guidelines on how to prepare for a security breach, the documentation needed to facilitate forensic investigations and containment, and how to minimize the consequences and impact of a security breach.

1. Introduction

Comparative statistics published by the Identity Theft Resource Center shows that the number of security breaches for all industries in the United States has been consistently increasing for the past seven years reaching an all-time record in 2017. Whether this trend is a result of more stringent laws and regulations forcing companies to report their security breaches or a constant increase of malicious and criminal activity, one thing is certain, the risk of suffering a security breach is increasing.

Therefore, organizations should be prepared to deal with a security breach. This need is even greater for organizations subjected to the Payment Card Industry Data Security Standard (PCI DSS) as cardholder data can be easily monetized, and the cost of a security breach can be higher due to the replacement of payment cards, fines, class action lawsuits and mandatory forensic investigations.

Preparation includes having a complete understanding of the consequences of not being adequately prepared, the incident handling process, the payment card brands' notification requirements, and the potential long-term impacts to the organization.

2. Lack of Preparation can be Devastating

Unless an organization has already experienced a data security breach, it may be difficult to grasp the devastating consequences and long-term impact a breach can have. Unfortunately, security professionals cannot learn from others' mistakes to better prepare for this type of situations because organizations that suffered a security breach rarely share details of their breach publicly, at least not voluntarily.

If details about past security breaches were shared, there would be plenty of practical information that one can learn from these incidents. For example, the chain of events that led to the security breach, how the organization uncovered the security breach, a chronology of response events, mistakes that if avoided would have minimized the cost of the security breach, the impact to the organization (brand, culture, staff, etc). Because this information is not being shared, security professionals often rely on leaks, unconfirmed information, gossip, and speculation to obtain useful intelligence to apply to their organizations.

There have been a few cases where the data breach is so undue, the number of records and individuals affected is so massive, or the negligence is so gross that official information is publicly shared. Equifax is one of these cases. In addition to being a publicly-traded entity, Equifax not only had to inform their stockholders of any events that may impact their stock value and expected revenue, but their security breach was so massive and its response to the data breach so plagued with errors that the organization was forced to release more information than usual. Equifax's response to the security breach was labeled "haphazard, ill-conceived and clumsy" (Krebs, 2017), "a public relations catastrophe" (Wiener-Bronner, 2017), and "incomplete, confusing and contradictory" (Borak, 2018).

Christian J. Moldes, Christian_moldes@hotmail.com

A review of Equifax's breach response will help organizations understand potential pitfalls and how to prepare for a similar incident. The following table outlines a chronology of events and an analysis of the timeline of the Equifax security breach.

Christian J. Moldes, Christian_moldes@hotmail.com

Date	Event	Timeline Analysis
March 10, 2017	U.S. CERT discloses a vulnerability in Apache Struts (NIST, 2017).	**Vulnerability**
March 19, 2017	Apache.org releases a security update and provides a workaround (Apache.org, 2017).	**Security Update:** ▪ Vulnerability + 9 days
May 13, 2017	First date the attacker accessed sensitive information (Equifax, 2017)	**Breach:** ▪ Vulnerability + 64 days ▪ Security Update + 55 days
July 29, 2017	Equifax's Security team observed suspicious network traffic associated with its U.S. online dispute portal web application. In response, the Security team investigated and blocked the suspicious connection (Equifax, 2017).	**Identification:** ▪ Security Update + 132 days ▪ Breach + 77 days
July 30, 2017	The Security team continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, the company took the affected web application offline that day (Equifax, 2017).	**Initial containment:** ▪ Breach + 78 days
August 2, 2017	Equifax contacted an independent cybersecurity firm, Mandiant, to assist in conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted (Equifax, 2017).	**Investigation:** ▪ Breach + 81 days ▪ Identification + 4 days
August 11, 2017	Investigators determined that, in addition to dispute documents, the attackers accessed database tables containing large amounts of consumer information (Godin, 2017).	-
August 15, 2017	Equifax learned that consumer information had likely been stolen, not just exposed (Godin, 2017).	-
September 7, 2017	Equifax announces cybersecurity incident involving consumer information (Equifax, 2017b).	**US Notification:** ▪ Identification + 40 days ▪ Investigation + 36 days
September 8, 2017	Equifax's public outreach and response after the breach is criticized. Website to assist customers is broken and provides confusing information (Krebs, 2017).	-
September 8, 2017	News outlets report that three Equifax executives sold shares of the credit-reporting company worth nearly $2 million shortly after a massive data breach was discovered. The sales occurred before the company announced the breach to the public on Thursday.	-

Date	Event	Timeline Analysis
September 14, 2017	Krebsonsecurity.com reports that the Equifax breach resulted in more than 200,000 credit cards stolen (Krebs, 2017b).	-
September 15, 2017	Equifax releases details on cybersecurity incident and announces the retirement of Chief Information Officer and Chief Security Officer (Equifax, 2017b).	**Executives retirement:** ▪ Identification + 48 days ▪ Notification + 8 days
September 15, 2017	Multiple news outlets question Equifax CISO's qualifications and fitness for the position having a major in music composition and no apparent technology or information security training (Arends, 2017).	-
September 19, 2017	Some news outlets point to the fact that many CISOs and security professionals may not have formal security training and that Equifax's problem was not necessarily their CISO (Fung, 2017) and (Blue, 2017).	-
September 20, 2017	Equifax sends breach victims to fake notification site (Godin, 2017b).	-
September 26, 2017	Equifax announces the retirement of Chief Executive Officer (Equifax, 2017c).	**CEO retirement:** ▪ Identification + 53 days ▪ Notification + 19 days
September 27, 2017	After public pressure, Equifax added an opt-out provision so customers can get out of the arbitration required by TrustedID, the credit monitoring service offered to affected customers. Without this provision, individuals wouldn't be allowed to sue, join class-action suit, or benefit from any class-action settlement (Isidore, 2017).	-
October 2, 2017	Equifax announces their cybersecurity firm has concluded the forensic investigation of the incident. The completed review determined that a total of 145.5 million U.S. consumers, 8,000 Canadian consumers were potentially impacted (Equifax, 2017d).	**Investigation completion:** ▪ Investigation + 61 days
October 3, 2017	Former Equifax CEO testifies before Congress (Fiegerman, 2017).	
October 10, 2017	Equifax announces 15.2 million UK records exposed in the cybersecurity breach (McCrank, 2017).	**UK Notification:** ▪ Identification + 73 days ▪ Investigation + 69 days ▪ Investigation completion + 8 days
October 17, 2017	Equifax credit assistance site served spyware (Krebs, 2017c).	-
Date	**Event**	**Timeline Analysis**

