Utrecht University

MBI Master Thesis

Preventing Data Breaches by Proactive Data mining

Author:	J.J. Peersman, BSc
E-mail:	J.J.Peersman@Students.UU.nl
Student #:	3117413
Enrolled in:	2009
Period:	March 2011 – December 2012
Supervision:	Dr. M. Spruit
	Dr. R.S. Batenburg
	A. Klunder
	M. Knuiman
Date:	December 28, 2012

Abstract

Data breaches, or compromises of sensitive data, at organizations became more common in the last couple of years. Various types of sensitive data can be defined, but this thesis focused on credit card data breaches. Credit card breaches are an actual topic and even though standards have been defined to protect the data, breaches still occur. Large organizations that store, process or transfer credit card data must be compliant with the Payment Card Industry Data Security Standard (PCI-DSS). This standard aims to assist and guide organizations in setting up and maintaining a secure basis for their IT environment. Events showed that just being PCI-DSS compliant is not enough to have a secure IT environment. Additional actions must be taken to try to prevent data breaches of credit card data. This research provides these actions and assists organizations by providing a method that they can use by answering the following question:

How can proactive data mining of security events help prevent data breaches of credit card data in a PCI DSS compliant environment?

The environment of a credit card transaction consists of three entities; Cardholder, Merchant and the Banks. The cardholder is the person who owns the credit card. The merchant is the organization that uses the credit card of the cardholder to receive money from the customer. The banks are the issuer (bank of the cardholder) and acquirer (bank of the merchant). A complex flow of data occurs during the payment transaction and an organization must always be aware of where this sensitive data is located. The merchant is a weak link in the complete chain, because he transfers the data from the customer to the banks and back. This research is therefore focused on the merchant.

The weakest link in the transaction process is the easiest target to be breached. A data breach consists of four phases (i.e. infiltration, observation, collection and exfiltration). During the infiltration, an attacker is trying to gain entrance to an organization network. In the second phase, the attacker maps the network and systems that are inside the organizational network and locates the data he/she is looking for; the credit card data. The collection phase is used for the capture of the systems that hold the credit card data and preparing it for transport outside of the organizational network. The last phase is the actual transport of data.

By investigating the process of a credit card transaction from customer to the bank, investigating current protection standards (PCI Data Security Standard) and by researching previous breaches, studies and having interviews with subject matter experts, a list of fifteen indicators is developed that are all warnings for a possible data breach:

Excessive logins	Improper account usage
Modification of Data	Improper protocol usage
Automatic launch of suspicious applications on boot	Uploading of unusual files
SQL Injection Attempts	Unusual running services
New unexpected user accounts	Registry Keys modification

Existence of suspicious files in system directory	Unknown/unexpected network connections
Unusual Log Files	Malware notification
Unusual high/low network activity	

These indicators are used in a method that can aid organizations (i.e. merchants) at developing a strategy that will help them discovering a data breach of credit card data in an early phase. This method is created based on interviews with subject matter experts and makes use of the indicators defined previously. The method consists of five main steps:

1) Identify Data

The first step is used to identify the sensitive data and data that will be used for the classification of indicators inside the organization. A location and mapping to different types of data is made to understand where all the data is located.

2) Map Indicators

The second step maps the fifteen indicators to data so it is clear which indicators can be used for the analysis. Thresholds and baselines must be defined to state what the "normal" operating state for each indicator is. Once indicators reach a certain value, it must be investigated more thoroughly to find out what caused this raise.

3) Vulnerability Management

Vulnerability management is a parallel step that must be performed on a regular basis to get an up to date status report of the IT environment

4) Data Mining

The fourth step is the actual mining for data. The indicators are linked to various types of security events (e.g. logs, reports, incidents). The gathering of valuable data from this enormous amount of information can be very complex and an appropriate data mining tool must be used to only capture the most important data. To focus only on the data that can be used to detect a breach in an early stage, data from the indicators should be used. Anomaly detection is a suitable tool to extract this data, but a well-defined baseline must be present in order to discover these anomalies (step 2).

5) Follow-ups

Actions plan must be made and used that cover each scenario that can occur, based on indicator values. A follow-up consists of multiple actions combined in an action plan and a solution review to check if the action plan worked for this specific situation.

The method is validated during interviews with subject matter experts in order to gain the best knowledge on what steps should be included. The method requires some additional validation by performing a real life case on this subject. A conclusion is made that the method can be used for all kinds of sensitive data (e.g. social security numbers & insurance numbers) than only for credit card numbers. The indicators might vary, but the reason behind it stays the same. The tactics of using indicators to narrow down the data remains the same.

Preface

This master thesis has been performed as part of the curriculum of the Business Informatics Master at Utrecht University. The research aims at organizations that transfer, process or store credit card data and provides a method that assists these organizations in preventing credit card breaches.

I received much support during the execution of this research from many people. I want to start by thanking my supervisors: Marco Spruit (Utrecht University), Ronald Batenburg (Utrecht University) Arjan Klunder (Deloitte) and Martijn Knuiman (Deloitte). They supported me throughout the duration of the research by providing me contacts for interviews, reviewing the work that has been done and other resources that could assist me.

I would also like to thank all the subject matter experts for their time and effort they put in the interviews. Furthermore I would like to thank my friends and family, fellow students and colleagues for all their support!

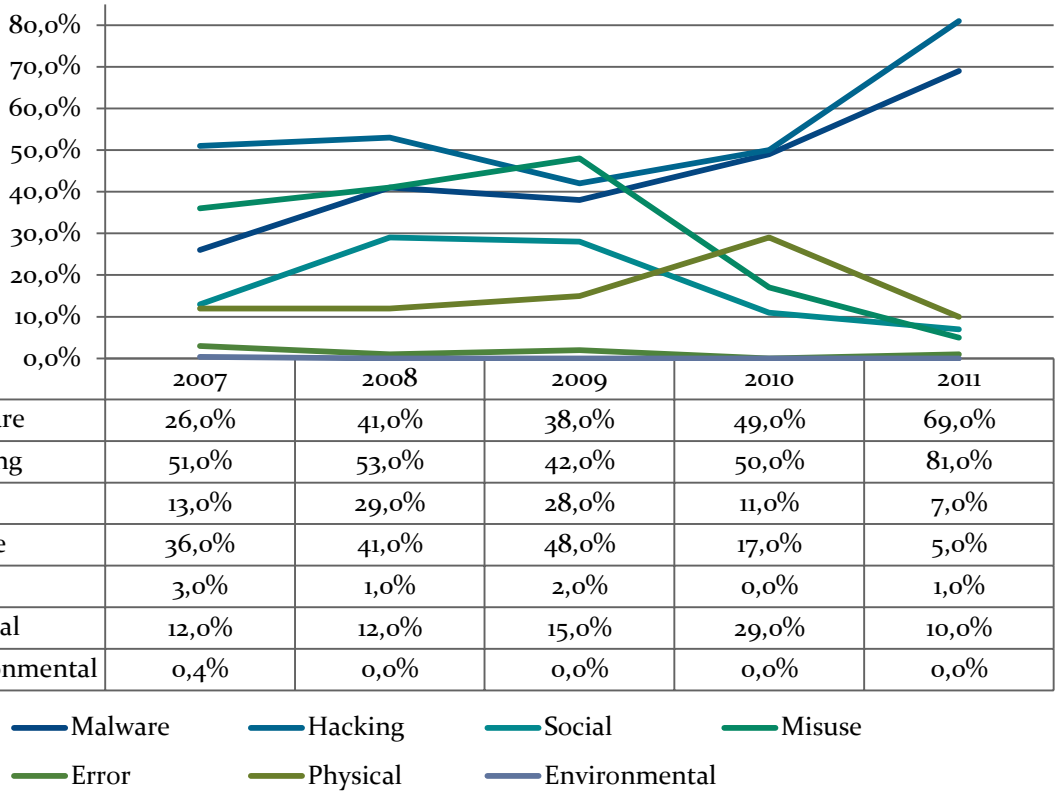
Table of Contents

List of Figures

List of Tables

1. Introduction

Purchasing goods or services with a credit card is an easy process for every customer. The transaction is fast, the customer does not need to pay immediately and still it receives the goods or services he/she asked for. One must be extra careful if sensitive data is involved in a task in order to protect this data. In credit card transactions, the protection of the cardholder's data is very important, because when this data gets into the hands of malicious people, payments can be made as if it was performed by the cardholder. The security of this, from the outside, easy process becomes rather complex when it is closely investigated. A number of parties are involved in the process; the customer, the organization, different banks and the cardholder network organizations (e.g. VISA & MasterCard). Especially the organizations that allow their customers to pay with credit cards are an interesting subject when it comes to security. They do not only transfer cardholder data from the customer to the banks, sometimes they process or even store this data internally. Data has always a high risk for being copied or deleted if it is not protected with an adequate technique such as encryption or a password, especially if it is stored on a physical medium.



	2007	2008	2009	2010	2011
Malware	26,0%	41,0%	38,0%	49,0%	69,0%
Hacking	51,0%	53,0%	42,0%	50,0%	81,0%
Social	13,0%	29,0%	28,0%	11,0%	7,0%
Misuse	36,0%	41,0%	48,0%	17,0%	5,0%
Error	3,0%	1,0%	2,0%	0,0%	1,0%
Physical	12,0%	12,0%	15,0%	29,0%	10,0%
Environmental	0,4%	0,0%	0,0%	0,0%	0,0%

Figure 1.1 Percentage of attacks used in breaches according to Verizon (2012)

Malicious people want to break into an organization and try to gain access to the internal network, systems and sensitive stored data in order to compromise this data. it is stored on a physical medium.

Figure 1.1 shows how the use of different techniques to break into an organization have evolved from 2007 till 2011 based on the data breach investigation reports by Verizon (Verizon, 2012). Every year in April, Verizon releases this report. It indicates that hacking is the number one used technique to access internal networks, closely followed by malware which share is still growing. Hacking includes techniques such as using backdoors, brute force attacks and SQL-injection, while malware is malicious software that creates points of entrance to the attackers. The result of this attack and the compromise of sensitive data is called a data breach.

The recent breach of the Sony PlayStation Network is a good example to illustrate the impact a breach can have for a large organization (McMillan, 2011). Attackers managed to gain personal data of over 77 million users of the gaming network, which include approximately 12700 credit card numbers and 11700 debit card records (AFP, 2011). Other sensitive data such as names, addresses, email addresses, birthdays, PlayStation Network logins/passwords and other profile data were compromised as well. Because of the high amount of accounts that have been breached, the impact it has on Sony is massive. The reputation of and trust in Sony as a secure organization has been damaged and a financial loss must be added to the breach as well. According to a financial press statement by Sony (2011), the breach cost approximately 14 billion yen ($183 million).

To minimize the possibility of breaches and have a secure environment, standards must be used as imposed by the large credit card network organizations. The Payment Card Industry Data Security Standard (PCI DSS) for example, which has 12 requirements for organizations that process, store or transmits credit card data. These 12 requirements should make sure an organization has a secure payment environment. Despite this effort of PCI DSS, there are cases of organizations that were compliant and still have had a data breach, e.g. Heartland Payment Systems (Cheney, 2010). This shows PCI DSS compliance alone is not enough to prevent breaches. Additional tools or methods exist that can tell whether a breach occurred or not, but these methods all work by detecting breaches after they occurred. It would be much better if methods could prevent breaches, or notice them in a very early stage. This can decrease the impact of the attack, because immediate actions can be taken to stop the attack and therefor minimizing the data loss.

A technique that can assist organizations in their effort to prevent breaches is data or process mining (Van der Aalst & De Medeiros, 2005). All applications and servers that are used within an organization must have log files according to PCI DSS that state every action the application or server performed. Furthermore, security events take place or warnings are given out by systems that are already in use. By investigating these log files real-time with a data mining tool, anomalies might be detected and acted upon immediately. Typical attacks usually do not take place in a couple of hours or even days, but it takes months from investigating the network to the actual compromise of data. Attackers spent almost six months and many hours after compromising the corporate network of Heartland Payment Systems, in order to hide their activities (Cheney, 2010). This timeframe also provides an opportunity to gather enough signals that indicate a breach is already going on or can happen in the near future. The main topic of this research is to investigate whether credit card breaches can be prevented.

2. Background

This chapter provides background information for this research such as the problem statement, research scope and questions and both social- and scientific relevance.

2.1. Problem Statement

Data breaches in general occur more and more these days (DatalossDB, 2012a) and the specific breaches that cover credit card data become a larger problem as well as Table 4.1 shows in chapter 4.1. Techniques, such as Intrusion Detection and Prevention Systems, monitor an organizational network for intruders. The importance of standards, e.g. PCI DSS, PCI PTS and PA DSS, is necessary to provide an overall baseline of security(PCI Security Standards Council, 2010a). Various breaches that include credit card data occur despite the effort put into the overall security of credit card transactions by the Security Standards Council with these standards (Cheney, 2010). Additional tools or techniques, which support PCI DSS needs to be in place to ensure a secure payment environment. An important technique that can assist the prevention of these credit card breaches is data mining as Vaidya & Clifton describe in their paper (2004). They mention the possibility of privacy preserving data mining (2004). This research continues the investigation how data mining can assist the prevention of credit card breaches by following problem statement:

How can organizations prevent credit card data breaches by using data mining?

By preventing is meant an early detection of a breach or attempt to a breach. The sooner a breach is detected, the better organizations can defend themselves against it. This thesis will create a method for organizations that, with the assistance of data mining, enables organizations to prevent or stop credit card breaches in an early stage.

The corresponding objective is:

Provide a method that assists organizations in preventing data breaches by implementing a proactive data mining solution on security events.

2.2. Research Question

This problem statement leads to the main research question:

How can proactive data mining of security events help prevent data breaches of credit card data in a PCI DSS compliant environment?

To answer this question, it is divided into five sub questions. These questions need to be answered before the main question can be answered. The chapters corresponding with the questions are written behind each question. The questions can also be found in diagram of the research method.

1: What does the environment in which a credit card transaction takes place looks like and what are the critical points? (Chapter 3)
2: What is a data breach and how is it constructed? (Chapter 4)
3: What are indicators of a data breach? (Chapter 4.3)
4: What are available security events/logs? (Chapter 5.1)
5: What data mining techniques are suitable for the indicators? (Chapter 5.2)

2.3. Scope

This research focuses on large merchants that transfer, store or process credit card data. These merchants should be PCI DSS compliant in order to accept credit cards as a payment technique, because PCI DSS ensures a basic security level. Smaller merchants that only have a few credit card transactions annually are not of interest for this research, because they are not the subject for large breaches. However, the impact of a breach on these small merchants can be much larger, because they might lack the proper financial power to cope with the breach (Stech, 2012).

This research focuses on organizations that are already compliant with PCI DSS. This standard leads to a foundation for a secure environment, because of the twelve requirements. Data mining of events can be used to further secure this environment. Detailed information about PCI DSS can be found in chapter 3.2.

The method that will be created in this research tries to prevent breaches and cannot be used to discover fraud in transactions. Furthermore, skimming of terminals is left out of this research so that the focus lies on the credit card data that is already inside a merchant's, payment provider's or even credit card corporation's environment.

The initial target for this research is credit card data, so any other sensitive data (e.g. social security numbers and electronic patient records) is not taken into account when creating the method.

2.4. Research Method & Strategy

The field of Information Systems (IS) research can be categorized in two types of research; behavioral science and design science. Behavioral science explains or predicts human behavior, while design science creates new artifacts (Hevner, March, Park, & Ram, 2004).This research creates a method (artifact) and is based on the Design Science Research method by Hevner et al.. The structure of IS research is shown in Figure 2.1.

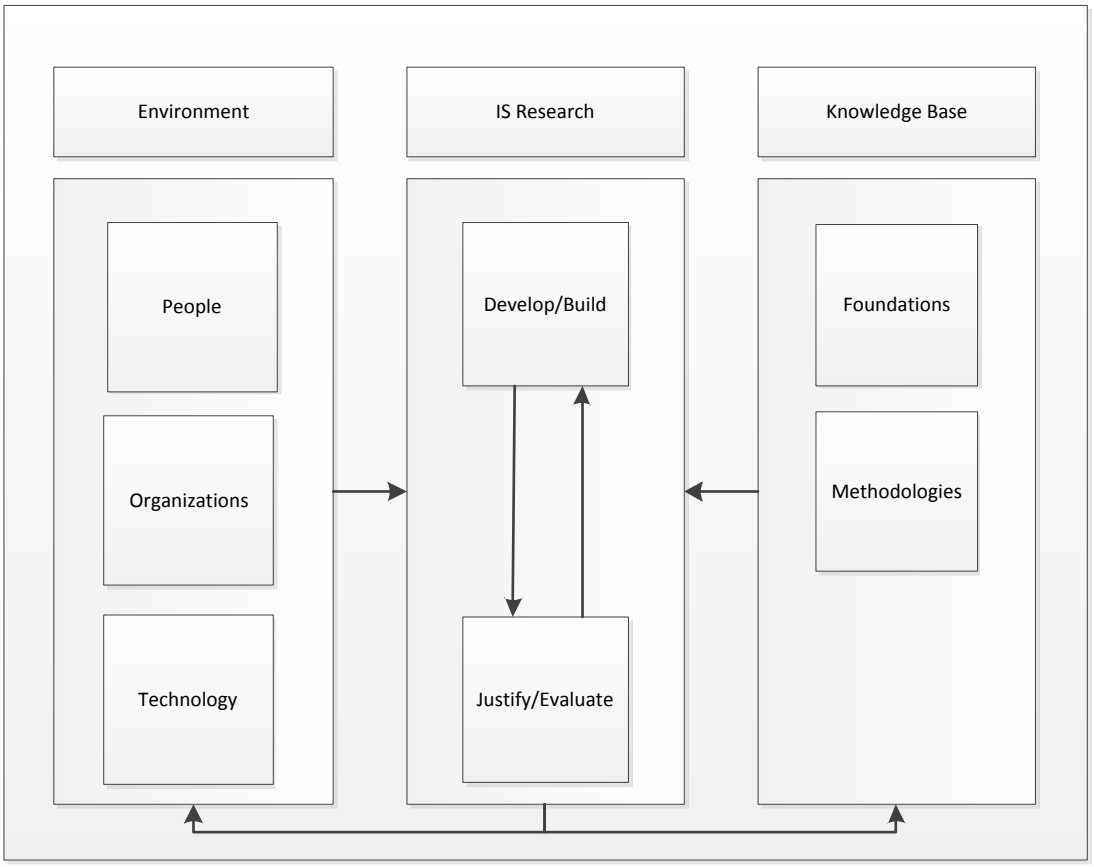


Figure 2.1 IS Science Research

Design science research consists of three pillars (environment, IS research and Knowledge Base). In the environment pillar, the problem space is defined and consists of people, organizations and technology. People perceive the goals, tasks, problems and opportunities that exist within their organization. The business within this organization needs to be evaluated within the context of strategies, structure, culture and business processes. Together with the existing technology, the problem space and business needs are defined. "The knowledge base provides the raw materials from and through which IS research is accomplished" (Hevner et al., 2004). The knowledge base contains both foundations and methodologies. With the two outer pillars in place, the actual IS research phase can take place. It combines the available knowledge of the environment and the knowledge base to either develop an artifact or validate human behavior.

Figure 2.1 provided the basic outline of design science research, but seven additional guidelines also need to be kept in mind during design science research according to Hevner (Table 2.1):

Table 2.1 Guidelines of design science research

Guideline	Description
Design as an artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Problem relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Design evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Research contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Research rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Design as a search process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Communication of research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

With the design science strategy in mind, a Process-Deliverable Diagram (PDD) of the research approach that is used in thesis is created and can be found in Figure 2.2.

The PDD notation is a technique used in method engineering for modeling methods and created by van de Weerd & Brinkkemper (2008). The PDD is based on the UML Activity Diagram. Activity Diagrams consist of activities and possible sub-activities, creating a hierarchical decomposition. Transitions are used to illustrate the flow from one activity to the next one.

The PDD consists of two sides; on the left side are the activities and on the right side are the deliverables of this research. The activities are ordered in a hierarchy; the large grey rounded rectangles are the main activities and they consist of multiple small white rounded rectangles, which are the sub activities. The description of activities is showed in the Activity Table (Table 2.2) and the deliverables are described in the Table of Concepts (Table 2.3).

In addition to the Activity Table & Table of Concepts, this section shortly describes the research method that is used in this thesis. The literature study phase contains research of the payment environment of a credit card transaction, the security standard and current issues in the transaction process. Another part of the literature study is the research of data breaches and corresponding indicators to such breaches. These indicators are solely based on literature in this phase and are validated in the next phase; the interviews with subject matter experts. The payment process and data breach part is also discussed as well as the impact of PCI DSS on the day-to-day business. Now that all the prerequisites for a prevention method are known,

the actual method can be constructed. Security events are defined as well as an analysis of data mining (-techniques). The creation of demands consists of an enumeration of demands for a breach prevention method. The final activity in this phase is the creation of the method. The method is evaluated with experts and that concludes this research.

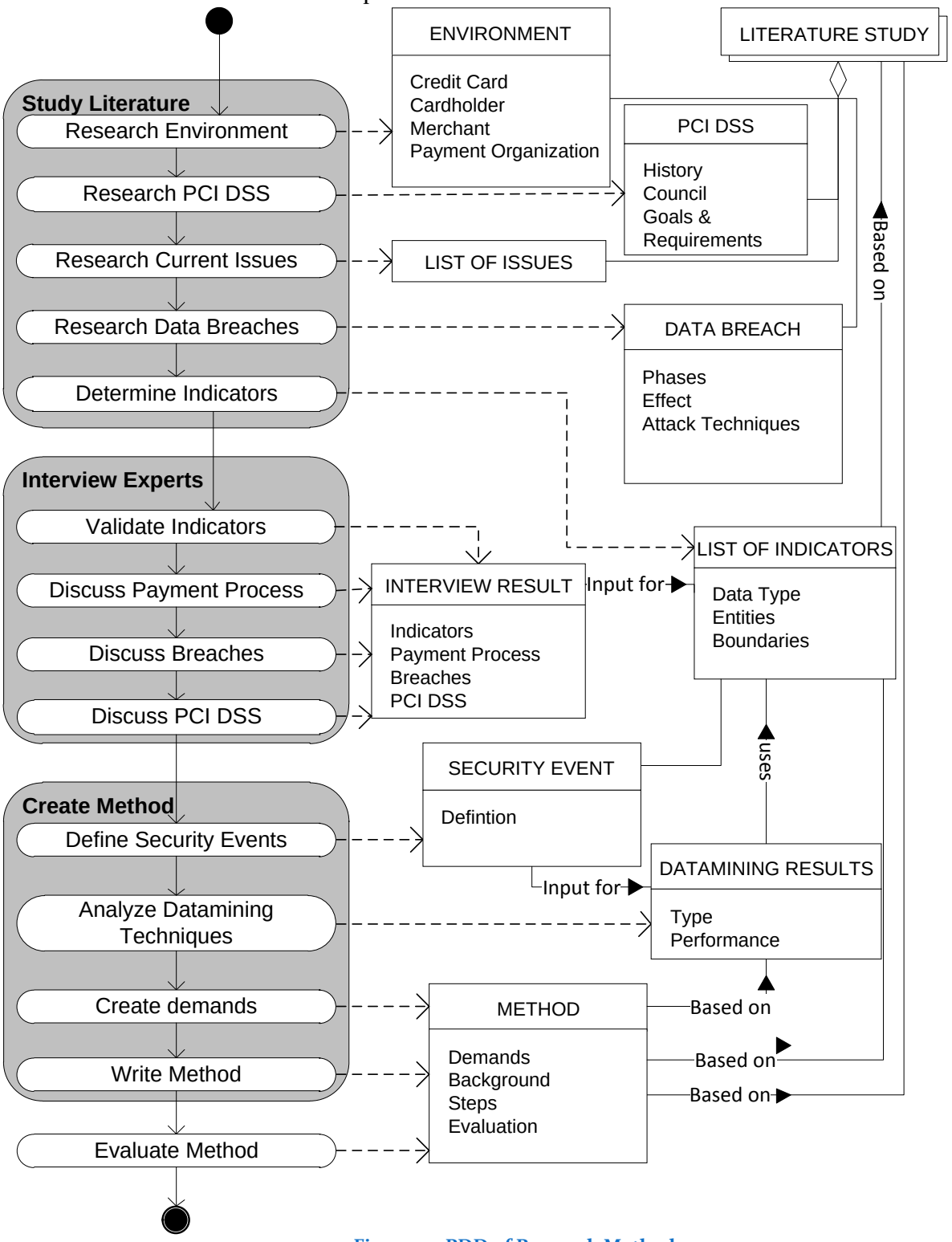


Figure 2.2 PDD of Research Method

Table 2.2 Activity Table

Main Activity	Sub Activity	Description
Study Literature	Research Environment	The environment of organizations that transfer, process or store credit card data is investigated in this activity. It is split up in the cardholder, organization and payment organizations (e.g. bank).
	Research PCI DSS	The Payment Card Industry Data Security Standard is the payment standard for organizations. This activity investigates PCI DSS and the corresponding requirements/goals.
	Research Current Issues	Critical points in the environment are addressed for every entity of the environment.
	Research Data Breaches	This activity investigates what a data breach is. It also explains what happens during a breach.
	Determine Indicators	Based on the characteristics of the previous activities, indicators are determined. They are based on literature.
Interview Experts	Validate Indicators	The list with indicators is discussed with the interviewees to validate the completeness of the list.
	Discuss Payment Process	The payment process of a credit card with all the entities as described in the environment chapter is discussed with the interviewees.
	Discuss Breaches	The concept of a breach is discussed with the interviewees and especially the possibilities to prevent breaches from happening.
	Discuss PCI DSS	The impact PCI DSS on an organization is discussed with the interviewees.
Create Method	Define Security Events	This activity defines what a security event is. This is necessary for the method to gain a good understanding.
	Analyze Data Mining techniques	Various data mining techniques are analyzed in order to find the best technique for every type of indicator.
	Create Demands	In this phase, the demands of the method, so what should this method do, are defined.
	Write Method	The actual method that uses data mining on security events is written in this activity.
Evaluate Method		The method is evaluated by getting feedback from experts.

