# Preventing credit card data breaches.

# A framework of critical indicators

Hans Peersman[1], Ronald Batenburg[2] and Marco Spruit[3]

[1] Deloitte Nederland, Utrecht, The Netherlands
hpeersman@deloitte.nl
[2] Utrecht University, Utrecht, The Netherlands
r.s.batenburg@uu.nl
[2] Utrecht University, Utrecht, The Netherlands
m.r.spruit@uu.nl

**Abstract.** 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. 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 warnings for a possible data breach. These indicators are structured in a way that can support organizations (i.e. merchants) at developing a strategy that will help them discovering a data breach of credit card data in an early phase. The indicator framework is validated during interviews with subject matter experts in order to gain the best knowledge on what steps should be included.

**Keywords:** data breaches, credit card, risk management, data mining

## 1 Introduction

Data breaches are rapidly increasing in both frequency, impact and media attention (DatalossDB, 2012). This specifically applies to breaches that cover credit card data. Techniques, such as Intrusion Detection and Prevention Systems, can monitor organizational networks 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 (SSC) 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). Data mining enables the principle that the sooner a breach is detected, the better organizations can defend themselves against it. A key condition for successful data mining however, is to define the 'right' indicators for credit card data breaches.

xxxx, p. x, 2012.

This paper 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 of less interest for this study, 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). We also focus 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.

This paper will present a framework for organizations that, assisted by data mining, enables prevention or holding credit card breaches in an early stage. The framework that will be presented in this paper aims to prevent breaches and cannot be used to discover fraud in transactions. Furthermore, skimming of terminals is left out of this study. Hence, the focus lies on the credit card data that is already inside a merchant's, payment provider' or even credit card corporation's environment. The initial target for this study 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.

The next section 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. Next it is explained what a breach is, what happens during a breach – and then what the indicators of a breach are. The framework to prevent data breaches in the future, validated by experts, is presented in the section afterwards. The paper concludes with a discussion and conclusion and a chapter with recommendations and further research.

## 2 Credit Card Transaction and the PCI SSC

In June 2001, Visa started 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.

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 1 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 1 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.

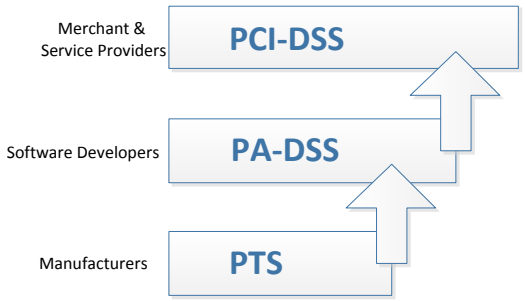


**Figure 1. PCI SSC Security Standards (PCI Security Standards Council, 2010c)**

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.

PCI-DSS is the standard for all merchants and service providers that store, transmit or process cardholder data (Chuvakin & Williams, 2010). It is stated that 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 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 1. They are divided into six goals with multiple requirements.

**Table 1. 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.

# 3 Data breaches

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. 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". I.e., it was based on a small sample set of data breaches and is currently extended with more breaches.

**Table2. 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. Table 2 shows the high-level outcome of this research. 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.

During a breach, data is compromised from an organization. An relevant question is how attackers succeed in gathering this data. A data breach can be broken down by of four phases; infiltration, observation, collection and exfiltration (Symantec, 2009). 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 of compromising).

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. As with previous years, Remote Administration Application (RAA) is by far the most used technique to infiltrate an organization. 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.

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 defence. Organizations that only focus on the outer perimeter have a disadvantage here, because attackers that can break this line of defence can perform actions more stealthy than within organizations that have multiple lines of defence. 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.

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. 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, ranked by occurrence in 2009. This analysis is based on a study of 200 data breaches in 24 different countries by SpiderLabs (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 A framework of critical data breach indicators

Based on the previous notions, the next step is set towards a framework of indicators to support credit card data breach prevention. To begin with, we analysed and compared four publications in this area:

- REF 1: Aldridge, J. (2010). Breach Indicators (retrieved from https://isaca-washdc.sharepointsite.net/webresources/Presentations/Conference-April2010-Session1.pdf)
- REF 2: Cheney, J. S. (2010). Heartland Payment Systems: Lessons Learned from a Data Breach. Philadelphia: Federal Reserve Bank of Philadelphia.
- REF 3: PricewaterhouseCoopers LLP. (2009). Safeguard your sensitive data (retrieved from http://www.pwc.com/us/en/it-risk-security/assets/safeguard_your_sensitive_data.pdf
- REF 4: 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)

Based on these publications, a 'theoretical' set of data breach indicators was discussed by eight semi-structured interviews held with various subject matter experts (Table 3). The interviews have a common foundation of questions that is used in every interview.