November 10, 2017	Equifax warns about impact of the data breach on its business. Massive breach will hurt sales and result in costs of $60 million to $75 million during the period and will cut revenue by 3% to 4% in the quarter. As of this date, Equifax shares have dropped around 25% since the company's disclosure of the breach (Reuters, 2017).	-
February 10, 2018	News outlets report that the Equifax hack could be worse than initially thought because additional information, including tax IDs and driver's license details, may have been accessed (Borak, 2018).	-

This timeline provides the following revealing information:

- PCI DSS Req. 6.2 requires all system components and software to be protected from known vulnerabilities by installing applicable vendor-supplied security patches within one month of release. It took Equifax more than four months (132 days) to identify this vulnerability and apply a critical security update to their systems.
- PCI DSS Req. 10.6.1 and 10.6.3 require organizations to review logs for all security events at least daily and follow up on exceptions and anomalies identified during the review process. It took Equifax 77 days to find out that they had suffered a security breach; time in which the intruder was probing systems and roaming freely on the network without any of these activities being detected. As astonishing as it can be, this is not unusual. Organizations continuously fail to protect their systems adequately, ensure an ongoing vulnerability management program, and implement a mature and effective process to review logs and investigate malicious activity (Moldes, 2015).
- It took Mandiant 36 days to confirm the scope of the breach for the United States and Canada, and 69 days to do the same for the United Kingdom. It is not easy to confirm the breach scope if there is poor documentation, inadequate network segmentation or lack of security event logging.
- Lack of response preparation led to victims being directed to a fake notification website and the actual website providing incorrect and misleading information resulting in public outcry on how this massive security breach was handled.
- As pressure mounted, in the middle of dealing with this incident, Equifax had to retire their Chief Information Officer and Chief Security Officer.
- Many people questioned the qualifications of their CSO as well as the criteria that the Board and CEO adopted to hire her.
- After dealing with the breach for 53 days, Equifax's CEO was retired.
- While not working for Equifax anymore, the former CEO had to testify before the Congress' House Energy and Commerce Committee.
- This data breach was a public relations nightmare for Equifax, and the long-term impact and consequences are yet to be seen.

Equifax failed to prevent this security breach because of a lack of a mature vulnerability management program. They failed to detect the security breach by not having an effective monitoring program. Moreover, they failed to minimize the impact of the breach by making several mistakes while dealing with this incident. Several questions arise as a result:

- Why did it take Equifax 36 days from the beginning of the forensic investigation to confirm that a security breach had occurred?
- Why did it take Equifax 61 days to identify and confirm the scope of the data affected by the security breach?
- Was the lack of documentation, audit trails and security logs making the forensic investigation more difficult and time-consuming?
- Was lack of defined boundaries (network segmentation and access controls) expanding the scope of the breach unnecessarily?
- What can organizations do to be better prepared to handle a security breach?

Many of the issues that Equifax had to face are the result of poor preparation. This preparation starts off with understanding the different phases of incident handling and the aspects they include which are explained in the following sections.

3. Incident Handling Phases

NIST (National Institute of Standards and Technology) special publication 800-61 Rev. 2 defines four major incident handling phases:

- Preparation
- Detection & Analysis
- Containment, Eradication, and Recovery
- Post-incident Activity

The PCI DSS does not provide any specific guidelines regarding incident handling other than what is stated in requirement 12.10, which states that an incident response plan must be implemented defining roles, procedures, reporting requirements, response, testing, training, and processes to evolve the plan. These requirements are not described in detail and, as such, organizations may be compliant with the PCI DSS requirements yet still end up ill-prepared when an incident occurs.

In the following sections, best practices for each of the incident handling phases are explained using guidance from the payment card brands and best practices from the industry.

All the references to PCI DSS requirements are excerpted from PCI DSS v.3.2 available on the PCI Security Standards Council website: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

4. Preparation Phase

The goal of the preparation phase is to get a team ready to handle incidents. This team can be comprised of internal resources as well as external parties. Preparation also includes

training people, documenting policies and procedures, and gathering all the required resources to handle a data security incident (NIST, 2012, pp. 21-23). This section will not address all these needs but only the ones specific to cardholder data and applicable to a PCI DSS security breach.

4.1. Documentation

Having accurate documentation is a critical factor to facilitate and speed up the work conducted by incident handlers and forensic investigators. Some of the documentation needed to deal with a security breach is listed in several sections and requirements throughout the PCI DSS; however, the reason why the PCI DSS requires this documentation and its relationship to incident handling may not be obvious. Many will only realize the value of having accurate and complete documentation when they are struggling to gather this information while dealing with a security breach at the same time.

Organizations can identify what documentation forensic investigators will need by reviewing the information required by the preliminary and final incident response report templates published by PCI SSC. Unfortunately, many organizations do not interact with these report templates until they are impacted by a security breach. These templates are available in the "Documentation library" section of the PCI SSC website.

Becoming familiar with these report templates, the type of information that PFIs (PCI Forensic Investigators) have to collect and analyzing how the organization could be better prepared to facilitate this information will greatly reduce the time required to respond, handle and report an incident. For example:

- "Window of system vulnerability": Do you have the audit trails and security logs that will help establish this window of time?
- "Total number of cards exposed": Do you have the audit trails and security logs that will help calculate the number of cards exposed?
- "Were the log files in any way amended or tampered with prior to your investigation starting?": Do you have audit trails and security logs that will help establish the integrity of the log files?

These preparation steps will definitely reduce the cost of handling a security breach as incident handlers and investigators will spend less time gathering and confirming the accuracy of documentation.

Most of the time, handlers and investigators will not be familiar with the organization's business processes, network and information architecture, security controls, and dataflows. If handlers and investigators have to spend time making sense of incomplete or inaccurate documentation, validating the accuracy of these documents, or gathering this information for the first time, major delays will be introduced in the incident handling and forensic investigation process. At a minimum, in order to effectively handle cardholder data security, the following

4.1.1. Information assets inventory

The importance of having an asset inventory cannot be overstated. Knowing exactly where the assets are would be critical to both implementing a protection plan and validating whether this plan has been insufficient to protect the assets at risk. Unfortunately, there are no current official statistics of the impact of not having an accurate asset inventory. For example, the last time that Verizon Data Breach Investigation Report (DBIR) included statistics of how unknown data and assets were a factor in a security breach was in 2009. In that report, they noted that 38% of the breaches in 2009 included a system storing data that the organization did not know existed on that system, 24% involved systems that had unknown connections, and 17% had unknown accounts or privileges (Verizon Business Risk Team, 2009).

Forensic investigators often point to the lack of accurate inventories as one of the issues that they deal with during incident handling and forensic investigations.