Table 2.3 Table of Concepts

Concept	Description
LITERATURE STUDY	Concept that covers the whole section that is based on literature. This includes the environment analysis, PCI DSS explanation, Current issues and the data breach analysis.
ENVIRONMENT	The environment concept contains the data from the environmental analysis, which is a credit card anatomy, cardholder-, organizational- and payment organizational environment.
PCI DSS	This concept contains a detailed analysis of the standard for organizations that accept credit cards for payments. It consists of a brief history of the standard, the security council and a description of the goals and requirements.
LIST OF ISSUES	This concept represents a list of current issues with data breaches.
DATA BREACHE	This concept describes what a breach basically is and what it consists of. Different phases are elaborated on as is the effect it has on organizations that are/were breached. The concept also contains a description of some popular attacking techniques.
LIST OF INDICATORS	This is the most important concept as it contains the list of indicators the whole research is based on. Per indicator are its data type, entities and boundaries for its classification stored.
INTERVIEW RESULT	The results of the interview consist of the evaluation of the indicators, payment process, data breaches and the impact of PCI DSS. This content can vary per interviewee based on its background.
SECURITY EVENT	This concept contains the description of a security event that is used throughout the thesis.
DATA MINING RESULT	This concept contains the results from the data mining analysis. This includes the type of technique and performance results based on literature study/interviews.
METHOD	The final method that describes how organizations should implement the proposed technique to prevent data breaches in the future.

2.5. Relevance

2.5.1. Scientific Relevance

A substantial amount of scientific research is performed on the topic of:

- credit card fraud; (e.g. Cahill, Lambert, Pinheiro, & Sun, 2004; Montague, 2004; Pritchard, 2011)
- security breaches (e.g. Acquisti, Friedman, & Telang, 2006; Verizon, 2011; Widup, 2011; Xu, Grant, Nguyen, & Dai, 2008)
- data mining (e.g. (Fayyad, Piatetsky-Shapiro, & Smyth, 1996; Vaidya & Clifton, 2004)

What is missing is the research that combines these three concepts. Researchers have investigated the combination of credit card fraud and data mining (e.g. Bhattacharyya, Jha, Tharakunnel, & Westland, 2011; Debreceny & Gray, 2010; Ngai, Hu, Wong, Chen, & Sun, 2011) but the addition of credit card breaches in combination with prevention is missing.

This research tries to fill the gaps in the data mining/data breaches research field with a strong focus on credit card data. Future researchers are able to adopt this research and extend it for example with other sensitive data (e.g. Social Security Number, Electronic Patient Record).

2.5.2. Social Relevance

A secure payment environment is important for organizations that process credit card transactions. For them it is of high importance to catch a possible breach as early as possible. Therefore it is desirable to prevent future breaches or detect them in a very early stage by using a method. This is not only better for the organizations themselves, but also for their customers. This research also aims at increasing awareness of the current problem with securing a payment environment that contains credit card data.

2.6. Thesis Outline

This section describes the contents of this thesis.

The next chapter focuses on the environment of a credit card transaction. It explains all the parties that are involved from the beginning of the transaction at a customer through a merchant's organization via different banks to the billing to the same customer. A closer look at breaches can be found in chapter 4. Here is explained what a breach is, what happens during a breach and what the indicators of a breach are. Chapter 5 contains the empirical research part, which includes the interviews with the experts. The method to prevent data breaches in the future is created in chapter 6. It shows what security events are and how data mining of these events and log files can prevent breaches. The result of the evaluation of this method can be found in chapter 7. The thesis concludes with a chapter 8 with a discussion and conclusion and a chapter with recommendations and further research (chapter 9). Chapter 10 lists the references used.

3. Cardholder Environment

It is clear from the introduction and background chapter that the security of credit card transactions seems to be a problem these days. This chapter provides a closer look at the environment in which such a credit card transaction takes place. This environment consists of different parties that together perform a successful transaction. There is the customer who wants to make a transaction with his credit card. This customer is referred to as cardholder in the remaining of this thesis. The second party is the organization that receives the payment from the cardholder. This organization is referred to as merchant in the remaining of this thesis. The final party involved in the transaction is the bank and card network organizations. Different banks with different roles exist and will be made clear in subchapter 3.1.4. Subchapter 3.1 analyzes the flow of data from a cardholder, through a merchant to the banks (of the cardholder and merchant) and back to the cardholder. Subchapter 3.2 describes the Data Security Standard and its influence in the overall security of the payment environment of a merchant.

3.1. Environment

The environment of a credit card contains the cardholder, the merchant and the bank. Before these parties are described in subchapter 3.1.2 and further, a basic understanding of what a credit card actually is and means is necessary.

3.1.1. Anatomy of a credit card

In essence, a credit card is nothing more than a plastic card with a magnetic stripe, where most recent cards also have an additional chip on it. All the vital information (cardholder's data) is stored in the magnetic stripe or chip and some data is even printed on the card itself. This section shows what information is stored in this cardholder's data on the magnetic stripe/chip and the card itself.

Printed

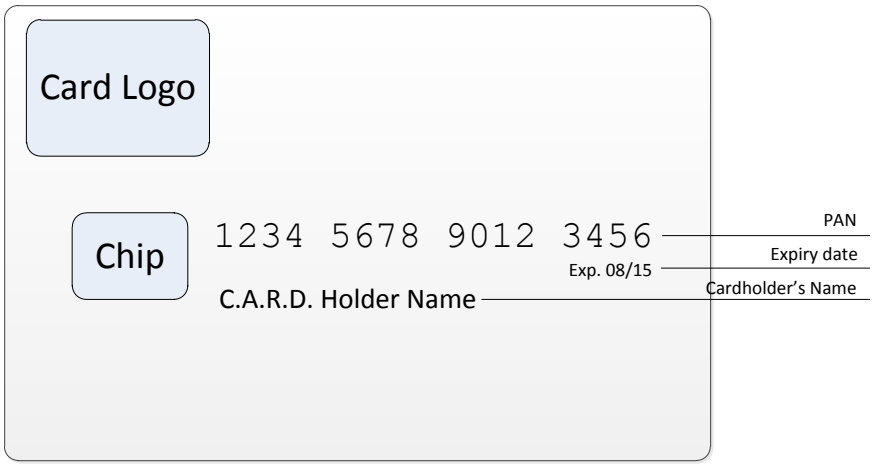


Figure 3.1 Front side of a credit card

A credit card has two sides, a front- and a backside. The front side is the side that, with many recent cards, holds the chip and/or cardholder name and number. The backside contains the signature of the cardholder and security codes. Figure 3.1 shows a systematic overview of the front side of a credit card. The information that is printed on this side is:

Primary Account Number (PAN); the PAN is 16 to 19 digit number. The number is not just a unique string of random generated digits; there is an ISO standard behind it; ISO/IEC 7812 (2006). The PAN consists of four different digit combinations(Stapleton & Poore, 2011):

Table 3.1 Major Industry Identifier Description ID

MII	Description
0	ISO and other industry assignments
1	Airlines
2	Airlines and other future industry assignments
3	Travel and entertainment and banking/financial
4	Banking and financial
5	Banking and financial
6	Merchandising and banking/financial
7	Petroleum and other future industry assignments
8	Healthcare, telecommunications and other future industry assignments
9	For assignment by national standard bodies

- The first digit is the Major Industry Identifier (MII) and represents the corresponding industry where the card is issued. Table 3.1 shows the different MII values and corresponding industries.
- The first six digits, including the MII, define the Issuer Industry Number (IIN) that represents the issuer.
- The next nine to twelve digits are the Individual Account Identification Number (IAIN) and represent a unique number created by the issuer to identify the owner of the card.
- The last digit, the Check Digit (CD), is a digit to check if the PAN is valid. This check is performed using the Luhn Algorithm (Li & Yao, 2011). This algorithm, also known as the modulo-10 algorithm, has three steps to check a PAN for validity:
    1. Multiply the value of alternate digits by 2, starting from the second rightmost digit;
    2. Add all the individual digits of the above products together with the un-doubled digits from the original number
    3. If the modulo 10 is equal to 0, then the number is valid, otherwise it is not.

Figure 3.2 shows an example of the Luhn check on PAN `123467890123456`. The sum of all the individual digits and the un-doubled digits is 64. 64 mod 10 is not equal to 0; therefore this example PAN is not a valid credit card number.

PAN	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
	X2		X2		X2		X2		X2		X2		X2		X2	
SUM:	2	2	6	4	1 0	6	1 4	8	1 8	0	2	2	6	4	1 0	6

Figure 3.2 Luhn Algorithm Example

Accountholder's name; for identification issues, the name of the cardholder is printed on the front side of the card, under the PAN.

Expiration Date; credit cards are not meant to last forever. Because of the usage of the card, the magnetic stripe slowly damages. Also the physical wear and tear to the card by swiping it through a terminal, or the tension from a wallet damages the card slowly. That is one of the reasons why credit cards have an expiration date, to make sure the card is always in a good condition. It is also a matter of security, because a card with an expired expiration date, as the name suggest, cannot be used anymore.

The information that is printed on the back of the credit card (Figure 3.3) is:

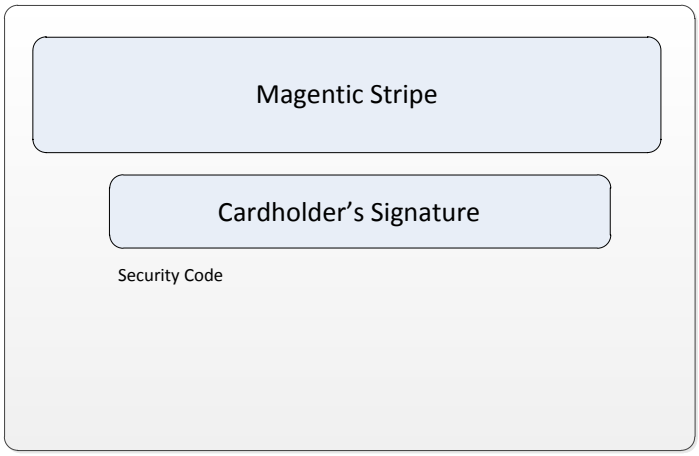


Figure 3.3 Back side of a credit card

Security Code; the security code is a code that validates the data that is given by the cardholder in card-not-present situations (situations where the physical card is not available at the merchant e.g. payments over the internet) or the data that is encoded on the magnetic stripe. For these two situations, a separate code exists. Card Issuers all have their own names for the security code like: Card verification Data (CVD), Card Verification Value (CVV), Card Verification Value Code (CVVC), Card Verification Code (CVC), Verification Code (VC) or Card Code Verification (CCV). The two types of security codes are distinguished by adding a "2" behind the name for the variant that is printed on the card. For example, the security code from VISA recorded on the magnetic stripe is called CVV and the code printed on the back is called CVV2. The Security Code is generated by encrypting the PAN, Expiration Date and Service Code with encryption keys only known to the issuing bank.

Signature; a signature from the accountholder is necessary to verify the identity of the accountholder when he hands over the card for a payment.

Magnetic Stripe/Chip

The information that is stored on the magnetic stripe consists of three tracks of data. A detailed description of the data and figures can be found in Appendix A. The three tracks of data(Padilla, 2002) exist of:

1. Track-1 is 79 or less digits in length. This track is also known as the International Air Transport Association (IATA) Track and is used by airliners for securing reservations with a credit card. Figure A.1 shows the components that are stored in this data track.
2. Track-2 is 40 or less digits in length. This track is also known as the American Banking Association (ABA) Track and is read by all Automatic Teller Machines (ATMs). All world banks must abide by it. The track contains the same data as the IATA track, but without the Format Code, the Name and some Field Separators. The most important difference is the missing Name field. Because this field is missing, the data can be all Binary-Coded Decimals (BCD), while the IATA track also needs to contain alpha-numeric data.
3. It is possible to store a third track, but it is almost never used in practice. None of the large card companies use this track, so it is mostly not even present on the magnetic stripe. Therefore, it is not addressed in this research.

This section showed the sensitive cardholder data that is being transferred during a transaction. The next section investigates the delivery of this data from the cardholder to a merchant.

3.1.2. Cardholder

A cardholder can provide his credit card data to merchants in three ways; automated, manual and via terminals. Automated means the merchant does not have to do anything in order to get the card data from the cardholder. This includes a cardholder who shops in a web shop and fills in his card details when he checks out. Manual means the merchant has to manually enter the card details into a system. This includes an order by phone or email. The last way is via a terminal and requires an additional device (Point of Sale, PoS) where the cardholder can swipe his card and the terminal captures and processes the card details. Section 3.1.3 investigates the ways of obtaining card details in more depth. These three payment methods can be divided into two groups (Figure 3.4); card-present and card-non-present situations. Card-present situations are all transactions where the credit card is physically shown to the merchant in order to make the payment, which is the case with a terminal. Card-non-present situations are all payments that do not require the card to be physically shown to the merchant. This is the case with payments via a web shop or by phone for example. The card-not-present situation is shown in the top, where all the relevant card data must be provided manually by the cardholder. The card-present situation provides the same card data, but this time the data comes directly from the card and together with the PIN-code or a signature, the transaction is performed. Figure 3.4, 3.5 & 3.6, for the cardholder and the other parties involved in the transaction, use shape and color coding to indicate whether an entity is transmitting, processing or storing cardholder data or it is a supporting entity. Table 3.2 shows the legend that corresponds with this coding.

Table 3.2 Data Flow Diagram Legend

Characteristic	Description
Green / Rounded	Entity is only transmitting cardholder data. No data is stored or processed.
Red / Squared	Entity transmits and stores/processes cardholder data
Yellow / Oval	Entity offers supporting functions, but it does not have contact with cardholder data
Red Line	Cardholder data is being transferred over this connection
Red dotted Line	Cardholder data is being transferred via one of these connections.
Black Line	No cardholder data is being transferred over this connection

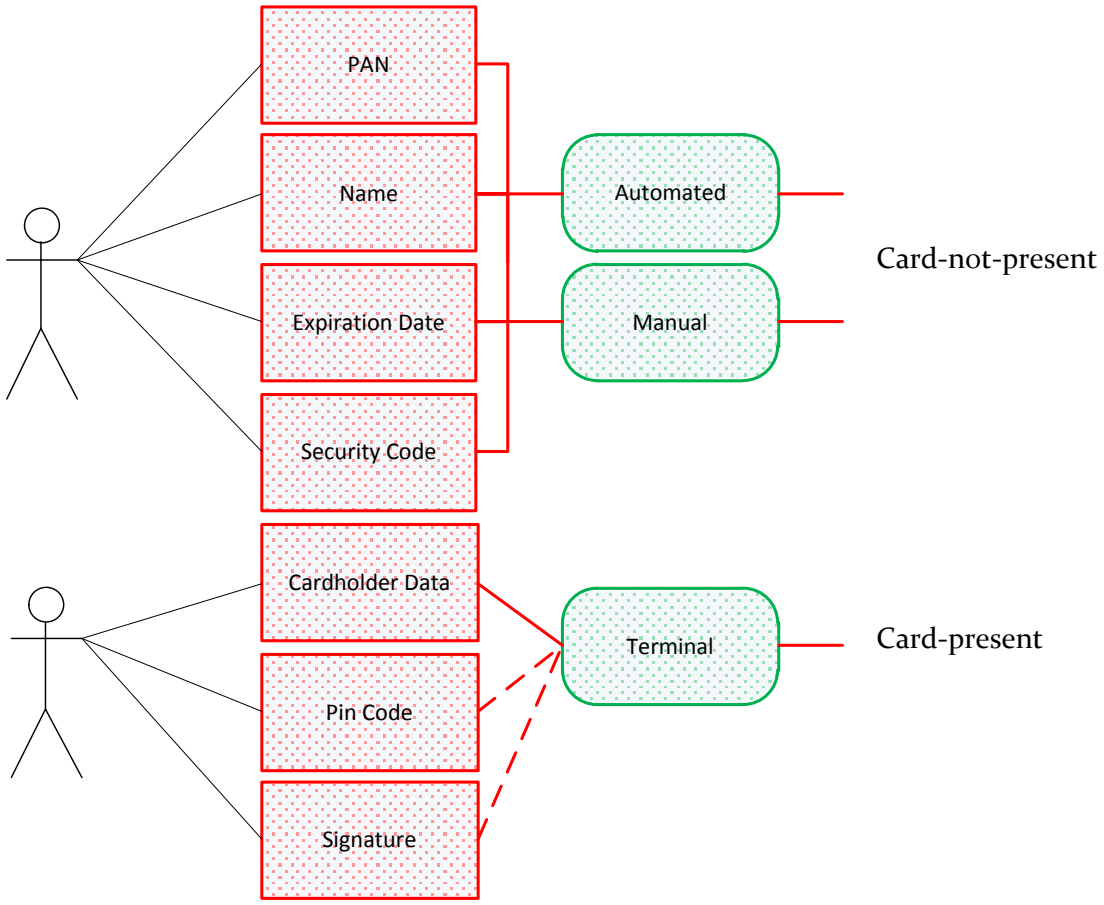


Figure 3.4 Data Flow of Cardholder

The cardholder data enters the merchant's organization in one of the three ways mentioned earlier. This concludes the cardholder's part of a credit card transaction. The next section continues the data flow within the merchant.

3.1.3. Merchant

Figure 3.5 shows the data flow of cardholder data within a typical merchant. The three ways of input are treated separately in this section, starting with automated.

Automated (e.g. web shop)

The cardholder data enters the, preferable, secure payment environment of the merchant located on the webserver. The customer fills in all his data and submits it. The webserver transmits this data to the payment gateway. This gateway functions as a man-in-the-middle between the merchant and the banks as it validates the card at the issuing bank. More about this validation and banks is in section 3.1.4 (Payment). When this validation is successful, the customer gets a notification that the payment will be performed and the order (including the cardholder data) is registered at the sales system and stored at the batch server. On a regular basis, all stored orders on the batch server are sent to the acquiring bank at once.

Manual (e.g. mail order & telephone order)

Manual payments require an additional activity from an employee, because the data must be entered into a system for further processing. After the data is entered into a CRM- or similar system, it follows the same path as the automated method. The validation of the card takes place while the customer is still in touch with the merchant (on-the-fly), so it knows if the payment can proceed or not.

PoS device (Terminal, imprinter)

If a customer starts the transaction at a terminal or similar PoS device, a direct connection with the payment gateway is made. It is up to the merchant if this request for payment is immediately forwarded to the acquiring bank, or stored at the batch server. The customer only provides the PIN code, or his signature and the physical card to the terminal, which reads the data from track-2 on the magnetic stripe. The CRM is skipped because the order already should have been stored. The only thing missing to complete the order was the payment, which is updated if the validation of the card is (un-)successful. Another PoS is a device (i.e. imprinter) that only requires the signature of the customer. A print of the credit card is made by the imprinter and the merchant fills in the required field (e.g. amount, date) and the customer signs this receipt and the transaction continues. The use of imprinters is out of scope for this research.

Payment Service Provider

Special organizations that focus on the transaction environment of merchants exist and are called Payment Service Providers (PSP). A merchant can outsource their complete payment process to these PSP's so they do not come in contact with credit card data at all. A hybrid solution, where the merchant collects the card data and sends it to the PSP for the completion of the transaction, is also possible and is showed in Figure 3.5.

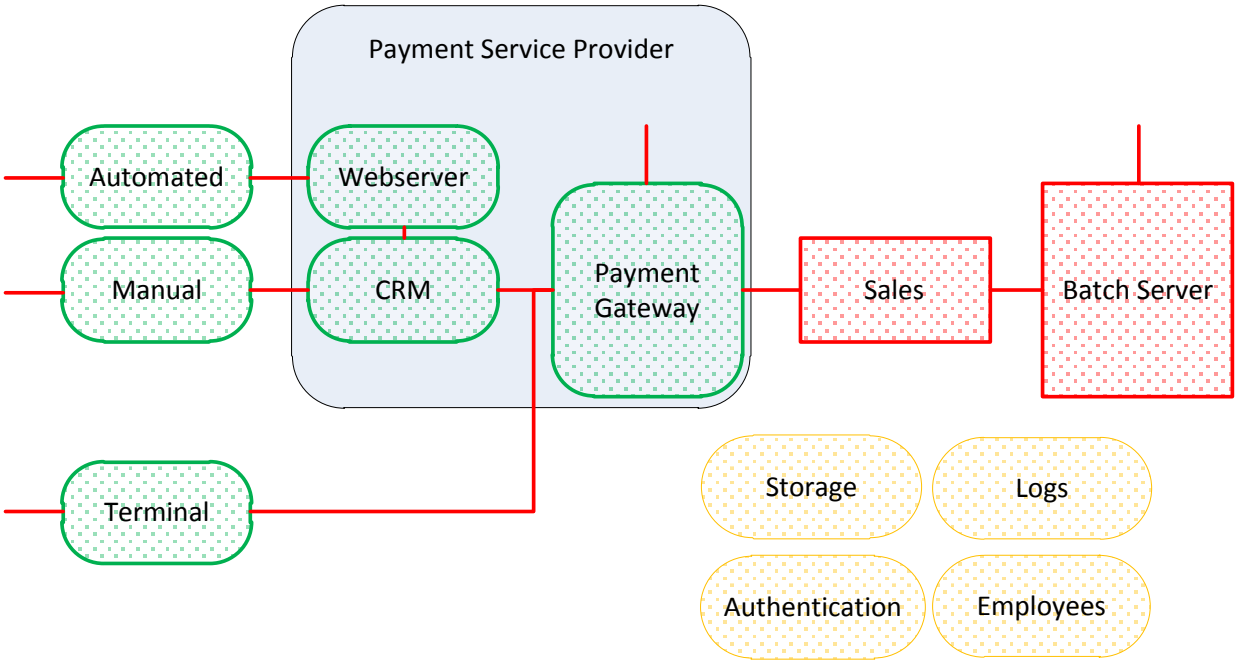


Figure 3.5 Data Flow within Merchant

Supporting Entities

The key entities in the payment process within a merchant are all explained, but there are also underlying/supporting entities that are relevant to the process as well:

- Storage; the storage entity represents the complete storage environment. This includes the storage servers, databases and management software.
- Logs; the log entity covers the whole log environment of a merchant. This includes logs generated on workstations, payment applications, servers, firewalls, virus scanners etc. The logs can be stored in a single log repository, which gathers log files throughout the network and places them in a central data base for further analysis.
- Authentication; every employee/system/application that needs access to the payment environment must be authorized.
- Employees; this entity not only represents employees as persons, but also contains all personal data of the employees, including their roles and responsibilities.

The process at the merchant is now finished. The data moves on to the next entity in the transaction; the banks.

3.1.4. Payment

This section of the payment process is about the actual payment, so the focus lies on the banks and card networks. Two types of banks exist; acquiring and issuing banks. An acquiring bank is a bank that accepts credit card transactions on behalf of the merchant. An issuing bank is a bank that provides cardholders with a credit card. The card networks act as a middleman between these two banks to make sure the payment is legitimate. There are three scenarios available in this part of the transaction; validation, payment and billing (CreditCards.com, 2009) and are shown in Figure 3.6. Red lines represent a flow of credit card data. Black lines represent confirmation messages or every other non-sensitive message. Green lines represent a flow of money.

Validation (1 till 4)

The merchant sends a request for payment to his acquiring bank (1). This bank forwards the request to the corresponding issuing bank for authorization (2). The result of the authorization is transferred back to the acquiring bank in the form of an authorization code when the authorization is successful (3). The acquiring bank approves the payment and notifies the merchant (4) (Evans & Schmalensee, 2005).

Payment (5 till 10)

The merchant sends a batch full of requests for payments to the acquiring bank (5). The batch is transferred to the card network (6), which will distribute every request to the right issuing bank (7). The issuing bank transfers the amount of money via the card network (8) to the acquiring bank (9). The acquirer finally pays the amount to the merchant (10).

Billing (11 & 12)

After the card network has requested the payment from the issuing bank and the issuing bank has transferred the money back to the acquiring bank, the cardholder is billed (11). The merchant receives an overview of his bill every month. The way in which a cardholder is supposed to pay this bill (12), e.g. immediately or in multiple terms that include interest, depends on the type of credit card that is being used and the corresponding contract.