**Table 3. Subject Matter Expert Interviews**

| # | Organization | Role | Duration | Topic |
|---|---|---|---|---|
| **1** | Dutch Consulting Organization | Director Security | 1:00 hour | Indicators |
| **2** | Dutch Consulting Organization | Manager Security | 1:00 hour | Indicators |
| **3** | Dutch Consulting Organization | Consultant Security | 1:30 hour | Indicators, Data Types |
| **4** | British Consulting Organization | Manager Security | 0:45 hour | Indicators, Data Loss Prevention |
| **5** | Canadian Consulting Organization | Manager Security | 0:45 hour | Indicators, Data Loss Prevention |
| **6** | Merchant | Payment Compliance Leader | 0:45 hour | Indicators, Payment Process, PCI DSS, Method |
| **7** | Payment Service Provider | Operation Director | 1:00 hour | Indicators, Data Breaches, Payment Process, Method |
| **8** | Payment Service Provider | Information Manager | 1:00 hour | Indicators, Data Breaches, Payment Process, Method |

Every interview was designed to move away from the specified path in order to gain additional in-depth detail about a certain topic. To achieve this goal probes were sed. 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 had the following layout:

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

The topics of credit card transactions, PCI compliance, data breaches and data mining were briefly mentioned to provide an overall understanding. Then the list of indicators was discussed. This is the part where the expertise and thoughts of the expert was 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 interviews, the framework of critical indicators is constructed. This is shown in Table 4.

**Table 4. The list of critical data breach 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 |

After name and description, the third column in Table 4 (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), as described the previous section.

Based on this framework, a basic method can be created that prevents a breach. For a large security organization, we define six steps to prevent a data breach:

- 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.
- 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 paper.
- 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.
- 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.
- 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.
- 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.

## 5 Conclusions

This paper described the environment of a credit card transaction and PCI DSS to make this environment more secure. After describing data breaches, four phases of a breach were defined. Based on literature and interviews with subject matter experts, a framework of critical indicators was created. Nex,t six steps for preventing credit card data breaches are defined.

A number of limitations and future research can be identified. As stated at the introduction, this study focused 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 paper, 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.

.

## References


1. 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.
2. Aldridge, J. (2010). Breach Indicators. Retrieved from https://isaca-washdc.sharepointsite.net/webresources/Presentations/Conference-April2010-Session1.pdf
3. Cheney, J. S. (2010). Heartland Payment Systems: Lessons Learned from a Data Breach. Philadelphia: Federal Reserve Bank of Philadelphia.
4. Chuvakin, A. A., & Williams, B. R. (2010). PCI Compliance. (W. Spangenberg, Ed.) (2nd ed.). Waltham, MA: Syngress Publishing, Inc.
5. DatalossDB. (2012). Dataloss DB Latest Incidents. Retrieved March 16, 2012, from http://datalossdb.org/index/latest
6. 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.
7. MasterCard Worldwide. (2003). Site Data Protection and PCI. Retrieved April 19, 2011, from http://www.mastercard.com/sdp
8. PCI Security Standards Council. (2010a). About Us. PCI Security Standards. Retrieved from https://www.pcisecuritystandards.org/organization_info/index.php
9. PCI Security Standards Council. (2010b). PCI DSS Quick Reference Guide. Retrieved from https://www.pcisecuritystandards.org/documents/PCI SSC Quick Reference Guide.pdf
10. PCI Security Standards Council. (2010c). PCI SSC Data Security Standards Overview. Retrieved May 24, 2011, from https://www.pcisecuritystandards.org/security_standards/index.php
11. 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
12. 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
13. PricewaterhouseCoopers LLP. (2009). Safeguard your sensitive data. Retrieved from http://www.pwc.com/us/en/it-risk-security/assets/safeguard_your_sensitive_data.pdf
14. 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/
15. Symantec. (2009). 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
16. 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
17. Vaidya, J., & Clifton, C. (2004). Privacy-preserving data mining: why, how, and when. IEEE Security and Privacy Magazine, 2(6), 19–27.
18. 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

19. Visa Inc. (2001). Cardholder Information Security Program. Retrieved April 19, 2011, from http://www.visa.com/cisp
20. 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