PCI DSS requires the following inventories:

- System components that are in scope for PCI DSS (Req. 2.3)
- All databases, tables, and files storing post-authorization cardholder data (Required in the Report on Compliance template, section 4.3)
- Any hardware security modules and other secure cryptographic devices used for key management (Req. 3.5.1)
- Logs of all media (Req. 9.7.1)
- Authorized wireless access points including a documented business justification (Req. 11.1.1)

Accurately identifying and defining the potential breach scope helps focus the investigation on only the affected components.

4.1.2. Dataflow and network diagrams

Dataflow and network diagrams provide the incident response team and forensic investigators with a quick understanding of the environment, scope, security zones, network segments, CDE (Cardholder data environment), and dataflows. If detailed enough, they may also provide ports/protocols allowed and the network security controls in place. This information would help understand what channels may have been exploited to get access to the CDE and where to find potential indicators of compromise.

A documented business justification for all services, protocols, and ports allowed into and out of the CDE would help differentiate and identify authorized inbound and outbound connections from unauthorized connections.

PCI DSS outlines the need for these diagrams in the following requirements:

- Diagrams that identify all connections between the cardholder data environment and other networks, including any wireless networks (Req. 1.1.2 and ROC reporting template, section 4.1)
- Diagrams that show all cardholder data flows across systems and networks (Req. 1.1.3)
- High-level network diagram of the organization's networking topography, showing the overall architecture of the environment. This high-level diagram should summarize all locations and key systems, and the boundaries between them (Required in the ROC Reporting Template, Section 2.2)

4.1.3. Cryptographic keys procedures

As mentioned in previous sections, incident handlers and forensic investigators need to have a complete understanding of how cardholder data is being protected in order to identify any potential ways in which these protection mechanisms may have been bypassed.

This understanding will be provided by having documentation describing the architecture of cryptographic solutions and procedures outlining how cryptographic keys are set up, rotated, and protected from access and tampering. This documentation should also include the locations of where these keys reside while in use and at rest, as well as the individuals who have been granted access to these keys.

If cardholder data is encrypted, the attacker will need access to the cryptographic keys to decrypt the data. The investigation will also include reviewing whether these keys were compromised.

The following PCI DSS requirements outline this documentation:

- Key-management policies and procedures that include at least the following: Access to keys is restricted to the fewest number of custodians necessary, key-encrypting keys are at least as strong as the data-encrypting keys they protect, key-encrypting keys are stored separately from data-encrypting keys, and keys are stored securely in the fewest possible locations and forms. (Req. 3.5)
- For service providers, documented description of the cryptographic architecture that includes: details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date; description of the key usage for each key; and inventory of any HSMs and other SCDs used for key management. (Req. 3.5.1)
- For service providers, documentation that the service provider provides to their customers outlining guidance on how to securely transmit, store, and update customers' keys, in accordance with Requirements 3.6.1 through 3.6. (Req. 3.6.a)

4.1.4. Configuration standards

Incident handlers and forensic investigators must identify all the system components that have been compromised. This task becomes difficult if an organization does not use automated configuration management, change management solutions, or file integrity checking solutions. Incident handlers and investigators use information from these solutions to identify any deviations from the approved configuration, unauthorized modifications, and tampering of systems. In the absence of these solutions, documented baseline configurations and change control records may help identify these components.

The following PCI DSS requirements outline these documentation requirements:

- Firewall configuration standards that include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone (Req. 1.1.4)
- Firewall and router configuration standards that include a description of groups, roles, and responsibilities for management of network components (Req. 1.1.5.a)
- Firewall and router configuration standards include a documented list of all services, protocols, and ports, including business justification and approval for each (Req. 1.1.6)
- Firewall and router configuration standards that identify inbound and outbound traffic necessary for the cardholder data environment (Req. 1.2.1.a)
- Documented policies and configuration standards that define the use of personal firewall software or equivalent functionality is required for all portable computing devices that connect to the Internet when outside the network, and which are also used to access the CDE (Req. 1.4.a)
- Configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted system hardening standards (Req. 2.2)
- Documented standards requiring the use of security protocols and strong cryptography for all locations, acceptance of only trusted keys or certificates, and protocols that only support secure versions and configurations (Req. 4.4)
- Configuration standards and processes requiring that a time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2 (Req. 10.4)

4.1.5. Change control documentation

As mentioned in the previous section, change control records could provide information that facilitates the security breach handling and investigation.

The following PCI DSS requirements outline these documentation requirements:

- A formal process for approving and testing all network connections and changes to the firewall and router configurations (Req. 1.1.1)

- Follow change control processes and procedures for all changes to system components (Req. 6.4)

4.1.6. Incident response plan and procedures

PCI DSS requires organizations to implement incident response plans and procedures. The following PCI DSS requirements outline these documentation requirements:

- Incident response procedures in the event unauthorized wireless access points are detected (Req. 11.1.2)
- An incident response plan in the event of a system breach that includes the following: (Req. 12.10):
    - Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands
    - Specific incident response procedures
    - Business recovery and continuity procedures
    - Data backup processes
    - Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database)
    - Coverage and responses for all critical system components
    - Reference or inclusion of incident response procedures from the payment brands

4.1.7. Third-party Contracts

PCI SSC recommends ensuring all contracts with third-party service providers, hosting providers, integrators, and resellers, and other relevant parties address incident-response management. Contracts should include specific provisions on how evidence from these environments will be accessed and reviewed, for example, allowing forensic investigators access to the environments affected by the security breach and under the control of the third-parties. (PCI SSC, 2015).

If these provisions are not included in the current contracts, they must be negotiated before a security breach occurs. The following aspects should be taken into consideration:

- When will each party initiate the pre-designated breach notification procedures to each other?
- Who will pay for incident handling and forensic investigations required?
- What level of access will be provided to the environment under control of the third-party?

- Whether the third-party will be able to choose the forensic investigation and incident handling firm
- What information and documentation under the control of the third-party will be shared with the organization?
- Whether the full content of the forensic reports will be shared with the organization
- What compensation the organization will receive in the event the security breach is a direct result of the third-party actions or areas of responsibility
- Confidentiality agreements to ensure that details about the security breach and forensic investigations are not leaked, either intentionally or unintentionally.

4.2. Key relationships

PCI DSS does not require an organization to establish relationships with key third-party entities before a security breach occurs. Organizations should establish these relationships in advance to avoid being subjected to the pressure and stress of having to identify and establish these relationships after a security breach has occurred.