There is a much more sophisticated model underneath the process that is described above. This includes for example direct costs involved for transactions. But it is not relevant for this research.

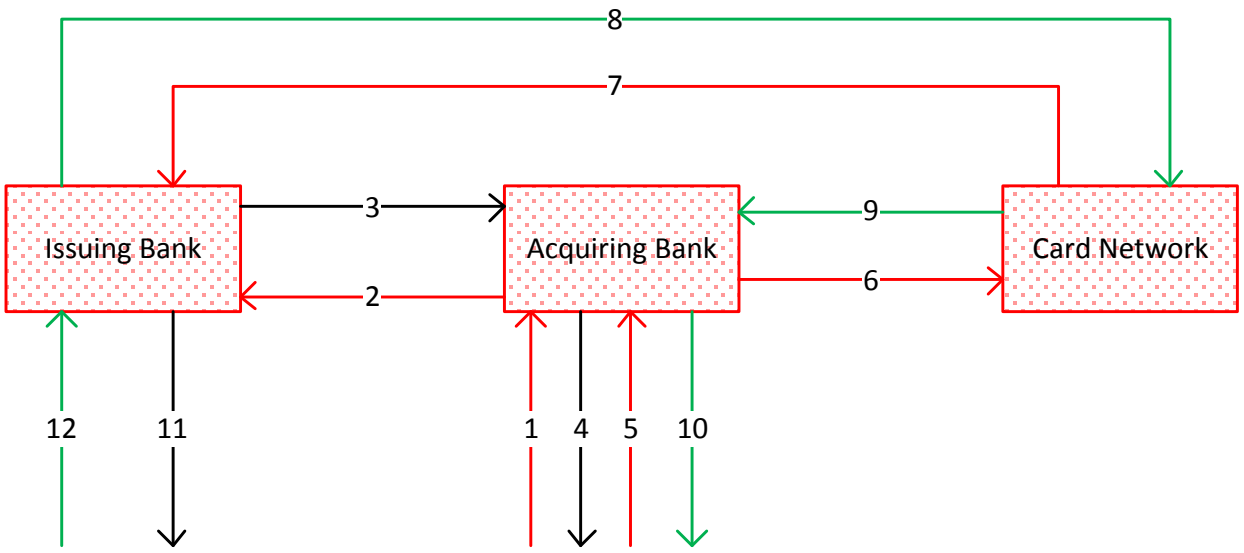


Figure 3.6 Data Flow Banks

The complete process from swiping a card to the authorization of the card only takes a matter of seconds.

This section concludes the complete transaction process. It showed the way in which the sensitive cardholder data from the cardholder travels to different entities in order to complete the transaction.

The next section focuses on the security of this process by uniform standards.

3.2. Payment Card Industry Data Security Standard

As chapter 3.1 showed, the transaction process of a credit card is a complex activity. Because of the sensitive nature of cardholder data, this transaction must be performed under strict and secure regulations. As with every process or activity, standards are available on how to perform the task in the supposed way. The standard for credit card transactions is the Payment Card Industry (PCI) Data Security Standard (DSS). This chapter describes the origin of this standard and its goals and requirements.

3.2.1. History

In June 2001, Visa started with a security program called Cardholder Information Security Program (CISP) to protect the cardholder's information (Visa Inc., 2001). It forced the cardholder information to be secure throughout the whole payment process, which includes merchants and service providers, that store, transfer and process this data. In 2003, MasterCard started a similar program called Side Data Protection (SDP) (MasterCard Worldwide, 2003). Because of the similarity of both standards, Visa and MasterCard decided to join forces and agreed to use the validation techniques described in CISP and use the rules of vulnerability scanning from SDP. In the meantime, other card brands have similar programs. Because these programs were so alike and merchants needed to comply with all the different brands in order to accept the card of that brand, a global standard was highly desirable. The five largest card network organizations (American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.) joined forces and created the PCI DSS. The standard is of great importance for the card brand, because it is their responsibility that the network is secure. By having such a standard, they oblige merchants and service providers to have a secure basis for their payment environment. The merchants and service providers must comply with this standard in order to perform any transaction that includes credit card data.

Because of ownership problems of the standard, the PCI Security Standards Council (PCI SSC) was founded in 2006 (PCI Security Standards Council, 2010a). This council is responsible for the development and maintenance of the standard. In October 2010, the improved version PCI- DSS 2.0 was introduced.

3.2.2. Security Standards Council

The SSC "develops, enhance, disseminates and assists with the understanding of security standards for payment card security" (PCI Security Standards Council, 2010b). 'Standards' imply there are more standards than solely PCI-DSS. The SSC has developed a total of three standards that provide the payment card environment with a secure basis. Figure 3.7 shows these three standards: PCI-DSS, Payment Application Data Security Standard (PA-DSS) and Pin Transaction Security (PTS). This division in standards is necessary because of the different requirements for the different parties involved in the payment environment. Figure 3.7 also shows the hierarchy between the three standards. PCI-DSS is meant for merchants, PA-DSS for software developers and PTS for manufacturers of PIN terminals. PTS is the hardware layer in the hierarchy while PA-DSS is the software layer and PCI-DSS is for the end-users of this hard- and software. The hardware layer has specific requirements compared with the software

layer, which in his turn has specific requirements compared to the end- users of the hard- and software. An overview of PA-DSS and PTS can be found in Appendix C.

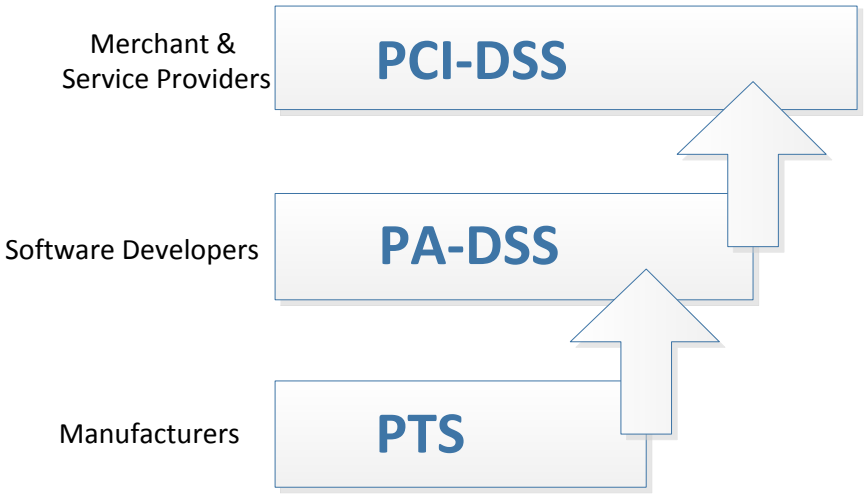


Figure 3.7 PCI SSC Security Standards (PCI Security Standards Council, 2010c)

The five card network organizations share equally in the SSC's governance and operations. Proposed additions or modifications to the standards by the Council are reviewed by other industry stakeholders, such as merchants, issuing banks, processors, hard- and software developers and other vendors.

The SSC also provides tools needed for implementation of the standards, such as assessments and scanning guidelines, a Self-Assessment Questionnaire (SAQ), trainings and education and product certification programs. Appendix B provides additional insight in the different validation techniques as offered by the SSC for PCI-DSS.

3.2.3. Goals & Requirements

PCI-DSS is the standard for all merchants and service providers that store, transmit or process cardholder data (Chuvakin & Williams, 2010). (Chuvakin & Williams) state a merchant as an organization that sells goods or services and accepts credit cards and they define a service provider as an organization that provides all or some of the payment services for a merchant. In the remainder of this thesis, I will focus only on the merchants.

In the end, the card network organizations are responsible for secure transactions since they provide the card and the underlying network. PCI-DSS reduces the risk of transactions that involve a credit card by motivating merchants and service providers to protect the cardholder data.

PCI-DSS has twelve main requirements that must be met in order to become compliant as shown in Table 3.3. They are divided into six goals with multiple requirements. A detailed description of the goals and requirements can be found in Appendix B.

Table 3.3 High-level Overview of Goals & Requirements of PCI-DSS 2.0 (PCI Security Standards Council, 2010d)

Goal	#	Requirement Description
Build and Maintain a Secure Network	1	Install and maintain a firewall configuration to protect cardholder data
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5	Use and regularly update anti-virus software or programs
	6	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7	Restrict access to cardholder data by business need to know
	8	Assign a unique ID to each person with computer access
	9	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes
Maintain an Information Security Policy	12	Maintain a policy that addresses information security for all personnel

In order to become PCI DSS compliant, an ongoing process must be followed. It consists of three main activities (PCI Security Standards Council, 2010b):

- Assess; identification of cardholder data and creation of inventory of IT assets and business processes for payment card processing. All these are analyzed for vulnerabilities that might expose cardholder data.
- Remediate; reparation of identified vulnerabilities and cardholder data is only stored when needed.
- Report;Submission of required remediation validation records and compliance reports to banks and card issuer.

Based on this validation report, an organization receives the status PCI-DSS compliant or not. The way in which this validation takes place is different for merchants and may also differ per card brand and transaction volume. Table 3.4 shows the different levels of merchants as decided by the card network organizations. The transaction volumes are annual volumes for all organizations. Based on the level, the validation methods (Table 3.5) are defined. A description of these validation methods can also be found in Appendix B. If an organization has a data breach in the past, it automatically becomes a level 1 merchant for the corresponding card organization.

Table 3.4 Merchant Levels

Level	American Express	Discover	JCB	MasterCard	Visa
1	>2.5 million	>6 million	>1 million	>6 million	>6 million
2	50k-2.5 million	1-6 million	<1 million	1-6 million	1-6 million
3	<50k	20k-1 million		20k-1 million	20k-1 million
4		<20k, other		<20k, other	<20k, other

Table 3.5 Validation methods per level

Level	Validation Method
1	Annual on-site Security Audit Quarterly network scan
2	Annual Self-Assessment Questionnaire (SAQ) Quarterly scan by Approved Scanning Vendor (ASV)
3	Annual SAQ Quarterly scan by ASV
4	Annual SAQ Quarterly scan by ASV (recommended or required)

Recent addition

The encryption of credit card numbers inside an organization is important when protecting against data theft. Various ways of encrypting data exist (e.g. Data Encryption Standard, Advanced Encryption Standard, Public Key Infrastructure) but for credit card data, tokenization is recommended by the SSC (PCI Security Standards Council, 2011). Tokenization will be discussed briefly in this section because it provides protection to stored data or data that is in transfer and it is one of the latest additions to PCI-DSS (august 2011).

Tokenization is included in PCI-DSS requirement 3.4: "Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs)"(PCI Security Standards Council, 2010d). Tokenization is a special form of encryption where not the complete data is encrypted with a key, but only a part of the data (Stapleton & Poore, 2011). Furthermore, this data is replaced with a token that looks like a random chunk of data from which it is unfeasible to compute the original data if only the token is known. This process is called token mapping. The token functions as a key that represents a record in a database, or data vault, that can replace the token with the original data. The PAN is still encrypted with an encryption technique so that the original PAN is never stored without proper encryption. The process where the token is replaced with its original data is called de-tokenization and should be restricted to authorized employees only. Figure 3.8 shows a systematic overview of the complete tokenization process. An application provides a PAN and an authorization code to the tokenization system. A check is performed to verify the authorization of the provided PAN. If this authentication fails, the complete process fails. If it succeeds, a token is generated or a token that already exists for this PAN is returned to the application. The PAN and token is

then stored in the card data vault. De-tokenization follows the same path as Figure 3.8, but instead of a PAN, the application provides a token and receives the corresponding PAN.

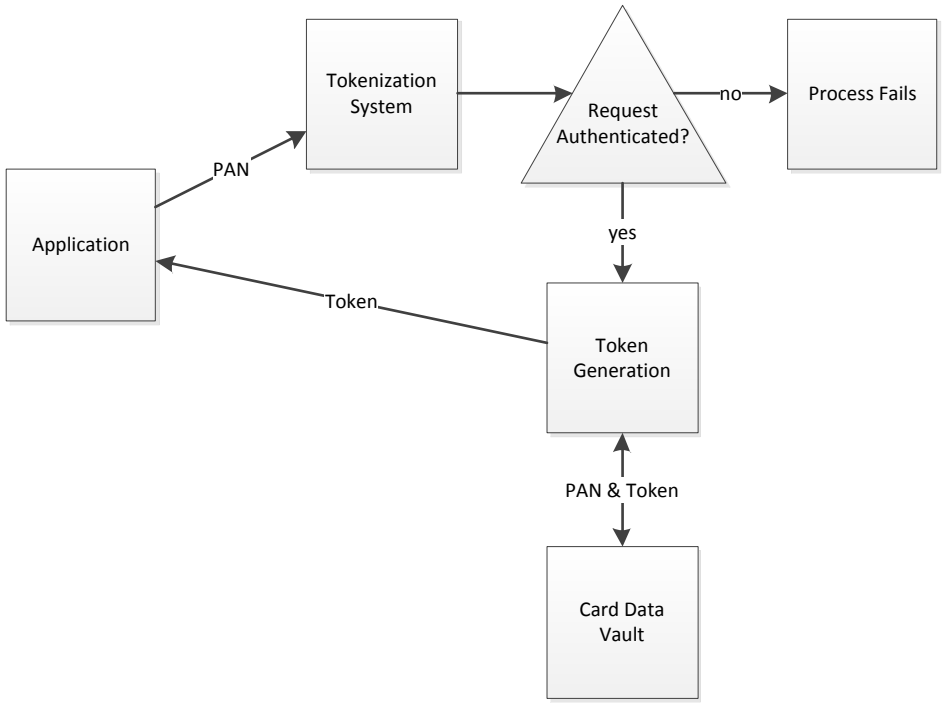


Figure 3.8 Tokenization Process (PCI Security Standards Council, 2011)

The card data vault can be physically at the merchant or stored locally at a third party service provider (Cheney, 2010).

Tokenization is used in a PCI-DSS context for encrypting the PAN and should be used wherever PANs are stored. Tokenization of authentication data, such as CVC/CVV codes, is not permitted by requirements of PCI-DSS. The CVC/CVV codes are only used for verifying the identity of the customer and to decrease fraudulent transactions. There is no need to use these codes after the transaction is completed and therefore no need to store them, even in an encrypted format. The data vault, which contains both tokens as PANs, is very sensitive and therefore the most attractive target for attackers. This source needs to be protected by any means.

4. Data Compromise & Indicators

The previous chapter discussed the environment of a credit card transaction that included all parties involved in this process. This chapter focuses on the compromise of data or the data breach. What is a breach, what are the effects of a breach, what happens during a breach and what are the indicators of a breach are some questions that are being answered. The list with indicators is the foundation for the data breach prevention method in Chapter 6.

4.1. Current Issues

A top ten of the largest data breaches of all time illustrates the risk of large breaches today. Table 4.1 shows this top ten based on data from an online data breach list (DatalossDB, 2012b). The table below is the legend for the Data column. The breaches that included credit card numbers are 1, 2, 4, 5, 8 and 10 (60%). As is visible from the table, the two largest breaches both included credit card data. Another important observation is that five of the ten largest breaches occurred in 2011 (nr. 4, 6, 7, 8 and 10).

Table 4.1 Largest data breaches to date (DatalossDB, 2012b)

Rank	Records	Date	Organization	Data
1	130.000.000	2009-01-20	– Heartland Payment Systems – Tower Federal Credit Union – Beverly National Bank	CCN
2	94.000.000	2007-01-17	– TJX Companies Inc.	CCN, NAA
3	90.000.000	1984-06-01	– TRW – Sears Roebock	SSN, FIN
4	77.000.000	2011-04-26	– Sony Corporation	CCN, NAA, EMA, MISC, ACC, DOB
5	40.000.000	2005-06-19	– Cardsystems – Visa – MasterCard – American Express	CCN
6	40.000.000	2011-12-25	– Tianya	MISC, PWD
7	35.000.000	2011-07-28	– SK Communities – Nate – Cyberworld	SSN, NAA, EMA, MISC, MED, DOB, PWD, ADD
8	35.000.000	2011-11-10	– Steam (Valve, Inc.)	CCN, EMA, MISC, ACC, PWD, ADD
9	32.000.000	2009-12-14	– Rock You Inc.	NAA, EMA, MISC
10	24.600.000	2011-05-02	– Sony Online Entertainment – Sony Corporation	CCN, NAA, EMA, MISC, ACC, DOB

CCN	SSN	NAA	EMA	MISC	MED
Credit Card Number	Social Security Number	Names	Email Addresses	Miscellaneous	Medical
ACC	**DOB**	**FIN**	**PWD**	**ADD**	
Account	Date of Birth	Financial	Passwords	Addresses	

Another interesting finding from the top ten breaches is that all of the ten breaches have been performed from the outside (external attacker). The top ten only includes breaches that occurred using a hack into the organizations. If other techniques are used, only the number 1 will be different, which is a fraud case. This breach was published on March 17 2012 and included 150 million records of customer information (no credit card numbers). It was an attack from the inside out where employees illegally sold customer information.

The issues with breaches are clear, but what exactly is understood by a breach? The next paragraph covers the definition of a breach or compromise in order to have a consistent mindset throughout the remainder of the thesis.

4.2. What is a breach or compromise?

The term data breach has various interpretations. A few are mentioned below, together with the definition that is created and used in this thesis.

Data breaches or compromises are:

- "The lost, theft or otherwise sharing of people's personal private data with unauthorized parties" (Widup, 2011)
- The compromise of data from an organization by attackers (Verizon, 2012)
- "The exposing of consumers' personal information to misuse" (Visa Inc., 2008)
- "An organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security Numbers, or financial information such as credit card numbers" (Peretti, 2008)
- "The exfiltration – the release of data from a system without the knowledge or consent of its owner"(Trend Micro, 2011)

In this thesis the following definition of data breaches is used:

The theft or compromise of sensitive information by attackers, both internal as external, without the knowledge of the owner.

The sensitive information is narrowed to only include cardholder data in this research.

Attackers are those persons who compromise the data and do not necessarily have to be someone from outside the organization, although in most breaches an external attacker causes the breach. In 2010, 7% of all the breaches were caused solely by internal persons, 83% solely by an external attacker and 10% by a combination of both internal as external (Verizon, 2011). Symantec states in their report (2009a) three types of attackers: well-meaning insiders, targeted attackers and malicious insiders. A description of these types of attackers, together with corresponding attacking techniques can be found in paragraph 4.6.

This research is about credit card transactions at merchants and payment service providers and therefor only focuses on the financial breaches (breaches that include both credit and debit cards). According to the Verizon, 25% of all the breaches and 56% of all the compromised records in 2010 were in the retail sector. Another 22% of all the breaches and 35% of all the compromised records were in the financial service sector. These numbers does not mean that all these records are also credit card data.

4.3. Effects of a breach

Every year, the average cost of a stolen record is computed by the Ponemon Institute. Together with Symantec (2011), they computed for 2010 the global average at $156 per record. It is important to understand that this number is just an average. For large breaches, this number will be significant lower and for small breaches significant higher because of the fixed costs that are necessary after a breach such as investigation costs. No matter the size of the breach, these costs are always made. Also the geographical location of the breached organization is relevant (e.g. US: $214, UK: $114). This is based on different national data protection policies that imply additional costs for some organizations.

Acquisti, Friedman and Telang researched the impact of data breaches at an organization on its market value (Acquisti et al., 2006). Their research showed a "statistically significant and negative impact, although it is short-lived". This research was based on a small sample set of data breaches and is currently extended with more breaches.

Table 4.2 Six Years of Data Breach results

Category	Results
Incidents	3.765
Records	806.200.000
Data breach costs	$156.700.000
Most common vector	Laptop Theft
Most records exposed	Hacking
Caused most damage	Outsiders

Widup (2011), together with the Digital Forensics Association, investigated data breaches from the past six year. **Error! Reference source not found.** shows the high-level outcome of this esearch. A total of 3.765 incidents occurred from 2005 through 2010 and included a total of 802.6 million records. The estimated cost for these breaches is over $156 million. This is not the final amount and a low estimate since 35% of all the breaches did not name a figure for records lost. The most common vector is the stolen laptop, as it has been for the last years. 48% of the compromised records were caused by hacking activities. As said before, the outsiders caused the most damage. An interesting finding is that only 15% of all the records included credit card numbers. Names, addresses and social security numbers were included in 65% of all the records.

4.4. What happens during a breach?

During a breach, data is compromised from an organization. An interesting question is how attackers succeed in gathering this data. A data breach consist of four phases; infiltration, observation, collection and exfiltration as shown in Figure 4.1 (Symantec, 2009a). It does not have a standard duration, neither does every phase has to take place. For instance, a malicious insider already has access to the network and probably also knows the location of the target data. Combinations of phases are also possible. For example, the collection and exfiltration phase can take place simultaneously if data is captured and send to the attacker on the fly (data being sent to the attacker on the moment he compromises it). The remainder of this subchapter describes the four phases of a data breach.

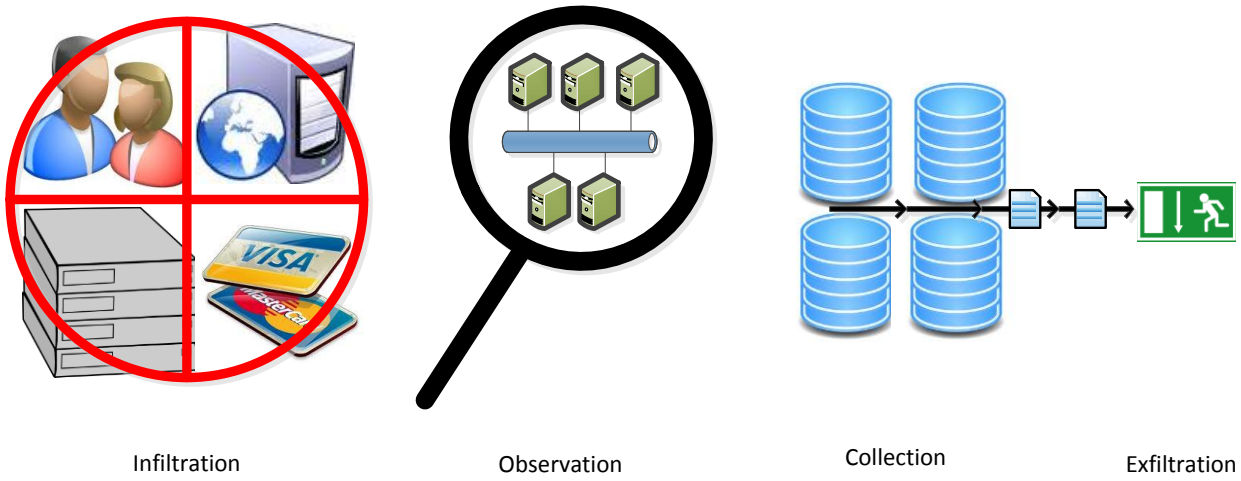


Figure 4.1 Four phases of a Data Breach

4.4.1. Infiltration

During the first phase of a breach, infiltration, the attackers search for a way of entry into the targeted organization. The way in which the attackers manage to penetrate the organization can be in different forms. Figure 4.2 shows these forms and ranked them by their occurrence in 2012.

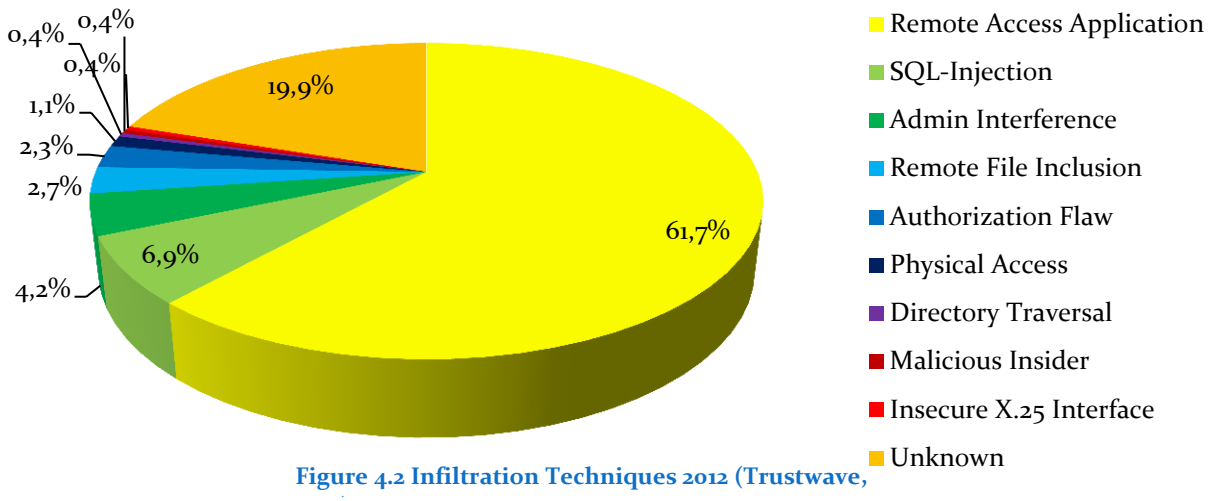


Figure 4.2 Infiltration Techniques 2012 (Trustwave,

Table 4.3 shows the difference between the distribution of infiltration techniques in 2012 and 2011 (Trustwave SpiderLabs, 2011). As with previous years, Remote Administration Application (RAA) is by far the most used technique to infiltrate an organization.