The following relationships should be established:

- PFI (PCI Forensic Investigator)
- Independent forensic investigator
- Federal law enforcement (FBI and Secret Service)
- External public relations agency (PR)
- Crisis management and communications agency
- Legal counseling
- Media contacts
- Identity protection services
- Information technology and security services

The need for these relationships is elaborated in detail in the following sections.

4.3. Incident Response Training

PCI DSS includes requirements for incident response training (Req. 12.10); however, it does not provide details regarding what this training should entail.

While organizations can train their internal information security staff to conduct preliminary containment activities, it would make more sense to retain external expertise immediately. Training is not a substitute for experience as external handlers and investigators are exposed to tens of incidents each year and learn from a larger team of fellow handlers and investigators.

Organizations that rely on internal staff to provide incident response capabilities may find that these resources are unavailable to take care of all the tasks required to deal with a security breach. Internal incident handlers would most likely spend most of their time on the following tasks leaving little time for hands-on response activities:

- Connecting external incident handlers and forensic investigators with internal teams and third-party service providers
- Coordinating incident handlers and forensic investigators' access to locations and systems affected by the security breach
- Gathering information as required by the incident handlers and forensic investigators
- Discussing crisis management and external communications
- Coordinating public relations response and external communications activities
- Coordinating notifications to law enforcement, payment processors, payment card brands, and others
- Reporting progress to the executive team
- Coordinating legal defense with internal and external legal counsel
- Coordinating containment activities
- Activating business continuity plans

Because of these multiple responsibilities, training would be better invested in first developing abilities to coordinate and manage incident response activities rather than developing technical incident handling skills. The following entities provide this type of training:

- CERT - Carnegie Mellon
  - Creating a Computer Security Incident Response Team
  - Managing Computer Security Incident Response Teams
- SANS Institute
  - MGT535: Incident Response Team Management
- FIRST
  - FIRST CSIRT Basic Course

4.4. Business continuity plans

In requirement 12.10, PCI DSS maintains that incident response plans should include business recovery and continuity procedures; however, it does not provide any specific instructions or recommendations for how this must be carried out. At minimum, business recovery and continuity plans should address the following aspects:

- Alternative methods to process card payments in the event the current payment technologies are compromised or unable to operate during the incident, e.g., Point of Sale Systems (POS), Pin Pads, Kiosks, applications, websites, etc.
- Alternative vendors or providers for services affected by compromised business partners
- Succession planning for C-level executives, directors, and managers

5. Detection and analysis phase

NIST states that incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every type of incident. Organizations should be prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors first (NIST, 2012).

One of the most important factors to identify a security breach is a mature process in place to track and monitor all access to network resources and cardholder data. Detecting an incident would require trained security staff, solutions to parse and aggregate security events and notifications from multiple different systems, and a process to monitor alerts and investigate suspicious activity.

5.1.1. Security events logs and audit trails

Incident handlers and forensic investigators use security events logs and audit trails to identify the attack vectors, compromised system components, cardholder data affected, and the scope of the security breach. Organizations should ensure that security events and audit trails have been implemented to cover potential attack vectors, hacking techniques, and hypothetical breach scenarios in case these are utilized by an attacker.

The following PCI DSS requirements outline these documentation requirements:

- Anti-virus software log generation is enabled, and logs are retained in accordance with PCI DSS Requirement 10.7. (Req. 5.2.d)
- An automated technical solution that detects web-based attacks is generating audit logs. (Req. 6.6)
- Audit trails to link all access to system components back to individual users (Req. 10.1)
- Audit trails to reconstruct the following events (Req. 10.2):
    - All individual user accesses to cardholder data
    - All actions that have been taken by any individual with root or administrative privileges
    - Access to all audit trails
    - Invalid logical access attempts

- Use of, and changes to identification and authentication mechanisms
- Initialization, stopping or pausing of audit logging
- Creation and deletion of system-level objects

- Changes to time settings on critical systems are logged (Req. 10.4.2.b)

5.1.2. Daily monitoring

PCI DSS req. 10.6 requires organizations to review logs and security events for all system components to identify anomalies or suspicious activity. The following logs and events should be reviewed, at minimum, daily:

- All security events
- Logs for all system components that store, process, or transmit CHD (Cardholder Data) and/or SAD (Sensitive Authentication Data)
- Logs of all critical system components
- Logs of all servers and system components that perform security functions

It may take months for an organization to find that a security breach has occurred, as it did with Equifax. Failing to detect a security breach within a reasonable timeframe, i.e., within days or a week at most, may weaken the organization's legal defense. If logs are reviewed daily as required, why it is taking organizations so long to detect a breach? The following are possible causes:

- Events and logs are not being reviewed as required
- Staff assigned to review events and logs is not appropriately trained to identify IOCs (Indicators of compromise)
- Staff assigned to review events and logs is not following up on suspicious activity
- Some system components may not have been properly configured to forward events and logs to a SIEM (Security Information and Event Management)
- The SIEM has not been configured properly to parse and aggregate security events and raise alerts

Under these circumstances, it would be very difficult for PFIs and QSAs to state that the organization was PCI-DSS compliant at the time of the security breach.

6. Containment, eradication and recovery phases

Once a security breach has been identified, the goal of the containment phase is to stop the bleeding by preventing the attacker from getting any deeper into the impacted systems or spreading to other systems. Containment can usually be accomplished by isolating infected systems, blocking suspicious network activity, and disabling services among other actions.

6.1. Retaining a PCI Forensic Investigator (PFI)

PCI SSC requires organizations that suffered a security breach to retain the services of a specialized forensic investigator, a PFI (PCI Forensic Investigator). These are investigators that have PCI SSC's training and certification and they are required to be independent of the entity they are investigating. An organization should ensure that it has no other relationships with the PFI it chooses. For example, if an organization's Qualified Security Assessor (QSA) also happens to be a PFI, that person cannot perform the investigation. (PCI Security Standards Council LLC, 2015)

A list of approved PFIs can be found on the PCI SSC website: https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators

6.2. Retaining other external services

6.2.1. External legal counsel

According to InfoLawGroup, a law firm specialized on information governance, privacy and data security, upon the discovery of a payment card, security breach, or even the suspicion of a payment card security breach, the company's internal legal counsel should be contacted immediately. The communications conducted with the involvement of an attorney can be asserted privilege and documents and conversations may not be admitted in a court of law (InfoLawGroup LLP, 2009)

The organization may need to retain external legal counsel not only to be able to assist with all the legal matters to assert privilege but also to establish a communication protocol concerning the incident, help implement the data preservation plan, and assist with lawsuits.

6.2.2. Independent forensic investigator

In addition to retaining a PFI, InfoLawGroup advises organizations to retain an independent forensic firm to act as the expert for the organization's legal team. Moreover, an independent forensic investigator may act as a counter-balance to the potential conflicts of interest of the PFIs, even more so in cases where compliance is a matter of interpretation and judgment (InfoLawGroup LLP, 2009).

InfoLawGroup also discusses the risks of using a PCI forensic investigator as its investigation is not protected by attorney-client or work product privilege, making its reports completely discoverable in a court of law.

6.2.3. Public relations firm and communications

A security breach is not a time to improvise; an incident response plan that includes how to engage with the public should be in place beforehand. In these circumstances, the organization should be able to show accountability and demonstrate that it still deserves trust (Melnitzer, 2014). This trust is rebuilt by demonstrating that the organization cares about the affected customers, can contain and limit the impact to customers, is able to learn from this security mishap, and that the organization would be able to protect any future data that customers share.

Actions taken by the organization to contain the security breach and minimize the damage caused to third parties should be communicated to all affected parties early and clearly. Organizations will benefit by retaining a PR firm specialized in handling security breaches to assist with developing a communication strategy, establishing pre-approved communication channels, and identifying any third-party services that will be needed.

The following aspects should be planned:

- Communication strategy. For example, who will be authorized to provide information regarding the security breach and actions taken by the organization?
- Communication channels. For example, an official website should be provided to communicate news of the security breach, investigation progress, and assistance that is to be provided to the affected parties. This site should be tested in advance to verify that it would be able to handle the workload of the entire customer base.
- Additional third-party services. For example, the organization should retain call center services to handle the workload increase caused by customer inquiries. The call center representatives should be provided with specific scripts according to the communication strategy.

The Federal Trade Commission provides helpful tips regarding how to notify affected parties and the use of model letters. For additional information refer to https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

6.2.4. Credit monitoring services

Although credit monitoring services have become the standard response to security breaches (Ben-Sachour, 2014), some argue that they may not be worth the cost (Kulp, 2017). An organization should analyze whether this service will be offered to affected parties and engage with credit monitoring vendors as part of a successful and effective preparation plan.

This service may not offer a practical benefit to the affected parties, but the organization should consider it as part of its public relations strategy. In some cases, not offering it may be construed as the organization not caring about the damage caused to the affected parties.

6.2.5. Information technology and security services

Depending on the scope of the security breach, containment and remediation activities usually overwhelm the organization's available resources. Organizations may need to retain information and security services firms to assist with containment and remediation efforts.

6.3. Reporting an incident

6.3.1. Payment card brands' notification procedures

The notification procedures vary among the payment card brands. Not being aware of this information, it may lead to complying with some of the payment card brand's notification procedures but not with all of them. The following table illustrates these main differences:

					
Notification	**Immediately** send an email to EIRP@aexp.com **no later than 24 hours after the incident** is discovered. Complete the Merchant Data Incident - Initial Notice Form and attach it to your email. For data incidents involving **10,000 or more unique American Express Card account numbers** (or otherwise at American Express's request), a PCI Forensic Investigator (PFI) must conduct this investigation.	**Within 48 hours** of an incident.	No public information is available.	Must notify MasterCard **immediately** when the Customer becomes aware of an ADC (Account Data Compromise) Event or Potential ADC Event in or affecting any system or environment of the Customer or its Agent. Must report an ADC Event **within twenty-four (24) hours of becoming aware of the Event or Potential Event**, and on an ongoing basis thereafter to MasterCard all known and or suspected facts concerning the ADC Event or potential ADC Event.	**Within three (3) business days of a suspected or confirmed account data compromise**, provide the Visa Initial Investigation Report to the acquiring bank or directly to Visa.
Forensic Investigation	Conduct a thorough investigation that **may require** you to hire a PCI Forensic Investigator	No public information is available.	No public information is available.	**Within seventy-two (72) hours**, engage the services of a PFI to conduct an independent forensic investigation to assess the cause, scope, magnitude, duration, and effects of the ADC Event or Potential ADC Event. The PFI engaged to conduct the investigation must not have provided the last PCI compliance report concerning the system or environment to be examined. Prior to the commencement of such PFI's investigation, the Customer must notify MasterCard of the proposed	Visa **may require a compromised entity to engage a PFI** to perform an independent forensic investigation. **Visa will not accept forensic reports from non-approved PFI forensic organizations.** PFIs are required to provide forensic reports and investigative findings directly to Visa.

					
				scope and nature of the investigation and obtain preliminary approval of such proposal by MasterCard or, if such preliminary approval is not obtained, of a modified proposal acceptable to MasterCard.	
Forensic Investigation Timeframe	The unedited report must be provided to American Express, **within 10 business days after completion**.	No public information is available.	No public information is available.	**Within five (5) business days from the commencement of the forensic investigation**, ensure that the PFI submits to MasterCard a preliminary forensic report detailing all investigative findings to date. **Within twenty (20) business days from the commencement of the forensic investigation**, provide to MasterCard a final forensic report detailing all findings, conclusions, and recommendations of the PFI, continue to address any outstanding exposure, and implement all recommendations until the ADC Event or Potential ADC Event is resolved to the satisfaction of MasterCard.	Provide Visa with the **initial forensic (i.e. preliminary) report within ten (10) business days from when the PFI is engaged (or the contract is signed)** Provide Visa with **a final forensic report within ten (10) business days of completion of the review.**
Contact Information	Report a data incident at **1-888-732-3750** or **EIRP@aexp.com** / International: **+1 (602) 537- 3021**	Call Discover® Global Network Security at **1-800-347-3083** to report a data security breach. If you have questions, email **AskDataSecurity@discover.com**	No public information is available.	Must report an ADC Event or Potential ADC Event through the Manage My Fraud and Risk Programs application. If a Customer does not have access to or requires an immediate response	Contact Visa at **(650) 432-2978** or **usfraudcontrol@visa.com**