Table 4.3 Infiltration Technique Differences 2012-2011

Technique	2012	2011	Difference
Remote Access Application	61,7%	55,0%	6,7%
SQL-Injection	6,9%	6,0%	0,9%
Remote File Inclusion	2,7%	1,0%	1,7%
Physical Access	1,1%	2,0%	-0,9%
Malicious Insider	0,4%	2,0%	-1,6%
Unknown	19,9%	18,0%	1,9%
Admin Interference	4,2%	--	--
Authorization Flaw	2,3%	--	--
Directory Traversal	0,4%	--	--
Insecure X.25 Interface	0,4%	--	--
Other	--	16,0%	--

RAA are all applications that are used for remote administration of computers; they provide total control over a machine. They can use a Graphical User Interface (GUI) or a command line to receive command from the user. Example of RAA tools are Remote Desktop that uses the RDP (Remote Desktop Protocol) and is built into windows or the popular commercial package PCAnywhere from Symantec.

The encryption and authentication of RAA tools has been and is still a common used vulnerability. A technique that can be used to exploit this vulnerability is the so-called Man-In-The-Middle (MITM) attack (Montoro, 2005):

1. The client thinks he connects to the server, but instead, he connects to the MITM. The MITM forwards the requests to the actual server.
2. The server provides the MITM his public key and some salt (i.e. random bits that are used for encryption) in clear text. The MITM forwards this package to the client, but changes the public key for another one for which he also knows the private key.
3. The client answers with random salt encrypted with the public key from the MITM.
4. The MITM decrypts this salt and encrypts it with the public key from the server and sends it to the server.
5. The MITM now has both the salt from the server and the client, which is enough to create the session keys that are used for further communication. All data that is being transferred between client and server can now be read by the MITM.

A description of the other infiltration techniques can be found in the Glossary at the end of this thesis. By all the means provided in this section, the attackers now have a point of entry into the organization's internal network.

4.4.2. Observation

The observation phase is meant to outline the organization's systems and scan network traffic in order to map the complete, or at least the most important part, of the internal network and systems. The techniques used in this phase are mostly the same as in the infiltration phase. The same holds for the collection phase.

The attackers are already inside an organization and past the first line of defense. Organizations that only focus on the outer perimeter have a disadvantage here, because attackers that can break this line of defense can perform actions more stealthy than within organizations that have multiple lines of defense. For this phase it is important to monitor your network. Any devices or protocols that should not be available on the network or are unknown should be investigated. By connecting to the organization network, attackers are able to make an outline of the systems in the organization and locate the data they are after.

4.4.3. Collection

In the third phase, the real compromise takes place. Attackers take over unprotected or unsecured systems and capture data from them. Even secured system can be compromised if the correct information, e.g., login/password combinations, is gathered prior to the compromise.

The attackers already have had access to the network of an organization and can now focus on more specific systems or parts of the organizational network. By doing so, they limit their detectability, because they are not performing actions on the complete network anymore. Therefore, systems that store or process sensitive data require more protection than other systems. Of course, the systems that do not store or process sensitive data must be secured as well, because they could be used to gain entrance to other systems.

4.4.4. Exfiltration

During the last phase of a breach, all the compromised data is sent back to the attackers. This can be done in multiple ways as Figure 4.3 shows, ranked by occurrence in 2009. This analysis is based on a study of 200 data breaches in 24 different countries by SpiderLabs (Percoco, 2010).

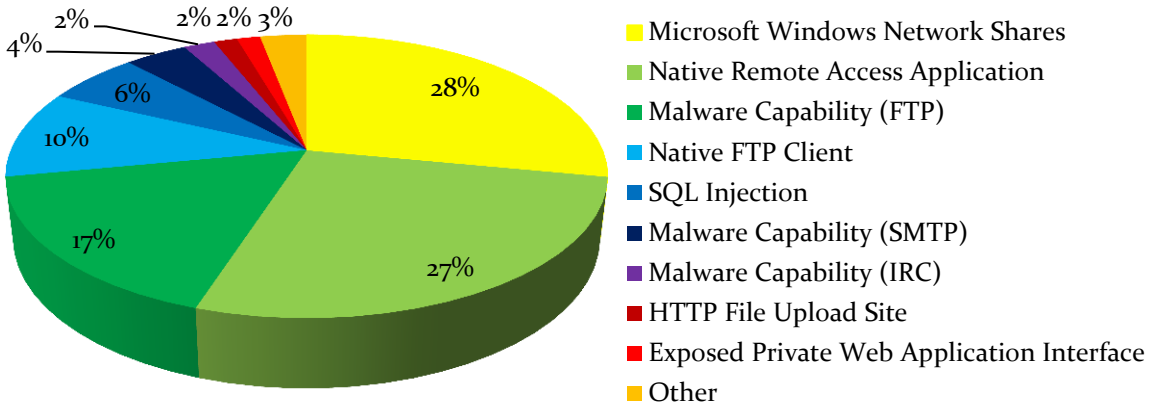


Figure 4.3 Means of Exfiltration (Percoco, 2010)

A short description of the results of Percoco's research is that in 27% of all the situations, remote access applications are used. These applications were also used to gain entrance to the organization in the infiltration phase. File Transfer Protocol (FTP) and HyperText Transfer Protocol (HTTP) are also popular techniques to transfer data. The use of these protocols together with malware is a frequently used combination. The relatively most frequently used technique is the use of the Microsoft Windows Network Sharing service to transfer records from the targeted machine to the machine of the attackers.

4.5. Data Breach Indicators & Current Processes

The foundation of the method that is created in chapter 6 is a list of data breach indicators. This chapter investigates indicators based on security events that might indicate a data breach.

4.5.1. Data Breach Indicators

A total of fifteen indicators have been selected from literature:

[1] (Aldridge, 2010)
[2] (PricewaterhouseCoopers LLP, 2009)
[3] (Verdurmen, Beierly, & Cleary, 2011)

and previous breaches:

[4] Heartland Payment Systems Breach (Cheney, 2010)

- Table 4.4 and The second column (IDPS Type) indicates to which type of Intrusion Detection and Prevention System it relates to. A more detailed explanation of these types can be found in section 4.5.3.
- The third column provides the name of the indicator
- The fourth column (Breach Phase) indicates in which phase of a breach this indicator occurs. The letters in the headers correspond with the first letter of the four phases (Infiltration, Observation, Collection and Exfiltration).
- The last column (Literature) provides the source of the indicator.

The sooner a breach is discovered, the faster it can be stopped and the better it is for the organization, because of the possible mitigation of further damage.

- Table 4.5 show these indicators together with some important details. The second column (IDPS Type) indicates to which type of Intrusion Detection and Prevention System it relates to. A more detailed explanation of these types can be found in section 4.5.3.
- The third column provides the name of the indicator
- The fourth column (Breach Phase) indicates in which phase of a breach this indicator occurs. The letters in the headers correspond with the first letter of the four phases (Infiltration, Observation, Collection and Exfiltration).
- The last column (Literature) provides the source of the indicator.

The sooner a breach is discovered, the faster it can be stopped and the better it is for the organization, because of the possible mitigation of further damage.

Table 4.5 provides a definition of all the indicators that is based on literature study and previous breaches and is formulated prior to the empirical research part with security experts. Table 4.4 provides more context information:

Table 4.4 Data Breach Indicators Phases

#	IDPS Type	Name	Breach Phase				Literature
			I	O	C	E	
1	Host Based	Excessive logins.		x			[3]
2	Host Based	Modification of Data			x	x	[3]
3	Host Based	Automatic launch of suspicious applications on boot		x	x	x	[3]
4	Network Behavior	SQL Injection Attempts	x	x			[3], [4]
5	Host Based	New unexpected user accounts		x	x		[3]
6	Host Based	Existence of suspicious files in system directory			x	x	[3]
7	Host Based	Unusual Log Files	x	x	x	x	[3]
8	Network Behavior	Unusual high/low network activity	x	x	x	x	[1], [2]
9	Host Based	Improper account usage	x	x	x		[2]
10	Network Based / Host Based	Improper protocol usage		x	x		[1]
11	Network Behavior / Host Based	Uploading of unusual files		x	x	x	[1]
12	Host Based / Network Behavior	Unusual running services			x	x	[1], [3]
13	Host Based	Registry Keys modification			x		[1]
14	Host Based / Network Behavior	Unknown/unexpected network connections	x	x	x	x	[2]
15	Host Based / Network Behavior	Malware notification	x	x	x	x	[4]

- The second column (IDPS Type) indicates to which type of Intrusion Detection and Prevention System it relates to. A more detailed explanation of these types can be found in section 4.5.3.
- The third column provides the name of the indicator
- The fourth column (Breach Phase) indicates in which phase of a breach this indicator occurs. The letters in the headers correspond with the first letter of the four phases (Infiltration, Observation, Collection and Exfiltration).
- The last column (Literature) provides the source of the indicator.

The sooner a breach is discovered, the faster it can be stopped and the better it is for the organization, because of the possible mitigation of further damage.

Table 4.5 Data Breach Indicators Description

#	Name	Description
1	Excessive logins	An account/workstation/server has an unexpectedly high number of login attempts or no logins at all for a certain period in time.
2	Modification of Data	A modification of data occurs on data that should not be changed. This can be critical organizational data or data located in system directories.
3	Automatic launch of suspicious applications on boot	Unknown applications or services are set to launch automatically during the boot process. This implies a whitelist of applications/services that should run during the boot process must be available.
4	SQL Injection Attempts	a currently implemented Intrusion Detection and Prevention System detect an SQL-Injection attempt on some webserver/database.
5	New unexpected user accounts	New user accounts appear on the network and they are not linked to an employee. Also user accounts that exists for a short period of time, e.g. they are only used to perform a single task, fall under this indicator.
6	Existence of suspicious files in system directory	Archived files, executables, deletion/copying/modification of data in system directory occurs. This can be extended with other critical directories or even complete databases/servers.
7	Unusual Log Files	if the chronologies of log file creation changes or they contain unusual items.
8	Unusual high/low network activity	Systems that should have a particular network activity are suddenly offline or have an increased network activity.
9	Improper account usage	User accounts are active on systems where they should not have access to.
10	Improper protocol usage	Network traffic contains unknown protocols, or protocols that are not used in the correct way. Either because they are misused or used in the wrong place.
11	Uploading of unusual files	Malware or other files that do harm to a system are uploaded by the attackers to the targeted systems. They create ways of entrance or maintain entrance to an organization for the attackers.
12	Unusual running services	Detection of services that are running, which are blacklisted, unknown or blocked by administrators.

13	Registry Keys modification	Modifications in the registry to bypass security policies occur.
14	Unknown/unexpected network connections	Unknown or blacklisted IP-addresses occur in the network or firewall logs. Also if known IP-addresses connect to servers/hosts that they should not connect to under normal circumstances indicate something is wrong.
15	Malware notification	Virus- or malware scanners detect suspicious files. If such a file is found, an immediate warning is signaled out.

Statistics

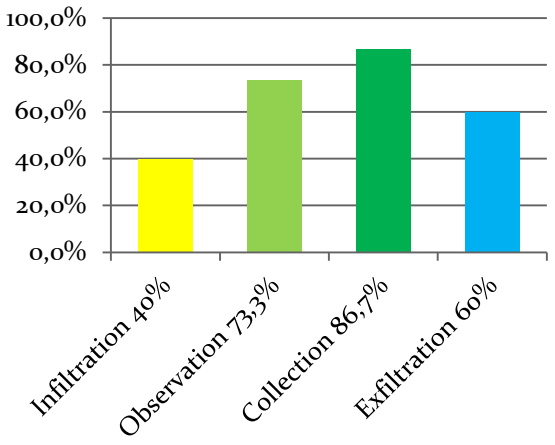


Figure 4.4 Indicators - Phases

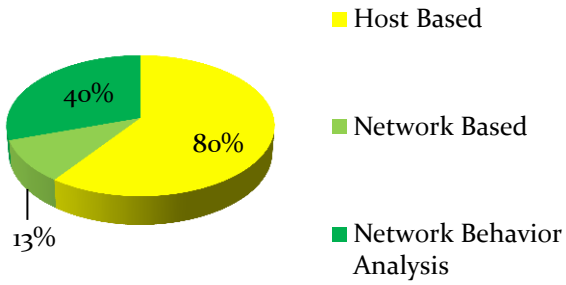


Figure 4.5 Indicators-IDPS types Distribution

Figure 4.4 shows the distribution of indicators onto the four phases of a data breach. The same holds for Figure 4.5, which shows the distribution of indicators into the four types of Intrusion Detection and Prevention Systems (IDPS). Section 4.5.3 provides more details about IDPS. Figure 4.4 shows that 40% of the indicators occur in the infiltration phase and 73.3% in the observation phase, where Figure 17 shows that 80% of the indicators are categorized in the Host Based type of IDPS. Although IDPS guidelines explicitly describe that wireless protocols and traffic cannot be monitored by network based IDPS (Scarfone & Mell, 2007), it is not used in this research. Because the IDPS types are only used for illustration purposes, the wireless type can be combined with the regular network based type, as section 4.5.3 explains.

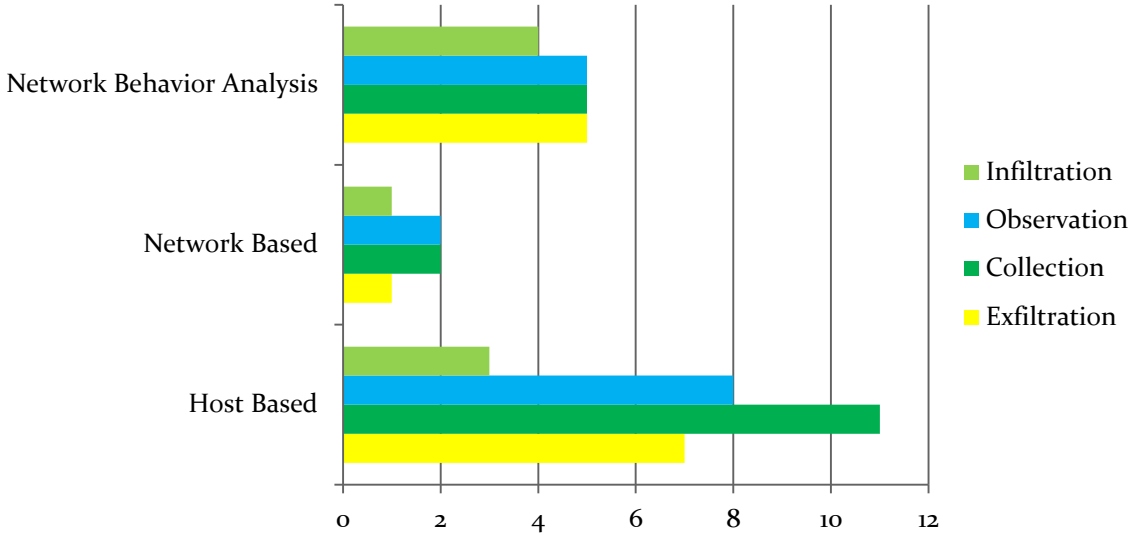


Figure 4.6 Relationship IDPS - Data Breach Phases

4.5.2. Log files

The list of indicators is known, but what is missing is a direct connection from the indicators to the actual data that is available in various log files, data bases and security warnings. The most desired implementation would be the use of a single log repository or log management (Libeau, 2008). This can be arranged by using special software that automatically collects all the log files or other relevant data from all the systems in the network. Tools like ArcSight Logger, store automatically collected events or logs in a repository. More details about such tools are available in section 6.1 about security events.

4.5.3. Intrusion Detection and Prevention Systems

The indicators have a lot of overlap with Intrusion Detection and Prevention Systems (IDPS), so they can be mapped onto each other. The indicators warn organization for possible intruders, which is the main purpose of an IDPS as well. A difference is the fact that the indicators are focused on credit card processing organizations. Four categories of IDPS exist and they are described in the NIST SP 800-94 Standard (Scarfone & Mell, 2007):

Network Based (NB); network based IDPS monitors network traffic for specific devices or segments of the network. It analyzes the protocols that are used within the different layers of the network to find suspicious activities.

Network Behavior Analysis (NA); is a type of IDPS that analyzes network traffic to identify suspicious flows of data. Malware and policy violations are examples of activities that are identified by NA.

Host Based (HB); these systems monitor the status of a single host in a network.

Wireless (W); Wireless IDPS monitors wireless traffic and analyses its protocols to identify suspicious activity. In this research, wireless IDPS are combined with network based; no separation between wireless and wired networks is made.

An example of a wireless breach is the breach of 2007 at TJX (Xu et al., 2008). It is still the second largest breach of all time as can be seen in Table 4.1. The attack started in 2005 when the attackers placed a telescope-shaped antenna towards a store to capture the wireless traffic inside the building. By doing so, the attackers could sniff (e.g. listen to the network) without being noticed. After two days of sniffing, the attackers were able to crack the WEP security of the wireless network. The credit card numbers that were sent over the wireless network were available for the attackers. Between May and December 2006, the attackers gained access to the TJX headquarters and got access to vital company and customer data that included around 90 million records that also included credit card numbers.

In October 2006, TJX noticed that something with the processing of some credit cards. An external party starts to investigate the case and found out that TJX was subject of a data breach. They discovered malicious software on their systems that was used to send the captured data to the attackers.

Table 4.6 Relation IDPS types - Data Breach Phases

Data Breach Phases / IDPS Types	Infiltration	Observation	Collection	Exfiltration
Host Based	3	8	11	7
Network Based	1	2	2	1
Network Behavior Analysis	4	5	5	5

Table 4.6 also shows the link between the indicators and the four types of IDPS. The relation between the indicators on one hand and the four data breach phases and three IDSP types on the other hand can be found in Figure 4.6. Host Based covers the most indicators compared to the types of IDPS. This makes sense since the most indicators are focused on single machines/persons. The actions a single machine or person makes are more important in the beginning of a breach (i.e. infiltration and observation) than network activity. Network based and network analysis indicators are more important when data is transferred between systems/persons.

4.6. What are attacking techniques?

When attacking organizations, three categories of attacks can be defined: external attacker, well-meaning insider and malicious insider. Security organization as well as researchers have identified these categories and corresponding activities (Symantec, 2009a).

4.6.1. External attacker

An external attacker is a person or a group of persons from outside the organization that penetrates into the internal network or bypasses security to capture sensitive data. Various vulnerabilities and/or activities are described that are based on the indicators discussed previously.

Table 4.7 Vulnerabilities External Attacker

Vulnerability	Description
System Vulnerabilities (Errors)	If systems lack the latest security patches or updates, they are exposed to any threat that focuses on a specific part of the system that is repaired with this patch. Wrong configurations of systems can also provide attackers with a point of access to the internal network.
Improper Credentials	Default passwords are known to attackers. When a new system is installed or a new account is created, the credentials must immediately be changed.
Hacking	Examples of hacking include: SQL-Injections, Buffer Overflows, Improper configurations, weak protocols, social engineering, and phishing. Websites are an often used source for gaining entrance to networks. By attacking the data base behind the website with SQL-injection, attackers can receive valuable information that puts them one step closer to their goal.
Malware	Malware is malicious software that runs on the background of a system. Without the knowledge of the user it can capture all its keystrokes or open vulnerabilities to let the attacker take over the machine or enter a specific network.

4.6.2. Well-meaning insider

Employees that neglect the security policies of an organization are a great threat to this organization. Well-meaning insiders are those insiders that do not do this on purpose. This negligence can be split up into five types (Symantec, 2009a).

Table 4.8 Vulnerabilities Well-meaning Insider

Vulnerability	Description
Data Exposed	Because of the high productivity at organizations, employees might store, send and copy sensitive information unencrypted to fasten the process. If an attacker is already present on the network (e.g. sniffing data) he can easily capture this unencrypted data that is send over the network.
Lost Laptops	Although a unsecured laptop does not directly lead to a data breach, it is an embarrassment for the organization and can

	be expensive if this laptop gets lost or stolen.
Email & Removable Disks	Unencrypted data that is sent out by email or removable disks has a high risk. Whenever this data is copied, it becomes a risk for sniffers on the network to pick up this data.
Third-party loss	If part of a payment process is outsourced, you lose control of the complete process, which can lead to a higher risk for breaches. Trust between the organization that outsources and the organization that performs the task is very important.
Automated business processes	Business processes that automatically distribute data to unprotected clients or unauthorized individuals can be captured by attackers who are on this unsecured network.

4.6.3. Malicious Insider

A malicious insider is a person who is working for an organization and willingly makes use of vulnerabilities in the organization.

Table 4.9 Vulnerabilities Malicious Insider

Vulnerability	Description
White Collar Crime	Employees who have access to sensitive data can use this data to improve a personal gain.
Terminated Employees	When an employee is fired, sometimes his account or active directory is not suspended immediately. This leaves an opportunity for the former employee to access data which he should not have access to.
Career Building	Employees can store work data on their home machines in order to build work samples for their future career. If this home computer gets stolen or hacked it has the same influence as if the organization is breached.
Industrial Espionage	Unhappy or underperforming employees who are planning to make the switch to another organization can use his confidential data to provide the new organization some benefits.

5. Empirical Research

Empirical research is used in research to validate or evaluate a statement, proposal or hypothesis that has been made. The reasons why empirical research technique is used is explained in paragraph 5.1. Paragraph 0 provides details about the interviewed subject matter experts and paragraph 0 shows the results that were gained from these interviews.

5.1. Approach

A proper and well-structured research approach is inevitable when conducting scientific or empirical research. Researchers have investigated many techniques for conducting interviews. This paragraph of the thesis elaborates on the choices that lead to the decision to select the used interview technique. It furthermore shows the interview setup with the interview approach and the desired feedback from the experts in the form of questions.

5.1.1. Background

Qualitative vs. Quantitative

A literature study alone is not sufficient enough to gain enough insight on the topic. Additional data is needed from experts in order to evaluate and discuss the research, in this case, the list of indicators and the method. This thesis will adopt a qualitative approach instead of quantitative research since it is desirable to gain in-depth data from the experts (Bryman, 1984). The number of interviewed experts is of less importance than the quality of the interviews (Bernard, 2000). Ten interviews that provide in-depth details are more valuable than twenty interviews that all stay at a high level. Also, qualitative interviews have the advantage of having the possibility to have interactive conversations over quantitative questionnaires with closed questions (Saunders, Lewis, & Thornhill, 2009). These interactive conversations are used to gain more relevant and in-depth information than can be gathered from a questionnaire.

Data collection

The empirical research approach is now narrowed to qualitative interviews, but still a decision must be made; the type of qualitative interview. Three types of interviews exist; structured, semi-structured and unstructured. Taylor & Bogdan (1998) describe in their book these three types. Table 5.1 shows a summary of the formats and benefits of every interview type.

Table 5.1 Qualitative Interview Types (Taylor & Bogdan, 1998)

Type	Format	Benefits
Structured	Each interviewee gets the same questions Little room for variation Standardized questioning No opinion of interviewer	Consistent data that can be compared across a number of respondents
Semi-structured	List of basic questions Room for variation	Questions can be prepared ahead Comparable qualitative data Freedom for interviewees
Unstructured	No structured guideline Let interviewee express themselves Little control over respondent's answers	Preliminary step toward more structured interviews

Qualitative research is often accompanied by un- or semi-structured interviews (Burnard, 1991). For this research, semi-structured interviews are used because on one hand of the basic consistency between all the interviews because of the standard questions and on the other hand of the freedom for every interviewee based on the room for variation. This variation is desirable because of the different backgrounds of the interviewees (e.g. Independent Security Experts and employees working at the transaction process of a large multinational). Fully structured interview are excluded based on the lack of variation and unstructured interviews are excluded because of their complete lack of guidance throughout the interview.

5.1.2. Interview setup

A total of eight semi-structured interviews were held with various subject matter experts. Table 5.2 shows some details about these interviews.

The interviews have a common foundation of questions that is used in every interview. For every interview it is possible to move away from the specified path in order to gain additional in-depth detail about a certain topic. A useful way of achieving this goal is the use of probes. A probe is a technique to get the interviewee to expand on a response, e.g. "Anything more?", or a period of silence (Hove & Anda, 2005).

The agenda of the interviews has the following layout:

- Introduction
- Explanation of the subject
- Understanding of the role and the environment of the interviewee
- Discuss the indicators
- Discuss the method
- conclusion

The interviews start with an introduction of the expert, the organization he/she is working for and me. My introduction also contains an introduction/explanation of the subject of this thesis. The topics of credit card transactions, PCI compliance, data breaches and data mining are briefly mentioned to provide an overall understanding. When the topic is known, the idea of the proposed method can be shared. This idea focuses on prevention vs. detection, security

events and proactive data mining techniques. After the idea of the method, the list of indicators is discussed. This is the part where the expertise and thoughts of the expert is gathered to improve this list of indicators. This improvement part consists of the following questions/determinations:

- Is the current list the final list?
- Should some indicators be removed or added?
- What are the quantifiable data types of each indicator?
- What is the correct measurement for each indicator?
- What is the impact/priority of each indicator?
- Can the indicators be grouped based on some characteristics?
- What are the boundaries or critical values of each indicator?

After the indicator discussion, the proposed method is briefly discussed.

The interviews have a timespan in the range of one hour till approximately one hour and a half.

5.2. Subject Matter Experts

Table 5.2 provides detailed information about the interviews with the subject matter- or domain-experts. This information includes a number for reference purposes, the type of organization, his or her role within this organization, the experience level, the date, the duration and the topics discussed during the interview. The list of indicators is the topic that returned in every interview.

Table 5.2 Subject Matter Expert Information

#	Organization	Role	Date	Duration	Topic
1	Dutch Consulting Organization	Director Security	31-10-2011	1:00 hour	Indicators
2	Dutch Consulting Organization	Manager Security	02-11-2011	1:00 hour	Indicators
3	Dutch Consulting Organization	Consultant Security	04-11-2011	1:30 hour	Indicators, Data Types
4	British Consulting Organization	Manager Security	21-11-2011	0:45 hour	Indicators, Data Loss Prevention
5	Canadian Consulting Organization	Manager Security	22-11-2011	0:45 hour	Indicators, Data Loss Prevention
6	Merchant	Payment Compliance Leader	25-11-2011	0:45 hour	Indicators, Payment Process, PCI DSS, Method
7	Payment Service Provider	Operation Director	02-12-2011	1:00 hour	Indicators, Data Breaches, Payment Process, Method
8	Payment Service Provider	Information Manager	05-12-2011	1:00 hour	Indicators, Data Breaches, Payment Process, Method

Summaries of each of the interviews can be found in Appendix D.

5.3. Results

The results of the evaluation of the indicators are based on eight semi-structured interviews. The summaries of the interviews can be found in Appendix D (Summaries of the interviews).

5.3.1. Evaluation of indicators

After the interviews, an updated list of indicators is constructed and is shown in Table 5.3. The names and amount of indicators has not been changed since the previous list, but the descriptions have been changed a bit. Based on the feedback from the interviews, the descriptions were too general (e.g. Improper Protocol Usage; a distinction is made between encrypted and unencrypted protocols). Other indicators were not complete in their coverage, so additional items were included (e.g. modification of data; attackers use this to wipe out their traces). The column with the types of IDPS is deleted, because it does not add any value anymore to the list. The columns that show the occurrence of the indicator in the four different phases are still there, because this still provides an overview of what indicators occurs in the first phases.

Table 5.3 Final List of Indicators

Name	Description	Breach Phase			
		I	O	C	E
Excessive logins	A specific account/workstation/server has an unexpectedly high number of login attempts or an excessive amount of logins attempts occur on random machines. If a lot of hosts are on the network, a lot of false positive because employees will surely provide some wrong passwords after all.		X		
Modification of Data	Modification of data is used by attackers to wipe their traces (e.g. deletion of temporarily created files/logs)	X	X	X	X
Automatic launch of suspicious applications on boot	Unknown applications or services are set to launch automatically during the boot process. This implies a whitelist of applications/services that should run during the boot process must be available.		X	X	X
SQL Injection Attempts	A currently implemented Intrusion Detection and Prevention System detect an SQL-Injection attempt on webservers/databases. The log files of these servers/databases contain evidence to such an attack, but once they are discovered it is already too late.	X	X		
New unexpected user accounts	New user accounts appear on the network and they are not linked to an employee. Also user accounts that exists for a short period of time, e.g. they are only used to perform a single task, fall under this indicator. User account can be created legitimately and illegitimately. Every user account must be linked to an actual employee and if this is not the case, warnings should be filed.		X	X	
Existence of suspicious files in system directory	Archived files, executables, deletion/copying/modification of data in system directories occur. This can be extended with other critical directories or even complete databases/servers. Can easily be verified using hashes of known system partitions that do not change.			X	X
Unusual Log Files	If the chronologies of log file creation changes or they contain unusual items. Has a connection with the deletion of data indicator.	X	X	X	X
Unusual high/low network activity	Systems that should have a particular network activity are suddenly offline or have an increased network activity. This indicator is highly subject to variances and has a lower importance than the others. The time where the unusual activity takes place is very important based on averages. Days should be split up in parts of an hour.	X	X	X	X
Improper account usage	User accounts are active on systems where they should not have access to.	X	X	X	
Improper protocol usage	Network traffic contains unknown protocols, or protocols that are not used in the correct way. Either because they are misused or used in the wrong place. If encrypted protocols are used (e.g. HTTPS and SSL) and the traffic needs to be analyzed, it has to be decrypted first which brings up another security issue.		X	X	
Uploading of unusual files	Malware or other files that do harm to a system are uploaded by the attackers to the targeted systems. They create ways of entrance or maintain entrance to an organization for the attackers.		X	X	X
Unusual running services	Services that are running, which are blacklisted/unknown/blocked by administrators. If such a service is detected, an immediate hash of the system must be made to check whether other suspicious activity takes place.			X	X
Registry Keys modification	Modifications in the registry to bypass security policies occur. Hashes also apply here			X	
Unknown/unexpected network connections	Unknown or blacklisted IP-addresses occur in the network or firewall logs. Also if known IP-addresses connect to servers/hosts that they should not connect to under normal circumstances indicate something is wrong.	X	X	X	X
Malware notification	Virus- or malware scanners detect suspicious files. If such a file is found, an immediate warning is signaled out. This indicator can be seen as a confirmation for the previous indicators.	X	X	X	X

5.3.2. Definition of data types/entities/boundaries

The evaluation of the indicators was the first part of the empirical research. The connection between indicators and actual data was the second part. Table 5.4 shows per indicator the corresponding data types. They are based on the interviews with the subject matter experts.

Table 5.4 Indicator Data Types

Name	Data Types
Excessive logins	System Logs
Modification of Data	System Hash
Automatic launch of suspicious applications on boot	System Logs
SQL Injection Attempts	Webserver/Database Logs
New unexpected user accounts	Identity Access Management Logs
Existence of suspicious files in system directory	System Hash
Unusual Log Files	Text Mining of logs
Unusual high/low network activity	Network Logs
Improper account usage	System Logs
Improper protocol usage	System Logs
Uploading of unusual files	Network Logs
Unusual running services	System hash/Logs
Registry Keys modification	Hash of registry
Unknown/unexpected network connections	Firewall Logs
Malware notification	Anti-Malware logs

All the relevant information from the interviews is now known and with this knowledge in mind, the method should be constructed. Before this method can be constructed, data mining as a technique has to be investigated. The next chapter starts with the investigation of data mining and how it can be used in the method and ends with the creation of the method.

Table 5.5 Data Type Descriptions

Data Type	Description
System Log	Log files generated by a system or application
System Hash	A hash file of a system or some directories of a system that is used as a reference to check for unwanted files/folders.
Webserver Log	A log from a webserver that, for example, shows activity to unknown sources or injection attempts.
Database Log	Logs from databases that stores all the actions that were performed on the database in a certain period of time.
Text Mining	
Network Log	Log files created by network equipment (e.g. routers, switches)
Registry Log	Changes in the registry can be logged. These changes can be verified using
Firewall Log	Firewall logs can show the source of an attack (IP-address) and can identify protocols that should not be available on the network.
Anti-Malware Log	Reports from periodic or automatic malware/virus scans.

6. Method

The previous chapters created a view of the transaction environment of credit cards, the anatomy of a breach and the results from interviews with subject matter experts. This chapter uses that knowledge to construct a method, which enables organizations to identify and quickly react on potential credit card breaches. The method is created in order to assist organizations in preventing data breaches by implementing a proactive data mining solution on security events. It uses data mining techniques to mine knowledge out of the indicators. Subjects that covered are: the definition of a security event, definition of data mining and corresponding techniques and frameworks and the creation of the method.

6.1. Security Events

Security events are mentioned earlier in this research and this paragraph provides a detailed description of such events. Security events are all events that can occur in an organization that effect the overall security. Examples are a possible breach of information security policies, failure of safeguards or a previously unknown situation that may be security relevant (British Standard, 2006). Security events can be observed in log files, network activity, incident tickets and deviations in resource usage (processor, memory, hard disk activity) for example. They are generated by applications, systems, users and systems (Scarfone & Mell, 2007). Examples of security events can be the successful and failed authentication attempts, security policy changes, anti-virus notifications. Basically, all the indicators that are mentioned in chapter 4.5.1 are examples of security events or can be identified by a security event and therefore can be investigated if the appropriate data is available.

Figure 6.1 and Table 6.1 shows the lifecycle of security events according to Libeau (Libeau, 2008)

Figure 6.1 Lifecycle of a security event

Table 6.1 Lifecycle of a security event description

Phase	Description
Generation	Every application, system or device generates security events. Policies should specify what information needs to be logged.
Collection	Once devices or applications are configured correctly for logging, these logs should be collected. This collection can be difficult if various systems use various types of log files.
Transport	Transportation only occurs if the collection and analysis point are separated. Transport should always be compressed, encrypted and authenticated.
Real-time Analysis	Security Event Management solutions are able to filter the enormous amount of log files that are collected to only show those entries that are of great importance (e.g. data breach indicators).

Storage	Log files can be stored in either relational databases or compressed files. Databases have the advantage of fast searches, but a large amount of processing and storage overhead. Compressed files can collect events at a higher rate, but have a low search performance.
Reporting	Reports should automatically be generated from the log files on various levels. High-level reports with only key performance indicators for the management and detailed reports for technical users or administrators.
Forensics	Forensics is the process of understanding the sequence of events leading to an incident. SEM tools can automate this process and support the forensics process.

Security events can be gathered automatically by specialized tools. Security Event Manager (SEM), also sometimes referred to as Security Information Manager (SIM) or SIEM (Security Information Event Manager) is an example of software that can automate the process of gathering security events. SEM software centralizes the collection and storage of log files or events that are generated within an organization. By doing do, all the security event notifications are gathered in a single database so they can be investigated in one place. This software is useful if an organization wants to gather all security events in a single application, but no distinction between or special attention to specific types of security events is made. For special type of security events, e.g. events with could lead to or indicate credit card breaches, special knowledge is necessary to understand what type of events are important to your organization. As mentioned before, the monitoring of security events can be done by using data mining as an addition to SEM software to gather the desired information. The method that is created in this thesis relies on the use of SEM but provide organizations with the extra knowledge of how to discover possible credit card breaches. The next paragraph provides more details about the data mining process and techniques.

6.2. Data Mining / Knowledge Discovery Process

This section describes various definitions of data mining and knowledge discovery and forms an introduction to the creation of the method in 6.3.

6.2.1. Knowledge Discovery

According to Frawley, Piatetsky-Shapiro and Matheus, Knowledge Discovery (KD) is “the nontrivial extraction of implicit, previously unknown, and potentially useful information from data” (Frawley, Piatetsky-Shapiro, & Matheus, 1992). Fayyad et al. (1996) state in their paper that knowledge discovery is “the nontrivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data”. To combine these definitions of knowledge discovery into a concrete definition that can be used in this thesis, the following will be used:

The process of identifying valuable information based on preselected data.

Preselected is used in the definition to include the data extracted from the indicators identified earlier. This data is used to generate knowledge (i.e. valuable information) that can be used to make decisions regarding the possibility of a breach.

KD is an overall process that has raw data as input and knowledge as output. This can be illustrated by a diagram of Fayyad et al. (1996) as can be seen in Figure 6.2. This figure shows the KD process with the different stages the data has on top and the actions that need to be taken to get to the new stage on the bottom. For the method that is created in the upcoming section, data mining is the most important element of the KD process. It is the bridge between the security events and the knowledge an organization has about its breach status and it is therefore highlighted in green in Figure 6.2. Above the figure are data elements that are used in the method to illustrate the KD process. More details can be found in the next section of this thesis.

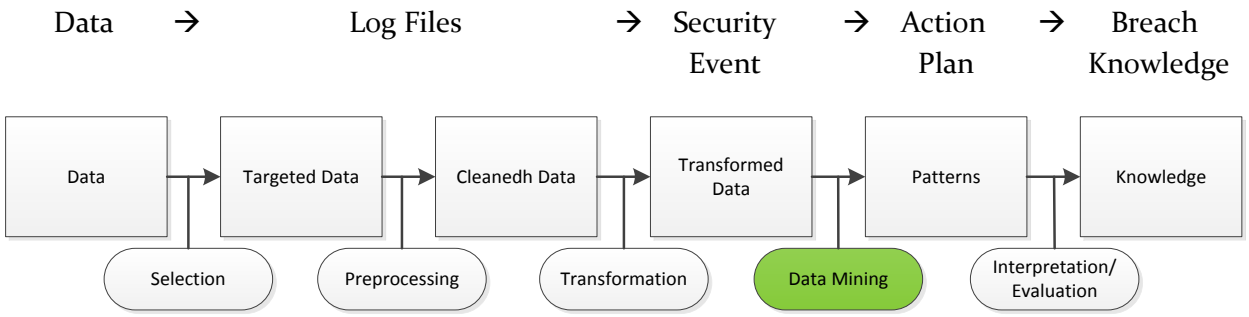


Figure 6.2 KDP (Fayyad et al., 1996)

Fayyad mentions five steps in his knowledge discovery process, which are described as follows:

1. **Selection**; a target set of data is selected or created, which can be a subset of an existing dataset. Meta-data is left out and only relevant information is used to have an appropriate amount of data to work with. The scope of the data is known and the data itself can be further processed.
2. **Preprocessing**; this step includes the removal of noise, if applicable; the collection of necessary information to model the noise and decisions on strategies for handling missing data. This is all done to ensure that the data that is being used for analysis is as clean and complete as possible so proper and valid knowledge can be extracted from it.
3. **Transformation**; this phase prepares the data so it can easily be handled by a data mining algorithm. For example, in order to have consistency in your data, all date values must have same format to sort security events by date. A security event can have the following timestamp "MM/DD/YYYY HH:MM:SS" while another security event's time stamp is "DD/MM/YYYY HH:MM:SS" or is only showing the MM/DD/YYYY so without an actual time. Transformation of data ensures that the data is consistent and can easily be read.

4. **Data mining**; this step performs the actual search in data and analyzes the data according to a predefined set of parameters. Data mining is explained in more detail in 6.2.3.
5. **Interpretation/Evaluation**; after the analysis of the data is done, the outcome needs to be interpreted or evaluated to investigate the results. The outcome of this step is the knowledge that organizations were searching for when they entered the raw data as input.

The KD process as it has been shown in Figure 6.2 is a standardized process and used in many researches. This process is not the only KD process that exists; another often used process/framework is the CRISP-DM framework.

6.2.2. Crisp-DM

The **CR**oss **I**ndustry **S**tandard **P**rocess for **D**ata **M**ining (CRISP-DM) is a standard for data mining started to develop in 1996 by DaimlerChrysler, SPSS and NCR (Larose, 2005). Version 1.0 was released in 1999. It provides a standard process for fitting data mining into the general strategy of a business unit. CRISP-DM is an iterative process and has a clear direction that leads the user through the phases. Figure 6.3 shows the six phases and the hierarchy by using arrows. The outer circle stands for the iterative nature of CRISP-DM.

The six major phases in CRISP-DM are (Chapman et al., 2000):

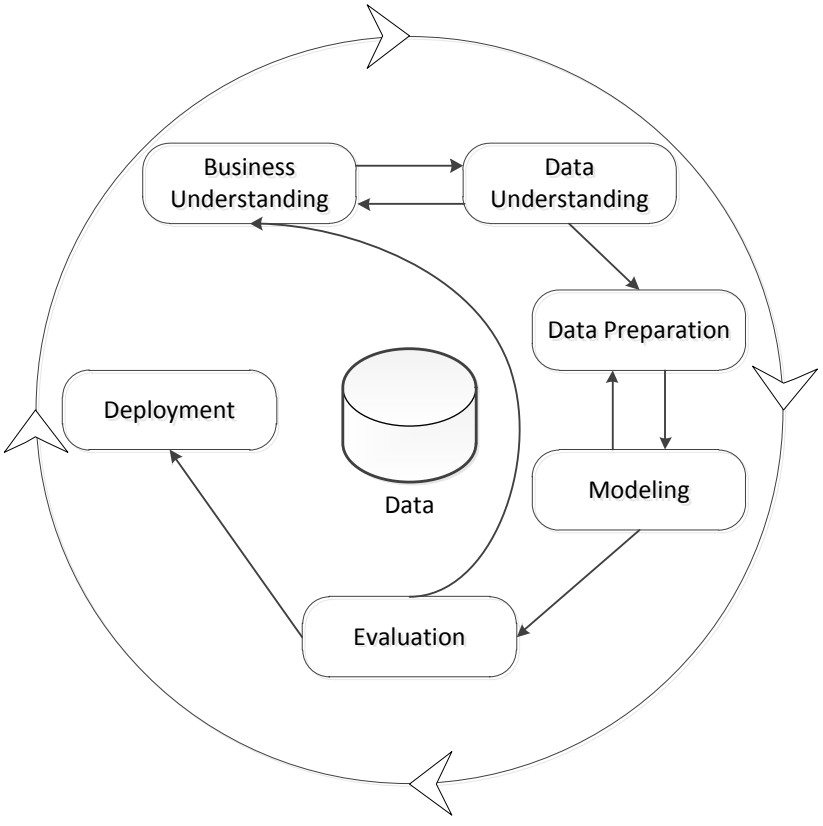


Figure 6.3 CRISP-DM Knowledge Discovery Process

- Business Understanding; understanding the project objectives and requirements from a business perspective. Converting this knowledge into a data mining problem definition and a preliminary plan designed to achieve these objectives.
- Data Understanding; Initial data collection and activities in order to get familiar with the data to identify data quality problems, discover first insights into the data or to detect interesting subsets to form hypotheses for hidden information.
- Data Preparation; all activities to construct the final dataset from the initial raw data. This include table, record and attribute selection as well as transformation and cleaning of data for modeling tools.
- Modeling; various modeling techniques are selected and applied and their parameters are calibrated to optimal values.
- Evaluation; a model is constructed, but before proceeding to the final deployment an evaluation of the model is very important. A key objective is to determine if there is some important business issue that has not been sufficiently considered.
- Deployment; the model needs to be presented in a way it is understandable by the business. The deployment phase can be as simple as generating a report till implementing a repeatable data mining process across the entire organization.

Each phase as described in Figure 6.3 consists of multiple sub phases or so called tasks, which can be seen in Figure 6.4. This thesis only point out that the tasks exists, but they are not covered in full detail in this research. For a full overview and descriptions of all the tasks, please see the CRISP-DM 1.0 step-by-step guide (Chapman et al., 2000).

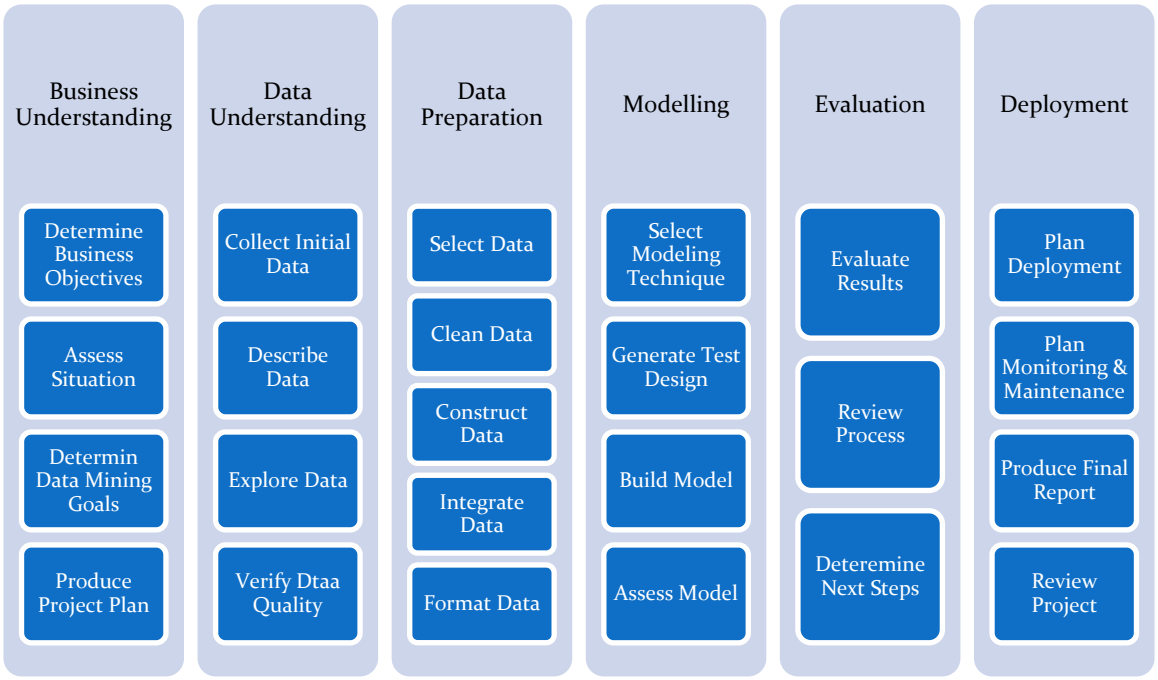


Figure 6.4 CRISP-DM Phases & Tasks

6.2.3. Comparison

How is the KD process of Fayyad et al. related to CRISP-DM? The phases designed by Fayyad et al. can be matched to the phases of the CRISP-DM model. There is a difference in the approach both processes have. Vleugel, Spruit, & van Daal (2010) describe in their paper this difference in approach of the KD process and the CRISP-DM framework. KD has a more data-driven approach; it start with selecting and understanding the data while CRISP-DM has a more business-driven approach as it starts with the understanding the business phase. Furthermore, CRISP-DM focuses on the implementation of data mining within a business unit; it ends with a deployment phase whereas KD only focusses on the data itself and ends with knowledge instead of a deployed product.

In order to get an overview of the currently used data mining approaches in organization, polls can be very helpful. These polls show for example that CRISP-DM is by far the most popular used data mining approach as can be seen in Figure 6.5 (KDnuggets, 2004, 2007). This figure shows the results of polls from 2004 and 2007 that asked what data mining framework/approach is used within an organization.. For both the polls, CRISP-DM scores over 40% while the runner up has 28% and 19% respectively in 2004 and 2007. The options were:

- CRISP-DM: the mostly used approach in the KDnuggets polls.
- SEMMA: approach designed by the SAS Institute that has five phases: Sample, Explore, Modify, Model, Assess (SAS Institute, 2012).
- My Own: I created my own data mining approach.
- My Organization's: my organization provides me a methodology that they created.
- Other: I use another approach that was not listed here.
- None: I do not use a specific data mining approach.

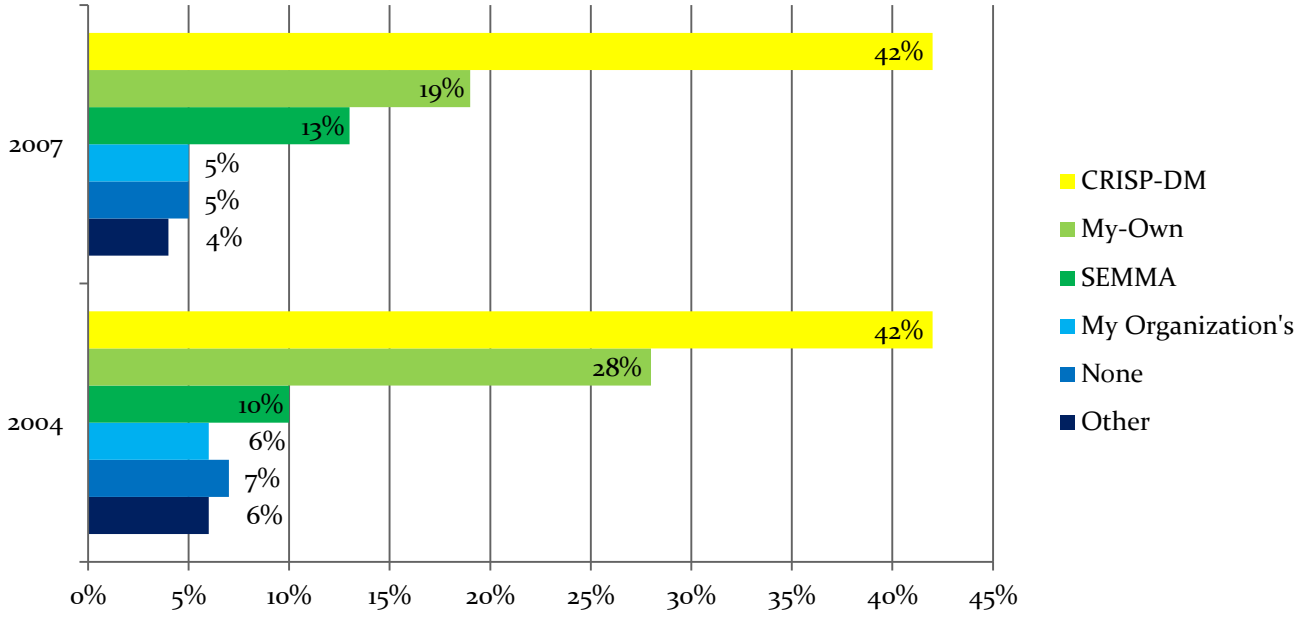


Figure 6.5 Most popular data mining methodologies according to polls (KDnuggets, 2004, 2007)

The method that is created in section 6.3 is built around CRISP-DM. It uses some parts of the approach, but also has some deviations.