					
				regarding an ADC Event, all inquiries may be sent to **account_data_compromise@ mastercard.com**	
Compromised Account Reporting	No public information is available.	No public information is available.	No public information is available.	Via My Fraud and Risk Programs application. **Within twenty-four (24) hours and continuing throughout the investigation and thereafter**, provide to MasterCard, in the required format, all PANs associated with Account data that were actually or potentially accessed or disclosed in connection with the ADC Event or Potential ADC Event and any additional information requested by MasterCard.	Visa CAMS (Compromised Account Management System)
Indemnification	American Express will not seek indemnification from your organization for an incident (a) involving less than 10,000 unique Compromised Card Numbers or (b) if: ▪ You notified American Express of the Data Incident pursuant to AMEX policy, ▪ You were in compliance at the time of the Data Incident with the PCI DSS (as determined by the PFI's investigation of the Data Incident) and ▪ The data incident was not caused by your wrongful	No public information is available.	No public information is available.	MasterCard may charge Operational Reimbursement (OR) and Fraud Recovery (FR) fees based on the number of compromised or potentially compromised accounts. In the event that the compromised entity is an e-commerce merchant where only PAN, expiration date, and/or the CVC code have been compromised, only OR will be invoked. Based on the totality of known circumstances surrounding an ADC Event or Potential ADC Event,	To qualify an account data compromise event under the GCAR (Global Compromised Account Recovery) program, Visa must determine all of the following criteria have been met: 1. A PCI DSS or PCI PIN Security or PIN Security Program Guide violation has occurred that could have allowed a compromise of Primary Account Number (PAN) and Card Verification Value (CVV) magnetic-stripe data and/or PIN data. 2. Primary Account Number (PAN) and Card Verification

					
	conduct or that of your covered parties You are liable for all other data incidents as follows. For a data incident involving American Express Card account numbers alone, you shall compensate American Express promptly by paying a data incident **non-compliance fee not to exceed US$100,000 per data incident**. For a data incident involving American Express Card account numbers with sensitive authentication data, you shall compensate American Express promptly: ▪ At the rate of $**5 per account number**. ▪ A data incident **non-compliance fee not to exceed US$100,000 per data incident**. For additional details refer to the Data Security Operating Policy.			including the knowledge and intent of the responsible Customer, MasterCard (in addition to any assessments provided for elsewhere in the Standards) may assess a responsible Customer **up to US$ 100,000 for each violation of a requirement of the PCI SSC**. If the Customer fails to comply with the procedures set forth in section 10.2 of the Security Rules and Procedures Manual, MasterCard may impose an **assessment of up to USD 25,000 per day for each day that the Customer is noncompliant** and/or disqualify the Customer from participating as a recipient of ADC OR reimbursement and FR disbursements, whether such disbursements are made in connection with the subject ADC Event or any other ADC Event, from the date that MasterCard provides the Customer with written notice of such disqualification until MasterCard determines that the Customer has resolved all compliance issues under this section 10.2. For additional details refer to the Account Data Compromise User Guide and the Security Rules and Procedures.	Value (CVV) magnetic-stripe data, and/or PIN data, is exposed at the compromised entity during the intrusion access window. 3. 15,000 or more eligible accounts were sent in one or more CAMS (Compromised Account Management System) IC (Internet Compromise) or RA (Research & Analysis) alerts and/or Visa Account Bulletin (VAB) alerts indicating Primary Account Number (PAN) and Card Verification Value (CVV) magnetic-stripe data is potentially at risk. 4. A combined total of US$ 150,000 or more recovery for all issuers involved in the event. 5. Elevated magnetic-stripe counterfeit fraud was observed in the population of eligible accounts sent in the CAMS alert(s) associated with the Account Data Compromise Event. Under the GCAR program, Visa uses a basic set of rules to calculate an acquirer's liability for issuer incremental counterfeit fraud losses and a pre-determined amount to cover operating expenses associated with accounts at risk in the compromise

					
					event. These calculations are based on eligible CAMS-alerted accounts and issuer-reported counterfeit fraud that occurred during the alert Fraud Window for one or more event alerts. Visa also may impose a liability cap for compromises that meet specified criteria to be deemed catastrophic, based on a balancing of the overall interests of the system. For merchant compromises where other criteria are met, the cap on the acquirer's liability is calculated based on the annual Visa sales volume of transactions submitted by acquirers for entities owned or controlled by the legal owner of the compromised entity. This will include Visa sales at all entities owned by the legal owner of the compromised entity. For additional details refer to the Visa Rules (Visa Core Rules and Product Service Rules).

Table 1 - Payment Card Brands Security Breach Requirements

Note. Information for this table was obtained from the payment card brands' websites listed below

For additional information refer to the following websites:

AMEX

- https://merchant-channel.americanexpress.com/merchant/en_US/data-security
- https://icm.aexp-static.com/Internet/NGMS/US_en/Images/DSOP_Merchant_US.pdf

Discover:

- https://www.discovernetwork.com/en-us/business-resources/fraud-security/pci-rules-regulations/discover-information-security-compliance

JCB

- http://www.global.jcb/en/products/security/data-security-program/

MasterCard

- https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/site-data-protection-PCI.html
- https://www.mastercard.us/content/dam/mccom/en-us/documents/SPME-Manual-Sept-2017.pdf
- https://www.mastercard.us/content/dam/mccom/en-us/documents/account-data-compromise-manual.pdf
- https://globalrisk.mastercard.com/online_resource/member-alert-to-control-high-risk-merchants-match-compliance-program/

Visa

- https://usa.visa.com/support/small-business/security-compliance.html
- https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf
- http://paymentworld.com/docs/training/visa/what-every-merchant-should-know-gcar-vol-091213-final.pdf
- https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf

6.3.2. Failing to report an incident

Failing to report an incident will be considered a violation of the payment card brand rules which contains specific sanctions for non-compliance. For example, Visa Rules contains enforcement mechanisms that Visa may use for violations including non-compliance assessments, being assigned to higher-risk categories, and even disqualification from the program (Visa, 2017).

6.4. Eradication and recovery phases

The goal of the eradication phase is to get rid of the attacker's artifacts on the machine. The goal of the recovery phase is to put the impacted systems back into production in a safe manner.

PCI DSS and the payment card brands rules do not provide any specific guidelines regarding how eradication and recovery must be conducted. However, this is a critical part of incident handling. Once the breach has been contained, eradication and recovery should be carefully executed. An affected company should be diligent in eradicating all pieces of malware deployed by the attacker which may include reinstalling systems from scratch to ensure no malware traces are left behind. Failing to do so may allow the attacker to regain remote access by using backdoors installed during the initial intrusion. The organization will have to report this new intrusion which may adversely affect your company's reputation.

7. Post-incident Activity

7.1. Additional PCI DSS assessments

After the forensic investigation, the payment card brands may require the organization to undergo a new PCI DSS assessment led by a QSA to identify any areas that require remediation. MasterCard may require the PFI to conduct a PCI gap analysis and include the results of that analysis in the forensic report. (MasterCard, 2017). If your previous PCI DSS assessment was conducted by a QSA, the payment card brands would require your organization to engage a different QSA company (Visa, 2016).