6.2.4. Data Mining Techniques

Various techniques exist for extracting meaningful information out of data. This section describes the most common techniques and explains which technique(s) is/are most suitable for this research. The data mining techniques description of Larose (2005) is used to provide a summary of these techniques.

Data Warehouse: All the log files might not be at a central depository. Tools like ArcSight Logger can be used to gather all logs and security events in a single location and analyze them.

Two types of detection algorithms based on IDPS are:

- Signature Based; an incident will be detected if it relates to a previous defined pattern or signature.
- Anomaly Based; an incident will be detected if it does not relate to a baseline or standard.

The remainder of this paragraph will describe various data mining techniques and select an appropriate technique to be used by the method.

Classification

Classification is the process of assigning records in data bases to a specific categorical value; the class. For example, a person who requests a loan is either categorized as allowed or denied based

on parameters such as income, debt, age etc. Every record consists of information that assists in deciding the target class value.

Clustering

Clustering works by grouping data into clusters, according to a given similarity or distance measure. The procedure most commonly used for this consists in selecting a representative point for each cluster. Then, each new data point is classified as belonging to a given cluster according to the proximity to the corresponding representative point (Garcia-Teodoro, Diaz-Verdejo, Macia-Fernandez, & Vazquez, 2009). All the records in a cluster have similar characteristics and are dissimilar with records that are not in the cluster. Clustering does not want to predict class records, such as classification, but to divide the data in groups. The similarity is maximized, while the dissimilarity is minimized.

Some points may not belong to any cluster; these are named outliers and represent the anomalies in the detection process. Clustering and outliers are used at present in the field of Intrusion Detection System (IDS) with several variants depending on how the question: is the isolated outlier an anomaly is answered. For example, the KNN (k-nearest neighbor) approach uses the Euclidean distance to define the membership of data points to a certain cluster. Some detection proposals associate a certain degree of being an outlier for each point. Clustering techniques determine the occurrence of intrusion events only from the data available in log files, therefore the currently installed IDS must be tuned to meet desired specifications.

Regression

Regression is a prediction technique, where the outcome of a value is predicted based on some input variables.

Association Rules

"The task of association seeks to uncover rules for quantifying the relationship between two or more attributes"(Larose, 2005). They have the form "*if* ANTECEDENT *then* CONSEQUENT". A well-known example is the shopping pattern of customers in a supermarket. Research showed that from the 1000 customer, 200 bought diapers and from those 200, 50 also bought beer (Larose, 2005).

Summarization

"Summarization is the process of finding a compact description for a subset of data" (Fayyad et al., 1996). Calculating the mean and standard deviation are examples of summarization. Summarization techniques are often used for automated report generation.

Anomaly detection

Anomaly, or outlier detection, is the process of finding objects that differ from most other objects. A graphical representation will be a scatter plot where the outliers lie far away from the other data points, as can be seen in Figure 6.6; a simplistic figure with red (outliers) and blue points (the normal ones).

Anomaly detection is often used in automated intrusion detection. Anomaly detection builds models of normal data and can detect deviations in observed data (Lazarevic, Ertoz, Kumar, Ozgur, & Srivastava, 2003). In their same study, Lazarevic et al. (2003) investigate which technique is most suitable to use for anomaly mining in intrusion detection systems.

They experiment with the following techniques:

- K-nearest neighbor; computing the Euclidean distance of the K-nearest neighbor from a certain point. The distances to the k-nearest neighbor of a data point must be greater than a threshold to mark that data point as an outlier.
- Nearest neighbor; the same as k-nearest neighbor, but with K = 1. The distance to the closest nearest neighbor of a data point must be greater than a threshold to mark that data point as an outlier.
- Mahalnobis distance; calculates the mean and the standard deviation of the "normal" situation. Points in data that have a greater distance to the mean of this situation are considered outliers.
- Density based local outliers (LOF); assigns to every data point a degree of being an outlier.
- Unsupported vector machines; tries to find a small region where most of the data is located and it labels data points in this region as normal. Data points in other regions are marked as outlier.

Frequent episodes

A frequent episode is a set of events that occur frequently within a time window (of a specified length). The events must occur together in at least a specified minimum frequency (Lee & Stolfo, 1998).

Table 6.2 shows an overview of the data mining techniques explained above and list the sources in table 6.3.

Table 6.2 Data Mining Techniques

	1	2	3	4	5	6	7	8
Classification	X		X				X	
Clustering	X				X		X	
Regression	X						X	
Association Rules	X	X						
Summarization							X	
Anomaly Detection	X	X	X	X	X	X		X
Frequent episodes		X						
Neural Networks	X							

Table 6.3 Data Mining Techniques References

Number	Reference
1	(Larose, 2005)
2	(Lee & Stolfo, 1998)
3	(Lee, Stolfo, & Mok, 1999)
4	(Lee et al., 2001)
5	(Garcia-Teodoro et al., 2009)
6	(Sequeira & Zaki, 2002)
7	(Fayyad et al., 1996)
8	(Lazarevic et al., 2003)

Table 6.2 and 6.2 show what researcher cover which data mining technique. These are used to make an analysis of which technique is most suitable for preventing credit card breaches.

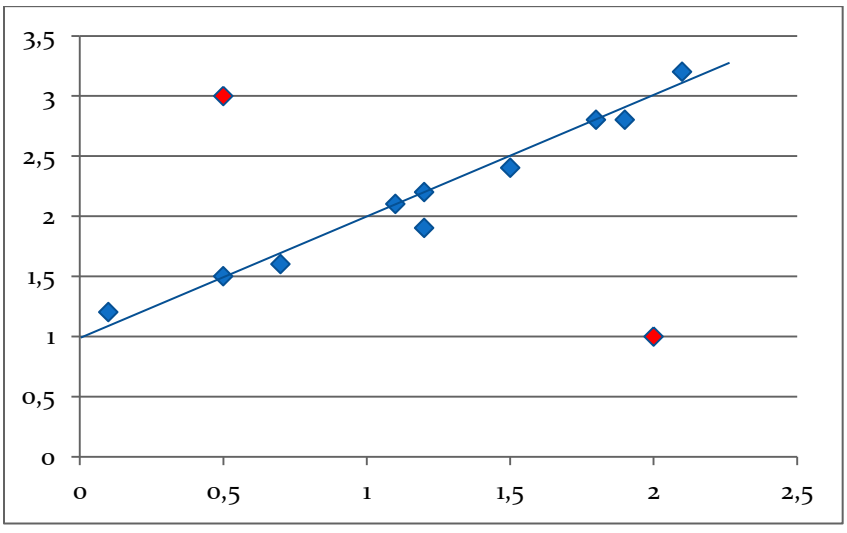


Figure 6.6 Anomaly Detection

Based on the previous mentioned techniques, anomaly detection is the most suitable technique for this research. There is no prediction or classification involved, nor is the relation between

attributes of high importance (association rules). Data in log files that is different from a normal situation, i.e. anomalies, is interesting to investigate. The data breach indicators all have a "normal" situation and if they deviate too much from this situation, i.e. the threshold has been reached; a warning or notification can be reported back by the data mining technique.

The LOF technique used in anomaly detection is proven to be most effective on a training set (Lazarevic et al., 2003). LOF consists of the following 4 steps:

1. For each data point (a), the k-nearest neighbor and k-nearest neighborhood is calculated
2. For each data point (a), the reachability distance is calculated with respect to another data point (b) by the following formula:

$$reachabilitydistance\ (a, b) = \max\{kdistance(b), distance(a, b)\}$$

3. For each data point (a), the local reachability density is calculated as an inverse of the average reachability distance based on the nearest neighbor of the minimum number of data points.
4. Finally, the LOF is calculated for each data point (a) by averaging the ratios of the local reachability density of (a) and the local reachability density of the nearest neighbor of the minimum number of data points.

For a detailed description of the LOF algorithm, please refer to the paper of Breunig, Kriegel, Ng, & Sander (2000).

6.3. Method

This paragraph contains the actual method that prevents a breach. What does the transformation from security events to a classification looks like?

Before proceeding to the method steps, a good understanding of the risks must be present in every organization. This consists of two phases according to Symantec, a large security specialized organization. (2009a):

- identify the types of information you want to protect and where it is exposed in the organization. In this case it is the valuable credit card information. In order to protect this information from being captured, organizations must be aware of the storage location of this information. Not only do they need to know the physical storage of the information, but also when this information is being transferred from one system or storage location to another.
- Assess the network and understand what areas are vulnerable to external attacks. By performing periodic analysis of the organizational network and systems (e.g. vulnerability assessments by an independent party) organizations can identify possible weaknesses in their infrastructure and systems that could lead to compromises of systems or data.

6.3.1. Demands of data breach preventing methods

A large security organization has defined six steps to prevent a data breach (Symantec, 2009b). A method that will assist organizations in preventing a breach must cover at least these six points:

1. Stop incursion by targeted attacks; the entrances to an organization must be blocked to make it as hard as possible for intruders to find a way of breaching the security mechanisms. The whole purpose of the method is to stop this incursion by targeted attacks and detect them as soon as possible.
2. Identify threats by correlating real-time alerts with global security intelligence; real-time alerts are necessary in order to detect an attack before it does too much damage. These real-time alerts are part of the security events mentioned earlier in this research.
3. Proactively protect information; Information must be protected at the source and not only at the perimeter. By using pro-active data mining on the log files and security events of security suites, the stored information in an organization is protected in real-time.
4. Automate security through IT compliance controls; the effectiveness of the procedural and technical controls must assessed regulatory and automatic checks on technical controls, such as firewall configurations and password settings will reduce the risk of exposing sensitive data. This check and control is exactly what this method does.
5. Prevent data exfiltration; this step focuses on the situation when attackers manage to gain access to the internal network. The exfiltration of data must be blocked. If an attack is detected in a very early stage, e.g. the infiltration or observation phase, and also blocked in this stage, the possibility of data exfiltration is kept to a minimum.

6. Integrate prevention and response strategies into security operations; a breach prevention and response plan is necessary in order to prevent breaches. The method is such an ongoing process and should be implemented into overall security operations for it to be effective.

6.3.2. Method Steps

The demands and background of the method are now known. This paragraph introduces the proposed method and elaborates on the various steps it contains. The most important input for the method is the list with indicators. They limit the scope for organizations and provide, together with the analysis of data mining techniques in this research, a good foundation for preventing data breaches in the future.

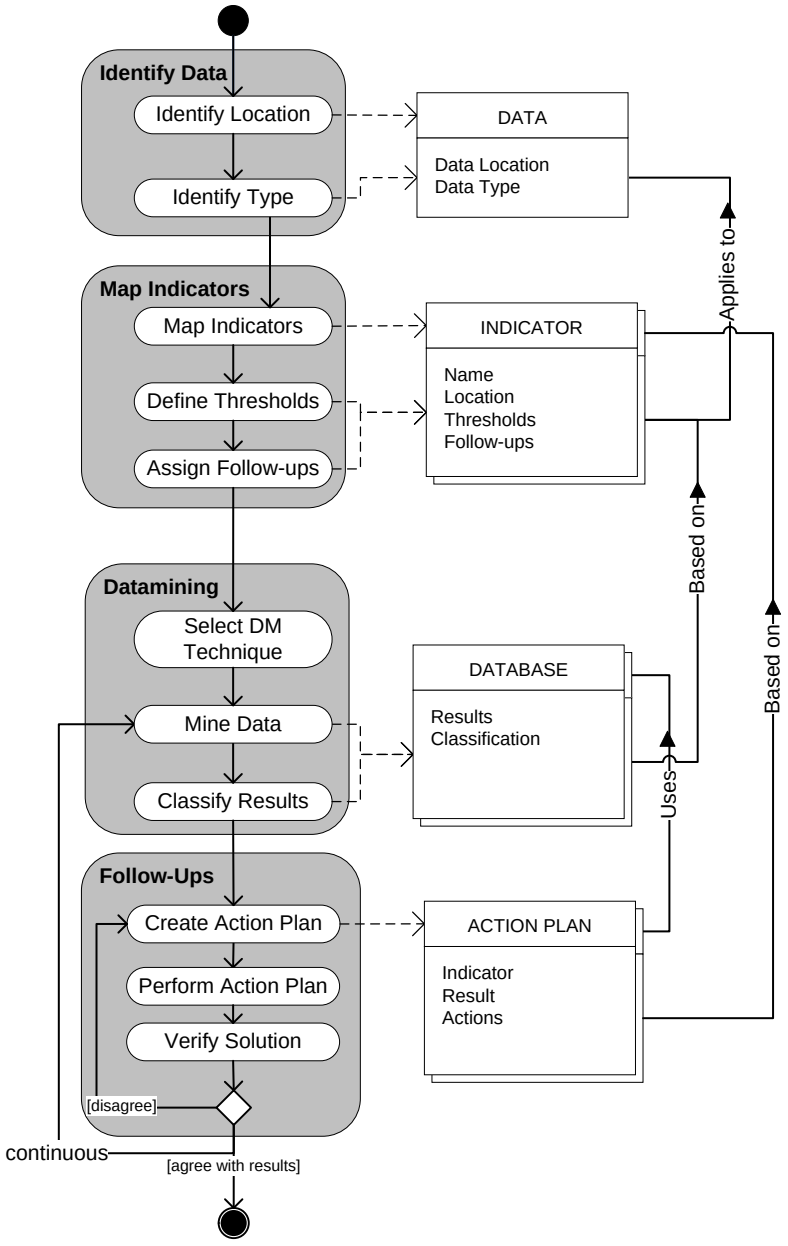


Figure 6.7 Proposed Method

Figure 6.7 shows the method by using the PDD (Process-Data Diagram) notation by van de Weerd & Brinkkemper (2008). Table 6.4 and Table 6.5 provide the corresponding Activity Table and Table of Concepts.

The method is divided into4 main activities in order to cover the requirements as mentioned before:

- Identify Data
- Map Indicators
- Data Mining
- Follow-ups

These four steps follow the logical principle of analysis → action → reaction. The analysis phase consists of the identification of data and the mapping of the indicators. The action phase is the actual data mining. The reaction phase is the analysis of the results together with the performing of the follow-up activities.

The next paragraphs provide a detailed description of these main activities. The following tables cover all the sub-activities and concepts designed in Figure 6.3 and are part of the PDD notation.

Table 6.4 Activity Table

Activity	Sub activity	Description
Identify Data	Identify Location	Identify the location of the data (data refers to security event data in the remainder of this thesis). This can be separated throughout the entire organization, or gathered in a single logger program.
	Identify Type	What is the type of the data? This information is needed to correctly assign it to the corresponding indicator.
Map Indicators	Map indicators	Map the indicators onto the found data based on the type and location of the data.
	Define Threshold	Thresholds for every indicator should be constructed to define the critical boundaries. A normal, improved attention and critical situation should be defined.
	Assign Follow-up	Follow-ups must be selected for every level of every indicator.
Data mining	Select DM Technique	In order to mine data correctly, the appropriate data mining technique must be selected first. This thesis suggests using anomaly detection to only focus on the abnormal behavior of security events. Of course, organizations are able to select a data mining technique of their preferences.
	Mine Data	Once the data and indicators are known, the correct data can be mined and the results stored. This mining consists of an import of data, running the data mining tool or program that contains the mining logic and predefined thresholds, parameters and other settings. The last part of this step is the export of the results of the mining.

	Classify Results	The results of the data mining step are analyzed using the thresholds to define the risk per indicator.
Follow-Ups	Create Action Plan	An action plan, that contains what follow-ups to perform must be created based on the results from the classification phase. Appropriate follow-ups must be selected or customized based on the impact of each classification. The follow-ups must mitigate the risk of a breach for organizations.
	Perform Action Plan	After the action plan has been created and has the proper approvals, the follow-ups must be performed by following the action plan.
	Verify Solution	After the actions have been performed, an analysis, basically going through the process once more for the indicators in scope, is needed to see if the actions had the desired effect, i.e. lowering the value of the indicator so that is becomes lower than the threshold. This means the risk is mitigated for this specific indicator. This does not mean the risk of a breach is completely solved. The additional run will determine if the follow-ups were sufficient enough.

The final line in the figure that goes back to the mine data phase represents the continuous process of the method. The first 2 steps are not continuous but should be performed on a regular basis.

Table 6.5 Table of Concepts

Concept	Description
DATA	The DATA concept consists of the location of the data and the type of the data. It represents the log files and security events that exist within the organization. By having this concept, organizations are aware of the location of their valuable data, both stored and in transfer.
INDICATOR	The INDICATOR concept is a list of indicators that are applicable on the available data within an organization. Information that is stored in this concept is: - The name of the indicator - The location where the indicator can be mined (based on the DATA concept). - Predefined thresholds that specify the various severity levels the indicator can reach, e.g. low, medium and high. Per level is defined when this level is reached. - - per severity level, appropriate follow-ups are specified. They clearly state what actions should be performed when this level is reached for this indicator.
DATABASE	The DATABASE concept contains the results of the data mining phase (based on the indicators). After the thresholds have been run over the mined data, a CLASSIFICATION RESULT is generated that contain the risk per indicator.
ACTION PLAN	An ACTION PLAN consists of the corresponding indicator and results of the data mining phase together with the selected follow-ups that need to be taken and the corresponding classification level of the indicator.

For a detailed description of the sub activities, please refer to Table 6.4.

6.3.2.1. Identify Data

The first step is to become familiar with the sensitive data that is transferred, transmitted or stored in an organization. In order to protect the data, an organization must know where it is located. Not only the location, but also the type of data and the owner must be documented.

6.3.2.2. Map Indicators

The second step covers the translation step from the list of indicators defined previously to the actual data (i.e. security events logging). The following steps need to be done for each indicator:

- Map it to data files
- Define thresholds
- Select or change appropriate follow-up

This step is the final step of the initial phase and only needs to be performed once in the beginning. These two steps need to be performed if systems changed or adjustments are made to the security policies in an organization.

6.3.2.3. Data Mining

The fourth step is where the actual mining of data takes place. A technique is selected to gather the required data. Anomaly detection is a good technique to use as mentioned earlier in this chapter, but organizations are able to use any technique they prefer. For example, an organization can have created a new technique that focusses especially on the structure of their organization. The data that is output of the data mining phase needs to be classified and interpreted to create appropriate follow-up actions in the next step.

6.3.2.4. Follow-ups

The final step covers the actions that need to be taken to solve the issues defined in the previous step. A plan is created to solve the issue and after it is performed, various actions are needed to validate if the actions were sufficient to solve the issue. If not, a new action must be created, or the old action needs adjustments in order to solve the issue.

Once all steps were followed in the method, organizations return to step 2 and perform the data mining and follow-up steps again on a regular basis.

Vulnerability Management addition

Vulnerability management should be performed by organizations as well to make sure they have a secure foundation. With a proper security, a breach is much less likely to occur than at organizations that have multiple security flaws.

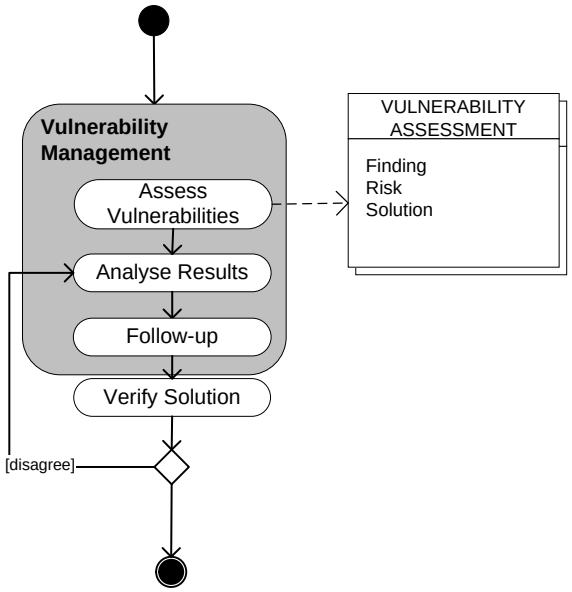


Figure 6.8 Proposed Method

The figure above (6.8) shows the steps organizations must perform for their vulnerability assessment. Table 6.6 and 6.7 describe the activities and concepts introduced.

Table 6.6 Activity Table Vulnerability Management

Activity	Sub-activity	Description
Vulnerability Management	Assess Vulnerabilities	An independent party must perform a periodical vulnerability assessment to identify risks in an organization's infrastructure and systems.
	Analyze Results	The result of the assessment, the report, must be analyzed to understand the findings presented in it.
	Follow-up	If everything is understood from the report, appropriate follow-ups must be selected and implemented.
	Verify Solution	After the follow-ups have been implemented, an analysis must be performed to check whether the follow-ups were successfully implemented. This can be done by performing another vulnerability assessment on the complete infrastructure/system or focusing only on the objects that changed.

Table 6.7 Table of Concepts Vulnerability Management

Concept	Description
VULNERABILITY REPORT	The VULNERABILITY REPORT is generated by the independent party that performed the vulnerability assessment. The report contains the following information: - The name of the system/application/infrastructure that has been assessed.

- A finding is an observation in a system/application/infrastructure that contains a (possible) weakness and/or risk to the organization.
- The risk that is associated with the finding states the impact and likelihood of the misuse of the found vulnerability. Normally this is scaled between low, medium and high. Critical can be used for extremely important findings.
- Per finding, a solution is given

6.3.3. CRISP-DM Framework

The method consists of four main steps: Identify Data, Map Indicators, Data mining and Follow-Ups. These steps are mapped onto the CRISP-DM framework to ensure a proven framework. Figure 6.9 shows the mapping of the method onto the CRISP-DM framework. The 4 steps that are mentioned in the method are chosen instead of the standard CRISP-DM steps, because they are more specific for this type of investigation.

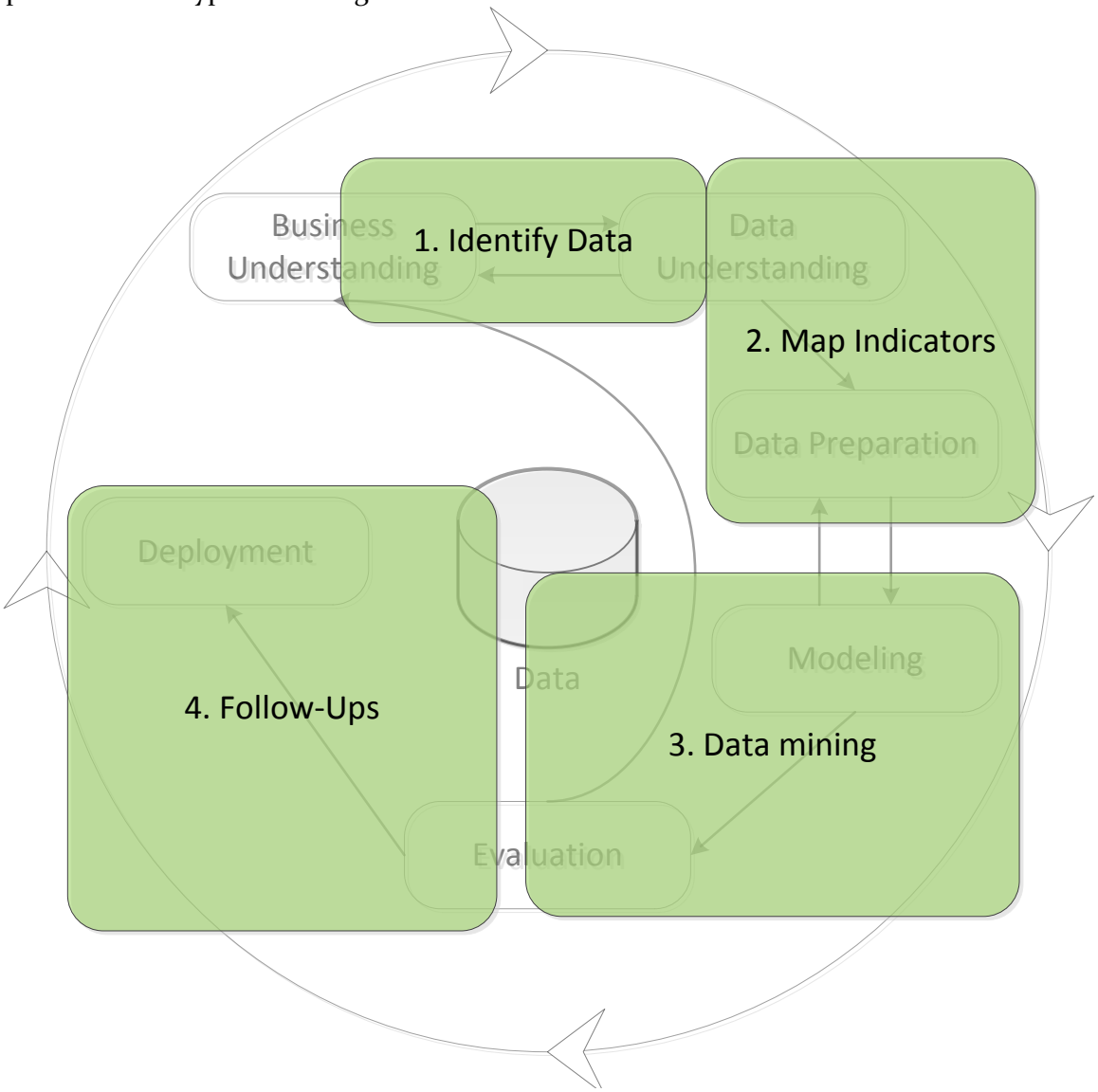


Figure 6.9 The proposed method mapped onto the CRISP-DM framework

The identification of data phase overlaps partly with business understanding and data understanding. It is more about data understanding (e.g. now the location of the data) than about the business understanding. The business understanding should be taken care of before proceeding with the method. The mapping of indicators is over the data understanding phase and data preparation phase as it is selecting proper data files for the mining phase. The mining phase is more or less equal to the modeling phase as it gathers the relevant information out of the rough data. The classification of the mined results has similarities with the evaluation phase as the results are analyzed. The follow-ups can be seen as the deployment of the method, where actions are performed. A part of this phase has similarities with the evaluation phase.