7.2. Changes in current compliance and reporting levels

The payment card brands will assign compliance and reporting Level 1 to the organizations that suffered a data security breach. This change ensures that going forward these entities are required to undergo an onsite PCI DSS assessment conducted by a QSA (MasterCard, 2018)

7.3. Staff termination

As mentioned in Section 2, Equifax's security breach ended up in the termination of several members of the organization including their CEO, CIO, CSO, and others. Terminating staff immediately after a security breach is not unusual. For example, Target's security breach also resulted in the resignation of both their CEO and CIO (Dezenhall, 2015). Nowadays, security breaches are impacting the executive leadership more than before; therefore, organizations have to be prepared to deal with critical members leaving the organization.

In order to minimize the impact of this risk, organizations should ensure the following items are implemented:

- Cross-training
- Documented architecture

- Documented operating procedures

7.4. Litigation

One of the most significant risks associated with a payment card breach is legal liability (InfoLawGroup, 2009). This legal liability includes the following:

- Consumer class action lawsuits
- Issuing bank class action lawsuits
- Merchant bank lawsuits
- Payment card recovery processes
- Payment card fines and penalties
- Federal regulatory actions
- State attorney general regulatory actions
- Shareholder lawsuits based on misrepresentation/omissions concerning data security.

According to InfoLawGroup, one of the key factors in determining whether a merchant will ultimately be liable or fined/penalized for a payment card security breach is their PCI compliance status at the time of the breach. The organization should base its legal defense on establishing this fact and that "reasonable security" has been achieved.

Unfortunately, according to the Verizon PCI Report, to this date, none of the companies that suffered a cardholder data breach were found compliant with the PCI DSS at the time of the breach (Verizon, 2017). Because of these statistics, the chances that an organization was compliant at the time of a security breach that impacts cardholder data are close to zero, and the potential for a strong legal defense, minimal.

A successful legal defense may require establishing a strategy that will include complying with the PCI DSS standard to the "letter of the law" and having processes and documentation that support this. Each time compensating controls are used to address specific PCI DSS requirements, the organization risks having used interpretative judgment that may not be shared by most security professionals, may not have followed security best practices, and that may not be considered "reasonable security" by the industry. In other words, organizations may find that their legal defense has been undermined due to the decision of using compensating controls.

7.4.1. How is liability determined?

Each payment card brand has its own criteria to establish liability. Refer to the information listed in the table in section 6.1 and to each payment card brand rule for more details.

7.5. Lessons learned phase

The goal of the lessons learned phase is to document what happened, learn from mistakes conducted during the incident, and improve the organization's capabilities to handle security incidents more efficiently and effectively.

PCI DSS requires organizations to develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments (Req. 12.10.6).

NIST SP 800-61 suggests scheduling a meeting within several days at the end of the incident to answer the following questions:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- Were the documented procedures followed?
- Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

During the security breach handling, organizations should keep these questions in mind. As mentioned in section 7.3, staff may quit or be terminated as a result of the security breach. Some of this knowledge may be lost because the staff directly involved is no longer working for the organization.

8. The cost of a PCI DSS security breach

The average cost per record in 2017 was $154 for retail, $223 for services, and $245 for the financial industry (Ponemon Institute, 2017). According to Ponemon Institute, the following factors influence the cost of dealing with a security breach:

- The unexpected and unplanned loss of customers following a data breach (churn rate)

- The size of the breach or the number of records lost or stolen.
- The time it takes to identify and contain a data breach. The faster the data breach can be identified and contained, the lower the costs.
- Detection and escalation costs including forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors.
- Post data breach costs. These costs include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions.

In order to minimize the cost of a security breach, organization should invest in the following controls:

- Minimizing data retention to strictly what is needed for business
- Compartmentalization and/or isolation to avoid a breach expanding to other network segments, systems or databases
- Implementing an effective monitoring process
- Training internal incident handling staff on the specific abilities and skills that would be needed
- Testing the incident response plan and procedures including all the activities of each phase

9. Conclusion

A security breach can be devastating to an organization as it will consequently be forced to deal with forensic investigations, operational disruptions, audits, bad publicity, lawsuits, staff resignations, and expensive remediation. The consequences may have a long-term impact on the organization. Being aware of these challenges and preparing by having the documentation, processes, resources, relationships, and staff readily available will help organizations react more effectively, minimizing the cost of dealing with a breach, and reducing the overall impact the incident otherwise may have in the organization

References

Apache.org (2017). "Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser". Retrieved December 16, 2017 from cwiki.apache.org website: https://cwiki.apache.org/confluence/display/WW/S2-045

Arends, B. (2017). "Opinion: Equifax hired a music major as chief security officer and she has just retired". Retrieved December 16, 2017 from arstechnica.com website: https://www.marketwatch.com/story/equifax-ceo-hired-a-music-major-as-the-companys-chief-security-officer-2017-09-15

Ben-Achour, S (2014). "Credit monitoring becomes a standard offer after breaches". Retrieved January 22, 2018 from www.marketplace.org website: https://www.marketplace.org/2014/09/09/your-money/credit-monitoring-becomes-standard-offer-after-breaches

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

Blue, V. (2017). "Why Equifax's error wasn't hiring someone with a music degree". Retrieved December 16, 2017 from www.engadget.com website: https://www.engadget.com/2017/09/22/dont-blame-equifax-hack-on-a-music-degree/

Borak, D. (2018). "The Equifax hack could be worse than we thought". Retrieved February 10, 2018 from money.cnn.com website: http://money.cnn.com/2018/02/09/pf/equifax-hack-senate-disclosure/index.html

Dezenhall, E (2015). "A Look Back at the Target Breach". Retrieved December 16, 2017 from www.huffingtonpost.com website: https://www.huffingtonpost.com/eric-dezenhall/a-look-back-at-the-target_b_7000816.html

Equifax (2017). "Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes". Retrieved December 16, 2017 from investor.equifax.com website: https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832

Equifax (2017b). "Equifax Announces Cybersecurity Incident Involving Consumer Information". Retrieved December 16, 2017 from investor.equifax.com website: https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628

Equifax (2017c). "Equifax Chairman, CEO, Richard Smith Retires; Board of Directors Appoints Current Board Member Mark Feidler Chairman; Paulino do Rego Barros, Jr. Appointed Interim CEO; Company to Initiate CEO Search". Retrieved December 16, 2017 from investor.equifax.com website: https://investor.equifax.com/news-and-events/news/2017/09-26-2017-140531280

Equifax (2017d). "Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation of Cybersecurity Incident". Retrieved December 16, 2017 from investor.equifax.com website: https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821

Farivar, C. (2017). "Equifax CIO, CSO "retire" in wake of huge security breach Equifax CIO, CSO 'retire' in wake of huge security breach". Retrieved December 16, 2017 from arstechnica.com website: https://arstechnica.com/tech-policy/2017/09/equifax-cio-cso-retire-in-wake-of-huge-security-breach/