6.3.4. Conclusion

With this method, organizations can discover indicators of a data breach by mining security events. The proper techniques to gather these log files should be implemented, whether by an existing tool or a tailor-made application. The tools described before and mentioned in the interviews are all good examples of tools that can be used for log management.

The data collection is one step, but the classification of this data is another important step of the method. A correct classification should be chosen based on organization specific characteristics. With these classifications in mind, proper follow-ups should be developed to act correctly if an indicator reaches a certain threshold.

The guidelines proposed in the method will aid organizations in setting up a secure environment and detecting credit card breaches in early phases because of the regularity and specific focus of the monitoring on indicators.

7. Method Evaluation

The method that assists organizations in preventing credit card breaches is now introduced. This chapter explains the steps that were taken to evaluate it and what the results of this evaluation were.

7.1. Approach

An approved way for evaluating this method is conducting interviews with subject matter experts. During the interviews, a draft version of the method was shown to the interviewees and a discussion was started on what should be included in the method and what is the best way to tackle the problem of preventing data breaches.

7.2. Evaluation

The outcome of the interviews is shown in this section. For a summary of all the interviews, please refer to Appendix D.

SME	Comments	Follow-ups
1	Organizations really need to know what is the sensitive data in your organization and where is it stored and who has access to it.	Follow-up actions should be of the form: • do nothing • send e-mail to person in charge • block traffic of certain systems
2	Try neural networks to identify normal and abnormal behavior.	n/a
3	If a possible breach is suspected based on some indicators, data mining analysis is performed on the log files to find more evidence of the breach. Monitoring should not be done constantly because it will generate a lot of overhead on systems.	n/a
4	The most important task of this method should be the correct correlation of log files and to extract the useful data out of the immense amount of log data.	n/a
5	n/a	-workstations can easily be isolated from the network if risks are identified on them. - a hash of critical system files/folders must be made at least once a day to detect suspicious services and/or uploaded files.

The table above shows the outcome of the evaluation. Per interview (number) is mentioned what the comments were on the method and what they would think appropriate follow-ups should be like. This latter is hard to accomplish because it is different for every organization and therefore left out of scope. The comments include items that should be part of the method, which were included in the final version.

7.3. Improvements

No real validation of the method is in place. For proper use of this method it needs to be tested during a real-life case. Unfortunately this was not possible during the performance of this research and is therefore marked as future work. This version of the method includes all the comments made by the subject matter experts during the interviews. The real-life case as a validation will test the method by implementing it at an organization. The results of the validation can be used as input for improvement. The focus on the validation must lie on step 4 (i.e. data mining). The other steps are known or proven activities, such as vulnerability management and identifying the location and identity of the sensitive data.

8. Conclusion

This thesis presented the research that was conducted to provide the answer to the research question that was stated in Chapter 2 This chapter provides the conclusions that can be drawn from the conducted research.

The sub research questions were:

1. What does the environment in which a credit card transaction takes place looks like and what are the critical points?
2. What is a data breach and how is it constructed?
3. What are indicators of a data breach?
4. What are available security events/logs?
5. What data mining techniques are suitable for the indicators?

The conclusions of the sub research questions are:

1. Chapter 3 described the full environment of a credit card transaction and PCI DSS to make this environment more secure. It provided the necessary background of credit cards to understand the upcoming chapters.
2. Chapter 4 covered the breach part of the research. It described what a breach is, what the risks are, showed the four phases of a breach and made the initial list of indicators of a breach.
3. The final part of chapter 4 focused on the indicators of a breach. Based on literature and interviews with subject matter experts, a final list of indicators was created in Chapter 5
4. Security event and logs were discussed in chapter 6 of this thesis. A definition of security event and log management tools was given.
5. Data mining was the final topic of this research and was mentioned in chapter 6. A suitable technique for security event mining was found and a method that uses this technique was created.

The main research question of this research was: How can proactive data mining of security events help prevent data breaches of credit card data in a PCI DSS compliant environment?

The five sub questions together provide an answer to this main question and together with the responses from the interview they form the conclusion of this research. Various tools exist that manage log files generated throughout an entire organization. These are general tools and do not focus on specific client needs. This research sketched the complete credit card environment of an organization and provided a method to implement security measures. It cannot be stated that credit card breaches can be prevented in the future, because new techniques always emerge and prevention tools must always act upon these changes. The increase in security awareness that this method provides gives organizations an advantage regarding the prevention of breaches, because they now know the points that requires special attention (i.e. the indicators).

9. Limitations & Further Research

Based on the information provided in this research, a few limitations and room for future research can be identified. First of all, the research focused solely on credit card breaches. While the research provided a complete background the credit card world, it is desired to investigate whether it is possible if other sensitive data (e.g. Name, addresses and electronic patient records) are also applicable for these indicators. It is quite possible that the same indicators can be used, because they turn out to be highly general intrusion indicators.

Second, the effects the method has and the possible increase in awareness for organizations has not been evaluated yet, because of the lack of time. The method has been evaluated to check whether everything that should be included is also included in it.

Third, the follow-ups that should be taken after an indicator reaches a certain level are not defined in this research, because they are too specific for an organization. The same holds for the thresholds of the indicators. Future research can focus solely on this point and try to determine proper follow-ups and thresholds for different types of organizations.

10. References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study. *Twenty Seventh International Conference on Information Systems*. Milwaukee.

AFP. (2011). Bank card numbers stolen in PlayStation breach: Sony. Retrieved from http://www.vir.com.vn/news/business/corporate/bank-card-numbers-stolen-in-playstation-breach-sony.html

Aldridge, J. (2010). *Breach Indicators*. Retrieved from https://isaca-washdc.sharepointsite.net/webresources/Presentations/Conference-April2010-Session1.pdf

Bernard, H. R. (2000). Introduction to Qualitative and Quantitative Analysis. *Social research methods: qualitative and quantitative approaches* (pp. 417–436). Thousand Oaks, CA: Sage Publication, Inc.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602–613.

Breunig, M. M., Kriegel, H., Ng, R. T., & Sander, J. (2000). LOF : Identifying Density-Based Local Outliers. *Proceedings of the ACM SIGMOD conference 2000* (pp. 93–104).

British Standard. (2006). *Information security management systems – Part 3: Guidelines for information security risk management*. Retrieved from http://iso.staratel.com/ISO17799/Doc/BS7799.3.1999/BS 7799-3-2006.pdf

Bryman, A. (1984). The debate about quantitative a question of method qualitative research : or epistemology ? *British Journal of Sociology*, *35*(1), 75–92.

Burnard, P. (1991). A method of analysing interview transcripts in qualitative research. *Nurse Education Today*, *11*(6), 461–466.

Cahill, M. H., Lambert, D., Pinheiro, J. C., & Sun, D. X. (2004). Detecting fraud in the real world. *Computing Reviews*, *45*(7), 913–930.

Chapman, P., Clinton, J., Kerber, R., Khabaza, T., Reinartz, T., Shearer, C., & Wirth, R. (2000). *CRISP-DM 1.0 Step-by-step data mining guide*. CRISP-DM Consortium. Retrieved from http://www.spss.ch/upload/1107356429_CrispDM1.0.pdf

Cheney, J. S. (2010). *Heartland Payment Systems: Lessons Learned from a Data Breach*. Philadelphia: Federal Reserve Bank of Philadelphia.

Chuvakin, A. A., & Williams, B. R. (2010). *PCI Compliance*. (W. Spangenberg, Ed.) (2nd ed.). Waltham, MA: Syngress Publishing, Inc.

Cisco. (2011). What Is the Difference: Viruses, Worms, Trojans, and Bots? Retrieved October 28, 2011, from http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

CreditCards.com. (2009). *How a credit card is processed*. Retrieved from http://www.creditcards.com/credit-card-news/assets/HowACreditCardIsProcessed.pdf

DatalossDB. (2012a). Dataloss DB Latest Incidents. Retrieved March 16, 2012, from http://datalossdb.org/index/latest

DatalossDB. (2012b). Dataloss DB Largest Incidents. Retrieved March 16, 2012, from http://datalossdb.org/index/largest

Debreceny, R. S., & Gray, G. L. (2010). Data mining journal entries for fraud detection: An exploratory study. *International Journal of Accounting Information Systems*, *11*(3), 157–181.

Evans, D. S., & Schmalensee, R. (2005). *Paying with plastic: the digital revolution in buying and borrowing* (2nd ed., pp. 9–10). Cambridge: Massachusetts Institute of Technology.

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From Data Mining to Knowledge Discovery in Databases. *AI Magazine*, *17*(3), 37–54.

Frawley, W. J., Piatetsky-Shapiro, G., & Matheus, C. J. (1992). Knowledge Discovery in Databases : An Overview. *AI Magazine*, *13*(3), 57–70.

Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., & Vazquez, E. (2009). Anomaly-based network intrusion detection : Techniques , systems and challenges. *Journal of Computers and Security*, *28*, 18–28. doi:10.1016/j.cose.2008.08.003

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

Hove, S. E., & Anda, B. (2005). Experiences from Conducting Semi-Structured Interviews in Empirical Software Engineering Research. *11th IEEE International Software Metrics Symposium (METRICS'05)* (p. 23). Como, Italy.

ISO/IEC. (2006). *ISO/IEC 7812 identification cards — identification of issuers — Part 1: Numbering system*. Retrieved from www.iso.org

KDnuggets. (2004). Poll: Data Mining Methodology (Apr 2004). Retrieved December 1, 2011, from http://www.kdnuggets.com/polls/2004/data_mining_methodology.htm

KDnuggets. (2007). Poll: Data Mining Methodology (Aug 2007). Retrieved December 1, 2011, from http://www.kdnuggets.com/polls/2007/data_mining_methodology.htm

Larose, D. T. (2005). Discovering Knowledge in Data.

Lazarevic, A., Ertoz, L., Kumar, V., Ozgur, A., & Srivastava, J. (2003). *A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection*. Minnesota.

Lee, W., & Stolfo, S. J. (1998). Data Mining Approaches for Intrusion Detection. *Proceedings of the 7th USENIX Security Symposium*. San Antonio, TX.

Lee, W., Stolfo, S. J., Chan, P. K., Eskin, E., Fan, W., Miller, M., Hershkop, S., et al. (2001). Real Time Data Mining-based Intrusion Detection. *Proceedings of the 2001 DARPA Information Survivability Conference and Exposition (DISCEX II)*. Anaheim, CA.

Lee, W., Stolfo, S. J., & Mok, K. W. (1999). A Data Mining Framework for Adaptive Intrusion. *Proceedings of the 1999 IEEE Symposium on Security & Privacy*. New York, NY.

Li, C., & Yao, Z. (2011). The Validation of Credit Card Number on the Wired and Wireless Internet. *Journal of Networks*, *6*(3), 432–437.

Libeau, F. (2008). Automating security events management. *Network Security*, *2008*(12), 6–9.

Luong, V. (2010). *Intrusion Detection And Prevention System : SQL- Injection Attacks. Prevention*. San Jose State University.

MasterCard Worldwide. (2003). Site Data Protection and PCI. Retrieved April 19, 2011, from http://www.mastercard.com/sdp

McMillan, R. (2011). Sony cuts off Sony Online Entertainment service after hack. *Network World*. Retrieved May 6, 2011, from http://www.networkworld.com/news/2011/050311-sony-cuts-off-sony-online.html

Montague, D. A. (2004). *Fraud Prevention Techniques for Credit Card Fraud*. Victoria: Trafford Publishing.

Montoro, M. (2005). Remote Desktop Protocol , the Good the Bad and the Ugly. Retrieved June 20, 2012, from http://www.oxid.it/downloads/rdp-gbu.pdf

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559–569. doi:10.1016/j.dss.2010.08.006

Nystrom, M. G. (2007). *SQL Injection Defenses*. *Information Security*. Sebastopol, CA: O'Reilly Media, Inc.

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems.

Proceedings of the 5th conference on Information technology education - CITC5 '04 (p. 177). New York, New York, USA: ACM Press. doi:10.1145/1029533.1029577

Padilla, L. (2002). Track format of magnetic stripe cards. *GAE UMC*. Retrieved July 18, 2011, from http://www.gae.ucm.es/~padilla/extrawork/tracks.html

PCI Security Standards Council. (2010a). About Us. *PCI Security Standards*. Retrieved from https://www.pcisecuritystandards.org/organization_info/index.php

PCI Security Standards Council. (2010b). *PCI DSS Quick Reference Guide*. Retrieved from https://www.pcisecuritystandards.org/documents/PCI SSC Quick Reference Guide.pdf

PCI Security Standards Council. (2010c). PCI SSC Data Security Standards Overview. Retrieved May 24, 2011, from https://www.pcisecuritystandards.org/security_standards/index.php

PCI Security Standards Council. (2010d). Payment Card Industry Data Security Standard version 2.0; Requirements and Security Assessment Procedures. Retrieved from https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

PCI Security Standards Council. (2010e). *Self-Assessment Questionnaire - Instructions and Guidelines*. Retrieved from https://www.pcisecuritystandards.org/documents/pci_dss_saq_instr_guide_v2.0.pdf

PCI Security Standards Council. (2010f). *Payment Application Data Security Standard version 2.0; Requirements and Security Assessment Procedures*. Retrieved from https://www.pcisecuritystandards.org/documents/pa-dss_v2.pdf

PCI Security Standards Council. (2011). *Information Supplement : PCI DSS Tokenization Guidelines*. *Security*. Retrieved from https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

Percoco, N. J. (2010). Data Exfiltration : How Data Gets Out. Retrieved September 18, 2011, from http://www.csoonline.com/article/570813/data-exfiltration-how-data-gets-out

Peretti, K. K. (2008). Data Breaches: What the Underground World of Carding Reveals. *Santa Clara Computer and High Technology Journal*, *25*(2), 375–413.

PricewaterhouseCoopers LLP. (2009). *Safeguard your sensitive data*. Retrieved from http://www.pwc.com/us/en/it-risk-security/assets/safeguard_your_sensitive_data.pdf

Pritchard, S. (2011). The Rise and Fall of Online Credit Fraud. *Infosecurity*, *8*(2), 24–27.

SAS Institute. (2012). SAS Enterprise Miner. Retrieved June 22, 2012, from http://www.sas.com/offices/europe/uk/technologies/analytics/datamining/miner/semma.html

Saunders, M., Lewis, P., & Thornhill, A. (2009). Collecting Primary Data Using Semi-Structured and In-Depth Interviews. *Research Methods for Business Students* (fifth., pp. 318–357). Essex: Pearson Education Limited.

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. *Nist Special Publication*. Gaithersburg, MD.

Sequeira, K. D., & Zaki, M. (2002). Anomaly-based data mining of intrusions. *Proceedings of the eighth ACM SIGKDD international conference on knowledge discovery and data mining* (Vol. 2002). Edmonton, Alberta, Canada.

Sony Sony Financial Statement 23-05-2011 (2011).

Stapleton, J., & Poore, R. S. (2011). Tokenization and Other Methods of Security for Cardholder Data. *Information Security Journal: A Global Perspective*, *20*(2), 91–99. doi:10.1080/19393555.2011.560923

Stech, K. (2012, March 12). Burglary Triggers Medical Records Firm's Collapse. *Wall Street Journal*. Retrieved from http://blogs.wsj.com/bankruptcy/2012/03/12/burglary-triggers-medical-records-firm's-collapse/

Symantec. (2009a). Anatomy of a Data Breach - Why Breaches Happen and What to Do About It [Whitepaper]. Retrieved from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-anatomy_of_a_data_breach_WP_20049424-1.en-us.pdf

Symantec. (2009b). 6 Steps to prevent a Data Breach. Retrieved November 28, 2011, from http://eval.symantec.com/mktginfo/enterprise/other_resources/b-6-steps-prevent-data-reach_20049431-1.en-us.pdf

Symantec. (2011). *2010 Annual Study : Global Cost of a Data Breach*. Retrieved from http://www.symantec.com/content/en/us/about/media/pdfs/symantec_cost_of_data_breach_global_2010.pdf

Taylor, S. J., & Bogdan, R. (1998). *Introduction to Qualitative Research: A Guidebook and Reference* (Third.). New York City: Wiley.

Trend Micro. (2011). Anatomy of a Data Breach. Retrieved December 23, 2011, from http://about-threats.trendmicro.com/RelatedThreats.aspx?name=Anatomy+of+a+Data+Breach

Trustwave SpiderLabs. (2011). *Global Security Report 2011*. Chicago: Trustwave. Retrieved from https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2011.pdf

Vaidya, J., & Clifton, C. (2004). Privacy-preserving data mining: why, how, and when. *IEEE Security and Privacy Magazine*, *2*(6), 19–27.

Van de Weerd, I., & Brinkkemper, S. (2008). Meta-modeling for situational analysis and design methods. In M. Syed & S. Syed (Eds.), *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications* (pp. 38–58). Hershey: Idea Group Publishing.

Van der Aalst, W. M. P., & De Medeiros, A. K. A. (2005). Process Mining and Security: Detecting Anomalous Process Executions and Checking Process Conformance. *Electronic Notes in Theoretical Computer Science*, *121*, 3–21.

Verdurmen, E., Beierly, I., & Cleary, P. (2011). *Identifying and Detecting Security Breaches*. *System*. Retrieved from http://usa.visa.com/download/merchants/identifying-detecting-breaches-012711.pdf

Verizon. (2011). *2011 Data Breach Investigations Report*. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

Verizon. (2012). *2012 Data Breach Investigations Report*. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Visa Inc. (2001). Cardholder Information Security Program. Retrieved April 19, 2011, from http://www.visa.com/cisp

Visa Inc. (2008). *Responding to a Data Breach; Communications Guidelines for Merchants*. *Security*. Retrieved from http://usa.visa.com/download/merchants/cisp_responding_to_a_data_breach.pdf

Vleugel, A., Spruit, M., & Van Daal, A. (2010). Historical data analysis through data mining from an outsourcing perspective : the Three-phases model. *International Journal of Business Intelligence Research*, *1*(2), 42–65.

Widup, S. (2011). *The Leaking Vault 2011 Six Years of Data Breaches*. Digital Forensics Association. Retrieved from http://www.digitalforensicsassociation.org/storage/The_Leaking_Vault_2011-Six_Years_of_Data_Breaches.pdf

Xu, W., Grant, G., Nguyen, H., & Dai, X. (2008). Security Breach : The Case of TJX Companies , Inc . *Communications of the Association for Information Systems*, *23*(1), 575–590.

Appendix A: Magnetic Stripe

Magnetic Stripe Data

Figure A.1 and Figure A.2 represent the Track1 data of the magnetic stripe of a credit card. Figure A.3 represents the Track2 data.

Track 1: The first row shows the type of data, the second row represents the number of digits, the third row represents the format of the digits and the last row represents related ISO standards. The types of data are in order of appearance: Start Sentinel, Format Code, PAN, Field Separator, Country Code, Name, Field Separator, Expiry Date, Service Code, Pin Verification Value, Discretionary Data, End Sentinel and Longitude Redundancy Check.

	SS	FC	PAN	FS	CC	NM	FS	ED	SC	PVV	DD	ES	LRC
#	1	1	<=19	1	3	2-26	1	4	3	5	var	1	1
format	%	A-Z	0-9	^	0-9	a-Z	^	YYMM	0-9	0-9		?	0-9
ISO			7812		3166								

Figure A.1 Track 1 Data

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
MII	IIN					IAIN												CD

Figure A.2 Primary Account Number

Track 2: The track contains the same data as the IATA track, but without the Format Code, the Name and some Field Separators. The most important difference is the missing Name field. Because this field is missing, the data can be all Binary-Coded Decimals (BCD), while the IATA track also needs to contain alpha-numeric data.

	SS	PAN	FS	CC	ED	SC	PVV	DD	ES	LRC
#	1	<=19	1	3	4	3	5		1	1
format	;		=	0=9	YYMM	0-9	0-9		?	0-9

Figure A.3 Track 2 Data

Appendix B: PCI-DSS

This section describes additional information about PCI-DSS, such as the 6 goals with their corresponding requirements (twelve) and the validation techniques (Chuvakin & Williams, 2010; PCI Security Standards Council, 2010b).

Goals & Requirements

The set of goals and requirements for PCI DSS 2.0 consists of six goals that cover the twelve requirements. This section describes these requirements but does not provide an in-depth understanding.

1. Build and maintain a secure network

Physical entrance to an organization is not required anymore to steal sensitive company data. The company network, together with the attached devices (e.g. workstations, POS devices), are targets for intrusion attacks. By having a secure network, attackers can be blocked from entering the organization.

RQ 1: Install and maintain a firewall and router configuration to protect cardholder data

Firewalls are used to control network traffic, i.e. data flowing in and out of computers and on the network. It regulates what data or devices are allowed to have access on the network. Routers connect two or more networks and/or devices.

RQ 2: Do not use vendor-supplied defaults for system passwords and other security parameters

The easiest way of gaining access to the payment environment is by compromising devices with default system passwords. When these devices are deployed, merchants do not always check and change the systems default settings. These default settings are mostly known and spread out on the internet

2. Protect cardholder data

Cardholder data is any data related to credit cards, as described in section 3.1.1. Merchants who transmit, process or store this data are expected to protect this data and prevent unauthorized access.

RQ 3: Protect stored cardholder data

No cardholder data should ever be stored unless it is necessary for the business. If this holds, it must be stored unreadable. Magnetic stripe data must never be stored.

Guidelines for not storing cardholder data are:

- Limit the storage time to that required for business purposes.
- Do not store sensitive authentication data after authentication.

- Mask the PAN when it is displayed.
- Render PAN unreadable when it must be stored.

RQ 4: Encrypt transmission of cardholder data across open, public networks

Open and public networks often do not use encryption for their transmission. Every data that is being transmitted on such a network can be captured and monitored by any person who has the right tools. Cryptography and security protocols must be used to secure all the data that is transmitted onto such a network.

3. Maintain a vulnerability management program

Vulnerability management is the process of finding weaknesses in a systematic and continuously manner. Regarding PCI, it is focused on the payment environment of a merchant.

RQ 5: Use and regulatory update anti-virus software or programs

Anti-virus must be used on every system to protect them from malicious software threads. An important issue is to make sure that all the anti-virus is always up to date with the latest virus definitions and is always running.

RQ 6: Develop and maintain secure systems and applications

Vulnerabilities in systems and applications (bugs) may allow attackers to access parts of systems/networks that they should not have access to. Security patches from software vendors repair these vulnerabilities and should therefore always be applied to the existing software. A process to rank vulnerabilities based on their risk and impact must be in place.

Software developed internally should always follow the PCI DSS guidelines

4. Implement strong access control measures

Access control allows organizations to physically or technically allow or deny access to cardholder data.

RQ 7: Restrict access to cardholder data by business need to know

Access to cardholder data should always be controlled by the business needs. This means that only those employees who should have access to certain parts of the payment environment are granted access.

RQ 8: Assign a unique ID to each person with computer access

If every employee is assigned a unique IFD, all the actions he/she makes on data and systems can be performed by and traced to authorized users.

RQ 9: Restrict physical access to cardholder data

Physical access to cardholder data must be restricted and monitored by controls. A clear distinction between personnel and visitors must be made. Visitors should always be authorized before accessing an environment that is cardholder related.

5. Regularly monitor and test networks

The networks, both wired and wireless are the backbone of an organization. If vulnerabilities occur in these networks, attackers can gain access to the network with possible disastrous consequences. Regular monitoring and resting of the network can discover and fix these vulnerabilities.

RQ 10: Track and monitor all access to network resources and cardholder data

Logging and tracking are essential for effective forensics and vulnerability management. Discovering the cause of a breach is very difficult without log files that contain traces of the attack.

RQ 11: Regulatory test security systems and processes

New vulnerabilities are always found by attackers and researchers. Al system components, processes en software should be tested frequently to ensure the security is maintained over time. Examples of test are:

- Presence of unauthorized wireless access points
- Quarterly internal and external network vulnerability scans
- Annually internal and external penetration tests
- Use Intrusion Detection and Prevention Systems for monitoring network traffic
- File integrity monitoring

6. Maintain an information security policy

A well-structured security policy informs employees about their role within the complete security strategy of an organization. All employees must be aware of the sensitive nature of cardholder data.

RQ 12: Maintain a policy that addresses information security for all personnel

This policy must contain at least the following items:

- All PCI DSS requirements must be addressed
- Daily operational security procedures
- Usage policies and procedures for critical technologies.
- A formal security awareness program
- The extensive screening of potential personnel
- Incident response plan

Validation techniques

In order to make sure every organization that must be compliant really is compliant, the Council has designed a number of validation tools/methods. Some organizations are allowed to perform tests by themselves, while other organizations are required to let an external party conduct the compliance and/or vulnerability tests. This distinction is made, based on the level of the organization. With the reports, merchants verify their compliance with the PCI-DSS.

Qualified Assessors

Qualified Security Assessor (QSA)

A QSA is an organization or individual certified by the Council to validate PCI DSS compliance of an organization by conducting an annual on-site review. Its main task is to perform an assessment of an organization that handles cardholder data against the requirements of PCI DSS.

Approved Scanning Vendor (ASV)

An ASV is an organization that validate adherence to the external vulnerability PCI DSS requirement by performing vulnerability scans. ASVs may use their own software, or qualified packages to perform the test.

Internal Security Assessor (ISA)

Organizations that want to strengthen their internal PCI DSS expertise and increase the efficiency of complying with the standard can follow a training to become an ISA. The training consists of three phases: Application, Training and Enrollment.

Self-Assessment Questionnaire (SAQ)

The SAQ is a validation tool provided by the Council that needs to be filled in by organizations that does not require an on-site review (PCI Security Standards Council, 2010e). It assists organization is self-evaluating their compliance with PCI DSS and it might be shared with the acquiring bank. Five different versions of the SAQ exist to meet various scenarios, as shown in Table B.1. This questionnaire is not the only part of the SAQ; an Attestation of Compliance is also added to complete the questionnaire.

Table B.1 Types of SAQs

Version	Description
A	Applicable to merchants who do not store cardholder data in electronic format and do not process or transmits any cardholder data on their systems. Those merchants are categorized as “card-not-present merchants”, which means e-commerce or orders by telephone or mail. They have outsourced all cardholder data functions.
B	Applicable to merchants who only process cardholder data via imprint or standalone dial-out terminals. It includes both card-not-present merchants and card-present merchants.

C-VT	Applicable to merchants that only use web-based virtual terminals to process cardholder data. A virtual terminal is an access point to an acquirer, processor or third-party service provider to authorize payment card transactions. The cardholder data is entered manually in the virtual terminal. Cardholder data is only transferred via these virtual terminals and is therefore not stored physically.
C	Applicable for merchants whose POS machines or payment application servers are connected to the internet. Cardholder data is not stored physically.
D	Applicable to all other merchants that do not fit in version A through C and all service providers that are defined by payment brands to complete an SAQ.

Attestation of Compliance (AoC)

The AoC is a merchant's or service provider's certificate that he is eligible to perform and has performed the appropriate Self-Assessment. Together with the Self-Assessment it completes the SAQ.

Report on Compliance (RoC)

The RoC has the following components:

- Contact Information and Report Date
- Executive Summary
- Description of Scope of Work and Approach Taken
- Details about reviewed environment
- Quarterly Scan Results
- Findings and Observations

Network Security Scan (NSS)

The Network Security Scan is performed quarterly by an ASV and scans the network and web applications of a merchant for vulnerabilities and misconfigurations. The ASV discusses the issues found and provides a method to repair them.

On-Site Security Audit

The on-site security audit is an annually audit performed by an external party and is mandatory for every level 1 merchant.

Appendix C: PA-DSS & PTS

Appendix B covered PCI DSS in more detail and this section continues the list of PCI standards with PA-DSS and PTS.

PA-DSS

The Payment Application Data Security Standard (PA-DSS) applies to vendors who develop payment applications that store, process or transmit cardholder data. PCI DSS does not apply to some vendors of payment software because they do not store, process or transmit cardholder data themselves. On the other hand, PA-DSS compliant applications do not make the user of the organization PCI-DSS compliant. The application must be implemented into the PCI-DSS compliant environment following the PA-DSS Implementation Guide.

The Payment Application Data Security Standard consists of thirteen requirements (PCI Security Standards Council, 2010f) which are shown in Table C.1. For a detailed description, please see the PA-DSS 2.0; Requirements and Security Assessment Procedures manual.

Table C.1 PA-DSS Requirements

#	Requirement
1	Do not retain full magnetic stripe, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block code
2	Protect stored cardholder data
3	Provide secure authentication features
4	Log payment application activity
5	Develop secure payment applications
6	Protect wireless transmissions
7	Test payment applications to address vulnerabilities
8	Facilitate secure network implementation
9	Cardholder data must never be stored on a server connected to the internet
10	Facilitate secure remote access to payment application
11	Encrypt sensitive traffic over public networks
12	Encrypt all non-console administrative access
13	Maintain instructional documentation and training programs for customers, resellers and integrators

PTS

Pin Transaction Security (PTS) applies to all organizations that manufacture devices that accept Personal Identification Numbers (PIN) in their transactions. The requirements in the standard must be followed in the design, manufacture and transport of a PIN-device by manufacturers. Merchants and service providers should always use PTS compliant PIN-devices and should be aware of the requirements that are associated with the compliance.

Appendix D: Interview Summaries

Summary interview 1: Security Expert 1

Date	Duration	Topic	Role	Type
31-10-2011	1:00	Indicators	Director (NL)	Face-2-Face

Background expert

This security expert has almost 16 years of experience in the field of IT Risk, Data Privacy, and Information Security Management

Table D.1 Comments on indicators Interview 1

Indicator	Comments
Excessive logins	Two types of excessive logins occur: excessive logins on random hosts and excessive logins on a specific target.
Modification/deletion of data	Modification and deletion of data can occur in every phase and is used in order to wipe the traces the attacker leaves behind.
Automatic launch on boot	Clear
SQL-Injection attempt	Can be visible in log files of the webserver and the database that is being targeted. Should be taken in mind that if SQL-Injection is discovered, it is already too late to protect the database structure or possibly even valuable data. Nevertheless, appropriate actions can be taken to protect the system for further damage.
Unexpected new user accounts	Account can be generated in a legitimate or illegitimate way. Needs to be filtered out in a way.
Archived files in system directory	Make this more general and rename it to suspicious files. The system directory is of course an important directory, but should not be the only directory to focus on.
Suspicious log files	Can be linked to the modification/deletion of data because of missing (parts of) log files.
Unexpected volume in network activity	This will generate a lot of false positives because network activity is highly subject to variances. This is not a strong indicator for preventing a breach.
Improper account usage	Clear
Improper use of protocols	Is hard to detect, because of the use of encrypted protocols such as SSL and HTTPS. To inspect this flow of data, it has to be decrypted to search the packets. This provides more control over the content of the data but generates another security issue, because this data is unencrypted at a point in the organization.
Downloading of suspicious files	Should be renamed to uploading of suspicious files onto the targeted machines by the attacker. The indicators should be based

	on the viewpoint of the attacker.
Unusual services running	Clear
Registry keys modification	Clear
Unknown/unusual network connections	Clear, Intrusion Detection and Prevention Systems.
Malware notification	Malware notification is a clear indicator, but it is nothing more than a confirmation of previous indicators. Logins, unexpected network connections, uploading of files and various others precede the malware warning from scanners.

Overall comments

What happens to the list of indicators when instead of an external attack, the attack starts from the inside? It is much harder to determine a breach if all the necessary steps are performed legitimately by authorized employees.

The order of the indicators can be done in various ways; think of a chronology order or by the ease of detection. Easy to discover indicators are: starting of a new service, creation of accounts, uploading of files, presence of files in directories where that should not be the case. But there is always a tradeoff between discoverability and usability of an indicator. For example, the creation of a new user account is an easy to monitor indicator, but it can be hard to make the distinction between legitimate and illegitimate creation.

In a nutshell the attack has the following layout: find an entrance to the organization; upload files to systems and change the boot sequence of services/applications to maintain the access and collect/extract valuable data. The attackers try to wipe every trace left behind to maintain its undercover status.

Why is SQL Injection the only attacking technique that is included in the list of indicators? For example the attacking techniques remote access application or malware are not included. Characteristics of these techniques are mentioned, but not the overall name of the technique. It might be better to split up SQL-Injection in multiple indicators, such as log files of the web and targeted database server.

In order to increase the focus on credit card transactions, a closer look at the transaction process is required to gain a more specified list of indicators. If the indicators specifically for credit card transactions can also be applied to other types of breaches (e.g. personal data), the method can be used it a much wider scope than solely credit card transactions.

Summary interview 2: Security Expert 2

Date	Duration	Topic	Role	Type
02-11-2011	1:00	Indicators	Manager (NL)	Face-2-Face

Background expert

This security expert has six years of experience in the field of Information Security and Code Reviewing.

Table D.2 Comments on indicators Interview 2

Indicator	Comments
Excessive logins	Will probably generate a lot of false positives if merchant has a lot of host machines (>100.000). There will always be employees who will enter their logins wrong.
Modification/deletion of data	Clear
Automatic launch on boot	Clear
SQL-Injection attempt	Clear
Unexpected new user accounts	Clear
Archived files in system directory	Clear
Suspicious log files	Clear
Unexpected volume in network activity	Clear
Improper account usage	Clear
Improper use of protocols	Clear
Downloading of suspicious files	Clear
Unusual services running	Clear
Registry keys modification	Clear
Unknown/unusual network connections	Clear
Malware notification	Clear

Overall comments

Credit card transactions occur on specific systems. This is a different environment than the regular business environment of an organization.

The indicators are just normal hack indicators and they do not focus on credit card transactions. The beginning of a hack or other intrusion is uniform for every type of sensitive data that is

compromised, whether it is credit card data or other personal data. The indicators are therefore to general for a credit card breach.

For credit card transactions the environment around terminals can be more important (e.g. skimming, sniffing of wireless networks) and is exclusively the case for credit or debit card transactions. This is however decided upon to leave it out of scope for this research, because the research focusses on the mining of indicators of a breach. The focus on terminals would result in a complete redesign of the research.

Summary interview 3: Security Expert 3

Date	Duration	Topic	Role	Type
04-11-2011	1:00	Indicators	Consultant (NL)	Face-2-Face

Background expert

This security expert works for a large multinational and focuses on the security of its payment system. This payment system accepts a variety of cards, including credit cards. Although the focus of this expert does not lie with the security of the credit card transaction, he is actively working on the security of another payment card, so he can still review the list of indicators and provide additional information if necessary.

Table D.3 Comments on indicators Interview 3

Indicator	Comments
Excessive logins	Generates a lot of false positives and false negatives. Will it be monitored locally on a workstation/host, or globally on a server? The payment system of an organization should be a closed system, separated from the other systems in an organization.
Modification/deletion of data	Focus on the content of log files. In order to detect modification, or attempts to modification of data, access control mechanisms can be used that write entries in log files every time a read-only file is tried to being written to. Time management.
Automatic launch on boot	Clear. This indicator does not need any improvements and is clear.
SQL-Injection attempt	Do not use SQL-Injection as an indicator, but split it up in suspicious log files or any other Intrusion Detection System Indicator.
Unexpected new user accounts	This indicator is very difficult to implement. By using requirements from Identity Access Management, a new user account can only be created if it is linked with an actual employee. Every employee can have only one user account, so a warning is signaled out if a new account is created and it is not linked to any employee.
Suspicious files in system directory	This can be easily detected by using hashes to check the integrity of a certain part of your files and folders on a workstation (e.g. system directory). This can be done locally to avoid false positives if users update their machine, or via a server in combination with a Public Key Infrastructure (PKI). Also a whitelist can be created to only allow known files to be present in certain directories.
Suspicious log files	Text mining of log files
Unexpected volume in network activity	Time is very important here. A day must be split up in for example 24 parts and an average network activity must be calculated for every part. By using this approach, a lot of false positives are excluded.
Improper account usage	Very abstract indicator.

Improper use of protocols	An example is malware that lowers the SSH standard to use vulnerabilities that are not present in the newer standard anymore. Another example is the bypass or misuse of a DNS server. Additional data can be added to the reply package of a DNS-request that can be compared with adding additional data to a SQL-query during a SQL-Injection attack.
Downloading of suspicious files	Clear.
Unusual services running	If a suspected service is discovered, an immediate hash of the system must be made to detect if anything else is infected or misused.
Registry keys modification	Can also be detected by using hashes on the registry files.
Unknown/unusual network connections	Firewall logs show the presence of unwanted devices/persons in the network.
Malware notification	Clear.

Overall comments

The first thought of the expert when we started talking about credit card breaches was fraud with these cards at a terminal (skimming).

Not every indicator can be used on every system. Excessive logins can be found on workstations but not on systems that perform credit card transactions.

The ordering of the indicators is hazardous. It is better to describe the relationship between two indicators than to clearly state an order of appearance. This relationship can assist in finding additional indicators that were not noticed before or draw conclusions based on previous found indicators.

An example of a credit card specific indicator is a large query result on a database that contains (encrypted) credit card data, especially if this request comes from an unknown or unusual source.

Method

The total risk should be based on three things: impact, accuracy and chance. If the risk is known and it falls in the category low, an entry to a log file is created. If it is a medium risk, a warning appears on the screen of an administrator. If it is a high risk, multiple persons should be emailed or called to create an overall awareness of the risk. Maybe the live environment should be switched with a backup environment to prevent further damage to the system. This cannot be done for the production environment; it should never be closed down automatically since this is affecting day-to-day business.

Workstations can easily be isolated from the network if risks are identified on them.

A hash of critical system files/folders must be made at least once a day. This detects suspicious services and/or uploaded files.

Summary interview 4: Security Expert 4

Date	Duration	Topic	Role	Type
21-11-2011	0:45 hour	Data Loss Prevention	Manager (UK)	Phone call

Introduction

This security expert is a manager specialized in IT Risk and Security and focuses on Data Loss Prevention and Encryption Deployment. He is working at this position for over six years now.

Data Loss Prevention

There are no specific Data Loss Prevention techniques for credit card data. It just covers DLP for every sensitive data that exists in an organization. Existing solution can be used for credit card data as well where for example card numbers can be tracked in emails.

An important part of prevention is to have a very strong firewall. This is in most cases the first contact attackers have with your organization.

Advanced DLP tools can discover unencrypted credit card numbers on the network or emails, but there is no or little room for customization.

You really need to know what is the sensitive data in your organization and where is it stored and who has access to it.

The access needs to be arranged by proper access policies and tools.

The best solution for every organization is a tailor made data leakage prevention tool that focuses on those indicators that are specific for your organization.

Follow-up should be of the form:

- do nothing
- send e-mail to person in charge
- block traffic of certain systems

The three stages that exist are monitor events, alert persons in charge and perform corresponding follow-ups.

Summary interview 5: Security Expert 5

Date	Duration	Topic	Role	Type
22-11-2011	0:45 hour	Data Loss Prevention	Manager (CA)	Phone call

Introduction

This security expert is a manager specialized in Vulnerability Management with a lot of experience with PCI DSS related projects. He is working at this position for six years. Vulnerability Management covers requirement 5 & 6 of PCI DSS 2.0.

Data Loss Prevention

The presence of an intruder or malicious activity can be detected by certain indicators, e.g.:

- A flag on database that prevent them from being copied. Every time this database gets a copy request, an issue must be filed and include the user who did the request, timestamp and targeted database.
- Clarification of excel files

Organizations can use tools such as Card Recon to identify the presence of unencrypted credit card numbers in various file formats. It can scan every workstation that is connected to the network and gives a detailed description of its findings. Card Recon uses little to no resources so that it can run on systems in the production environment without significant performance loss.

PCI DSS

"To provide the method with a credit card focus, you need to focus more on the twelve requirements of PCI DSS".

Section 5: logs

Section 6: access control

Password

Change management system

Why is PCI DSS not enough to secure the payment process?

1. Immature; the objective is really tense
2. Minimal baseline;

The desired flow should be from your current security and use PCI DSS to test this security. PCI DSS should not

Information Protection Tools

Perimeter of access

Interactive Voice Response (IVR) & Voice Over IP (VOIP)

Vedasys :

DLP tool, but Card Recon is better.

Summary interview 6: Merchant 1

Date	Duration	Topic	Role	Type
25-11-2011	0:45 hour	Credit Card Process Evaluation	Payment Compliance Leader	Phone Call

Credit Card Transaction Process

The process of a credit card transaction within a merchant as showed in Figure 3.5 shows the correct process on a high level. What could be included is the real-time scan for fraudulent transactions by either banks or the merchant self. But since this is not in the scope of this research it shall not be included.

Impact of PCI DSS

PCI DSS requires a lot more logging for every application that has contact with credit card numbers. Change Management becomes much more important. Systems have to be changed by the merchant in order to meet compliance with the standard.

Credit Card Specific Indicators

The Luhn-algorithm can be used to identify valid credit card numbers floating around in the network. Credit Card Network Organizations used to only use credit card number that passes this Luhn test, but American Express stopped using this check for their credit card numbers. What can still be used to detect every credit card are the first six digits of a card number; the Issuer Identification Number.

Method

Try Neural Networks to identify normal and abnormal behavior.

Summary Interview 7: Payment Service Provider 1

Date	Duration	Topic	Role	Type
02-12-2011	1:00 hour	Data Breaches, Payment Process	Operational Director	Face-2-Face

Introduction

This Internet Payment Service Provider (PSP) provides services all over the world. It processes both national as international transactions. PSP's are founded to assist organizations in performing transactions. For organizations, this transaction environment is a very complex environment which is mainly the cause of the intense security measures that are necessary. PSP's core business is this transaction environment and they are highly specialized in it. This PSP works with over 100 different payment methods all over the world.

Breach Prevention

"The best way to prevent organizations from suffering from a breach is to outsource the transactions environment to a third party or PSP". Hereby, organizations do not have to be PCI DSS compliant and do not have to think about complex security measures, which also come with high costs.

Data breaches that include credit card data are a huge problem, but skimming at POS (terminals) is still a huge problem as well.

Breach prevention consists of two steps:

1. Do not let attackers manage to gain entrance to your organization and if they do,
2. Make sure they cannot access the data

"Above the basic guidelines of PCI DSS, we use Hardware Security Modules (HSM), which functions as a key management …

Impact of PCI DSS

"The advantage of our company is that we started when PCI DSS 1.0 was found. This became the foundation of our product". Their product is very flexible and can easily be adapted to any future changes in the standard.

Method

"If we suspect a possible breach by some indicators, we perform a data mining analysis on our logs to find more evidence of this breach. We are not constantly monitoring every log file to detect such a breach, since this creates a lot of overhead on our systems".

Summary Interview 8: Payment Service Provider 2

Date	Duration	Topic	Role	Type
05-12-2011	1:00 hour	Data Breaches, Payment Process	Information Security Manager	Face-2-Face

Introduction

This organization is, just as interview 7, a global Payment Service Provider. Its main global payment method is credit cards. In The Netherlands this is Ideal, where credit cards are the least used payment method.

This organization has three different products

1. The merchant collects all the essential data from the customer and sends this data to the PSP. This collection occurs completely on the merchant's site, so he must be PCI DSS compliant in order to perform the transaction.
2. The merchant makes the order but the payment is done on the server of the PSP. Hereby, the merchant does not see any credit card data and does not have to be PCI DSS compliant in order to allow credit card transactions.
3. The last product is a mix of the first and second product.

Breach Prevention

The payment process is an automated process that runs in an isolated environment.

To prevent breaches from POS devices (e.g. skimming) an end-to-end encryption must be used.

Impact of PCI DSS

"The biggest impact on our organization was the translation from PCI DSS 1.1 to 1.2". Version 1.2 introduced key encryption application. "We are currently investigating the implementation of PCI DSS 2.0".

Web application penetration tests are used to test the security of new and existing applications. White-box-tests, which are used internally and black-box tests, which are performed by an external party are used to test this security.

Logging

A typical organization produces a lot of logs. These logs cannot be scanned by hand but needs to be collected and scanned using automated software. Furthermore, not everything needs to be logged. If you do so, this will generate a lot of overhead on servers and decreases performance. "In our organization, only system and firewall logs are used and no application logs to reduce the processing power that is needed".

Method

“The most important task of this-, or such a similar method, should be the correct correlation of log files and to extract the useful data out of the immense amount of log data”. ArcSight is such a log management tool that also includes analysis of gathered log files.

The payment environment of most organizations runs on Linux and almost no virus or other malware is available for Linux. Log files of anti-malware software are therefore not a very relevant indicator. For workstation or hosts that run other Operating Systems that are vulnerable to malware (e.g. Windows) this indicator is correct.

Glossary

Remote Access Application

Some entries in this figure leave traces behind in log files or any other system that monitors an organization's security. For instance, every remote access application that connects to the network is/should be logged by systems or devices such as routers/switches or port scanners. The log files contain data such as origin of the connection, data and time, session length etc., while port scanners alert system managers when unknown connections are present on ports, entrances on a networking device where other device can connect to, that should not be there.

Social Engineering

Social engineering is a popular technique used by attackers that is different from every other attack, because it aims for the compromise of data from a person rather than brute force break into a system to gain access (Orgill, Romney, Bailey, & Orgill, 2004). It consists of two aspects, a physical and psychological aspect. An example of a social engineering attack can be an attacker who calls an employee and make him/her believe he is from the IT department of the organization. The attacker has a plausible story that requires the username and/or password from the employee. Unaware employees might provide their username and/or password to the attacker, not knowing being a victim of a social engineering attack. Employees who are aware of the social engineering phenomena and suspect the phone call should immediately create a security event to warn other employees.

E-mail Trojan

E-mails that contain malicious software (malware) or Trojan horses are still a large threat for data breaches. A Trojan is a piece of software that appears legitimate, such as a PDF, an image or a Word document, but in reality it contains malicious code that damages the system (Cisco, 2011). Trojans are named after the wooden horse the Greek used to infiltrate Troy.

An "advantage of Trojans is that they cannot reproduce themselves by infecting other files or duplication. The only way to get infected by a Trojan is to install them from a medium, mostly via e-mail attachments. When such an attachment is opened, the malicious code is activated and the Trojan is installed. An up-to-date virus scanner that scans all attachments in e-mails is a must for securing organizations to this type of attacks. When a Trojan horse is found in an e-mail by such a scanner, a security event must be created to warn other employees.

The most common damages a Trojan inflicts are creation of backdoors, stealing data, deletion of files and activating/spreading other malware (viruses, worms).

SQL Injection

SQL (Structured Query Language) injection is still, even after a decade, the most popular way for breaking into a web-based application. It is used in order to gain information out of databases that are used by these web-based applications (Nystrom, 2007). These applications use SQL to "talk" to and retrieve data from the underlying database.

A typical SQL Injection consist of three steps; reconnaissance, probing for vulnerabilities and the attack itself. The reconnaissance step is meant for the discovery of systems and services that are operating in the environment. Once they are known, the probing step finds vulnerabilities that can be used later in the attack. Special tools can be used that will assist the attacker by scanning webservers for vulnerabilities. The actual attack is a combination of multiple techniques which include AND/OR-, comments-, string concatenation-, UNION injection-, hexadecimal- and whitespace manipulation attacks (Luong, 2010).

SQL Injection can be prevented by secure coding, monitoring for attacks and the implementation of a Network Intrusion Detection System (Nystrom, 2007). The best way in defending against SQL Injection is secure coding; if the webserver contains solely secure programmed applications, attackers cannot use any technique to gain access to it. Developers must be made aware of this issue and follow best practices in order to have secured applications. If, however, attackers still try to breach a webserver, this can be notified by the use of network monitoring tools or Intrusion Detection Systems by logging SQL errors or unauthorized SQL queries for example.

Content Management System Portal

Attackers can gain entrance via a poorly secured Content Management System Portal (CMSP). Such a portal is used to gain access to the data that is stored in a CMS. CMS are designed to create a central repository where multiple users can contribute and share the data that is in the repository. A CMS can provide access to the data based on the different roles employees have. If the CMSP is poorly configured, attackers can gain access to the data that is stored inside it.

Legitimate Access

Legitimate access is access by persons who legitimate have access to systems or data sources. Misuse of this access is hard to monitor because the attack takes place by persons who should have access and therefor nothing strange happens.

Physical Access

Physical access is the actual entrance to an organization. This can for example be done by using fake or copied entry cards to a specific floor/building. If attackers manage to enter an organization they are one step closer for reaching their goal. Physical access is only a small percentage of all the infiltration attacks, but despite the actions that can prevent such attacks (e.g. biometric recognition) it still occurs.

Remote File Inclusion

Remote File Inclusion (RFI) is a security issue in programming code. If a certain script receives data from the outside, there is always the possibility that this data is sent by an attacker. It then could be corrupted to make the script perform actions it is not supposed to do. RFI allows an attacker to run code on the server of an organization. RFI can be prevented by using data validation inside your scripts that examine every input that enters the script from the outside.