Fiegerman, S. (2017). "Former Equifax CEO testifies before Congress". Retrieved December 16, 2017 from money.cnn.com website: http://money.cnn.com/2017/10/03/news/companies/equifax-ceo-congress/index.html

Fung, B. (2017). "Equifax's security chief had some big problems. Being a music major wasn't one of them". Retrieved December 16, 2017 from www.washingtonpost.com website: https://www.washingtonpost.com/news/the-switch/wp/2017/09/19/equifaxs-top-security-exec-made-some-big-mistakes-studying-music-wasnt-one-of-them/

Godin, D. (2017). “A series of delays and major errors led to massive Equifax breach”. Retrieved December 16, 2017 from arstechnica.com website: https://arstechnica.com/information-technology/2017/10/a-series-of-delays-and-major-errors-led-to-massive-equifax-breach/

Godin, D. (2017b). “Equifax sends breach victims to fake notification site”. Retrieved December 16, 2017 from arstechnica.com website: https://arstechnica.com/information-technology/2017/09/equifax-directs-breach-victims-to-fake-notification-site/

Identity Theft Resource Center. (2017). “ITRC Breach Statistics 2005 - 2016”. Retrieved January 16, 2018 from www.idtheftcenter.org website: https://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf

Identity Theft Resource Center. (2017b). “Data Breach Report”. Retrieved January 16, 2018 from www.idtheftcenter.org website: https://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport_2017.pdf

InfoLawGroup LLP. (2009). “PCI DSS Incident Response: The Legal Perspective”. Retrieved January 16, 2018 from www.infolawgroup.com website: https://www.infolawgroup.com/2009/07/articles/breach-notice/pci-dss-incident-response-the-legal-perspective/

Isidore, C. (2017). “If you want help from Equifax, there are strings attached”. Retrieved January 22, 2018 from money.cnn.com website: http://money.cnn.com/2017/09/08/technology/equifax-monitoring-services/index.html

Krebs, B. (2017). “Equifax Breach Response Turns Dumpster Fire”. Retrieved December 16, 2017 from krebsonsecurity.com website: https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/

Krebs, B. (2017b). “Equifax Hackers Stole 200k Credit Card Accounts in One Fell Swoop”. Retrieved December 16, 2017 from krebsonsecurity.com website: https://krebsonsecurity.com/2017/09/equifax-hackers-stole-200k-credit-card-accounts-in-one-fell-swoop/

Krebs, B (2017c). “Equifax Credit Assistance Site Served Spyware”. Retrieved December 16, 2017 from krebsonsecurity.com website: https://krebsonsecurity.com/2017/10/equifax-credit-assistance-site-served-spyware/

Kulp, K (2017). “Credit monitoring services may not be worth the cost”. Retrieved January 22, 2018 from www.cnbc.com website: https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html

La Monica, Paul (2017). “Equifax execs sold stock before hack was disclosed”. Retrieved January 22, 2018 from money.cnn.com website: http://money.cnn.com/2017/09/08/investing/equifax-stock-insider-sales-hack-data-breach/

MasterCard. (2017). “Security Rules and Procedures – Merchant Edition – 14 September 2017”. Retrieved January 16, 2018 from www.mastercard.us website: website: https://www.mastercard.us/content/dam/mccom/en-us/documents/SPME-Manual-Sept-2017.pdf

MasterCard. (2018). “What merchants need to know about securing transactions”. Retrieved January 16, 2018 from www.mastercard.us website: website: https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html

McCrank, J. (2017d). “Equifax says 15.2 million UK records exposed in cyber breach”. Retrieved December 16, 2017 from www.reuters.com website: https://www.reuters.com/article/us-equifax-cyber/equifax-says-15-2-million-uk-records-exposed-in-cyber-breach-idUSKBN1CF2JU

Melnitzer, J (2014). “Chantal Bernier: Data breach response is 'not the time to improvise'”. Retrieved January 16, 2018 from http://business.financialpost.com website: http://business.financialpost.com/legal-post/chantel-bernier-data-breach-reponse-is-not-the-time-to-improvise

Moldes, C. (2015). “Compliant but not secure: Why PCI-Certified Companies Are Being Breached”. Retrieved December 16, 2017 from www.sans.org website: https://www.sans.org/reading-

room/whitepapers/compliance/compliant-secure-pci-certified-companies-breached-36497

NIST (2012). "Computer Security Incident Handling Guide". Retrieved December 16, 2017 from nvlpubs.nist.gov website: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST (2017). "CVE-2017-5638 Detail". Retrieved December 16, 2017 from nvd.nist.gov website: https://nvd.nist.gov/vuln/detail/CVE-2017-5638

PCI Security Standards Council LLC (2015). "Responding to a Data Breach: A How-to Guide for Incident Management". Retrieved December 16, 2017 from www.pcisecuritystandards.org website: https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf

Ponemon Institute (2017). "2017 Cost of Data Breach Study – Global Overview". Retrieved December 16, 2017 from www.ibm.com website: https://www.ibm.com/security/data-breach

Reuters (2017). "Equifax Warns About Impact of Data Breach on its Business". Retrieved December 16, 2017 from fortune.com website: http://fortune.com/2017/11/10/equifax-warns-data-breach-business/

SANS Institute. (2016). Security 504.1 Incident Handling Step-by-Step and Computer Crime Investigation. SANS Institute.

Verizon (2017). "2017 Payment Security Report". Retrieved January 16, 2018 from www.verizonenterprise.com website: http://www.verizonenterprise.com/verizon-insights-lab/payment-security/2017/

Visa (2016). "What To Do If Compromised". Retrieved January 16, 2018 from usa.visa.com website: https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

Visa (2017). "Visa Product and Service Rules". Retrieved January 16, 2018 from usa.visa.com website: https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf

Wiener-Bronner, D. (2017). "Equifax turned its hack into a public relations catastrophe". Retrieved January 16, 2018 from money.cnn.com website: http://money.cnn.com/2017/09/12/news/companies/equifax-pr-response/index.html

Acknowledgments

Special thanks to the following individuals who graciously offered themselves to proofread this paper and suggested additional content:

- Ciske van Osteen, Manager Global Intelligence, Verizon Enterprise Solutions
- Tiff Joseph Cook, Investigate Response Consultant, Verizon RISK Team
- Sally Vandeven who acted as SANS advisor for this paper.

Special thanks to the following individuals who read this paper and provided feedback:

- Wahid Iqbal, Managing security consultant, IBM
- Douglas A. Brown, Global Operations Manager, X-Force IRIS, IBM

Last Updated: June 19th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
SANS Cyber Defence Canberra 2018	OnlineAU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced