Heartland Data Breach Analysis

Cingolani Alessandro
Master Degree in Cybersecurity
Sapienza University of Rome

Zamparini Matteo
Master Degree in Cybersecurity
Sapienza University of Rome

February 13, 2020

Abstract

Around 2008 an US company, called Heartland, suffered from a massive data breach, which resulted to be biggest leak of cardholder data until that time. This report briefly recall, by citing official sources and newspapers, the most important event happened both before and after the attack with the aim of describing later which weaknesses affected the company at the time. Since Heartland relied only on PCI-DSS compliance, a description of main security controls that were not present is provided and subsequently two cyber-security framework (NIST and CIS) are applied to the case in order to understand if they could have mitigated some of the main consequences to highlight the importance of implement such standards as a preemptive defense to concrete cyber attacks. At the end a summary section compares advantages and drawback, derived from their practical application, of both frameworks.

1 Introduction

On January 20 2008 Heartland Payment System, a US-based payment processing and technology provider, announces publicly, on the same day of the President Obama's inauguration, that it had suffered a devastating security breach within its processing system.
At the time of the misdeed Heartland processed 100 million payment card transactions per month which lead this attack to be considered the biggest data breach ever occurred (until that moment).
The company both before and in the course of the breach was in compliance with the Payment Card Industry Data Security Standard (PCI DSS)[10], required by credit card providers such as Visa and Mastercard in order to be approved to process their card's payments.
The hackers managed to enter inside the company's system by exploiting an SQL injection present in an eight years old web login page, subsequently, they spent 8 months attempting to access the payment processing network while trying to avoid detection from the several different anti-virus systems used by Heartland.
After hackers exploited the web-login page vulnerability Heartland conducted several security audits engaging third-party companies all of which have confirmed that it was PCI compliant. Notwithstanding Visa first alerted Heartland about "*suspicious activity surrounding certain cardholder accounts*" nearly one year later and this lead the company to call U.S. Secret Service and hire two breach forensic teams to investigate[3]. A malicious software, that apparently allowed the hackers to stole the data, was discovered.

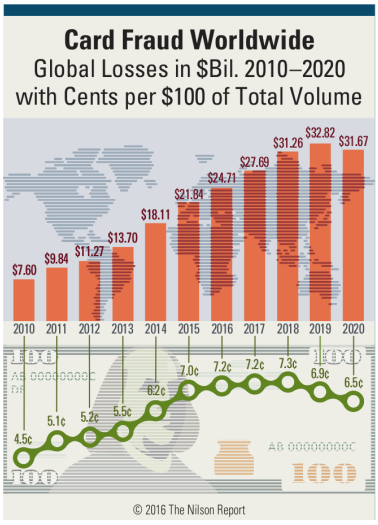

Figure 1: Taken from the Nilson Report[9]

The company specified that no merchant data, cardholder Social Security numbers (SSN), unencrypted personal identification numbers (PIN), addresses or telephone numbers were jeopardized as a result of the

breach; however, the stolen data includes the digital information written into the magnetic stripe present on credit and debit cards. Equipped with this information, criminals can design counterfeit credit cards by imprinting the same stolen data on manufactured cards. Although this can seems quite useless, according to the Nilson Report[9] those kinds of thefts was a very profitable business at the time which caused 7.6 Billions of dollars losses globally only in 2010 [Fig. 1].
On the other hand, in terms of revenue, Heartland reportedly had to pay around $145 million in compensation for fraudulent payments, according to Judge. The figure includes a fine of nearly $60 million from Visa, another of about $3.5 million with "American Express" along with approximately $26 million in legal fees.[11]
After the breach the CSO Jonh South has focused his efforts on staying ahead of future breaches, employing security technology to do so and working to increase communication with industry colleagues.

Figure 2: Heartland stock price, analysis, 9/1/2009-30/1/2009, (source: finance.yahoo.com)

2 Company Security Policies and Status

One interesting aspect of that breach is that Heartland were aware of the potential security threats that could target those companies that process payments and consequently at the time various security policies were put in place.
By examining the 2008 company's "Form 10-K"[4], a required annual report that gives to stakeholders an overview of company's financial performance, company state that "*We place significant emphasis on maintaining a high level of security in order to protect the information of our merchants and their customers.*".
This sentence is then justified in accordance with the applied security policies since the report remarks that they maintained current updates of networks, operating system security releases and virus definitions in conjunction with third-party regularly test that aimed to detect systems for vulnerability to unauthorized access. Furthermore sensitive data stored inside databases (like cardholder numbers) were protected with tripe-DES encryption which represented the highest commercially available standard for encryption.
The company also have emphasized their certifications pointing out that they successfully applied the Payment Card Initiative Data Security Standard (PCI-DSS) which reviewed Heartland's payment processing and Internet-based reporting systems.
Along with that they also implemented an annual "SAS-70" review engaging external auditors and publishing the "*Report on Controls Placed in Operation and Tests of Operating Effectiveness*" and meanwhile is mentioned that they undertook an independent Cyber-Risk Assessment.
On the same document, specifically in the "Risk Factor" section, Heartland explicitly presents the possibility of "Unauthorized disclosure of merchant and cardholder data through breach of our computer systems" consciously explaining the related consequences of this event, such as sanctions by Visa and MasterCard.

Unauthorized disclosure of merchant and cardholder data, whether through breach of our computer systems or otherwise, could expose us to liability and protracted and costly litigation.

We collect and store sensitive data about merchants, including names, addresses, social security numbers, driver's license numbers and checking account numbers. In addition, we maintain a database of cardholder data relating to specific transactions, including bank card numbers, in order to process the transactions and for fraud prevention. Any significant incidents of loss of cardholder data by us or our merchants could result in significant fines and sanctions by Visa, MasterCard or governmental bodies, which could have a material adverse effect upon our financial position and/or operations. In addition, a significant breach could result in our being prohibited from processing transactions for Visa and MasterCard.

Our computer systems could be penetrated by hackers and our encryption of data may not prevent unauthorized use. In this event, we may be subject to liability, including claims for unauthorized purchases with misappropriated bank card information, impersonation or other similar fraud claims. We could also be subject to liability for claims relating to misuse of personal information, such as unauthorized marketing purposes. These claims also could result in protracted and costly litigation. In addition, we could be subject to penalties or sanctions from the Visa and MasterCard networks.

Although we generally require that our agreements with our service providers who have access to merchant and customer data include confidentiality obligations that restrict these parties from using or disclosing any customer or merchant data except as necessary to perform their services under the applicable agreements, we cannot assure you that these contractual measures will prevent the unauthorized use or disclosure of data. In addition, our agreements with financial institutions require us to take certain protective measures to ensure the confidentiality of merchant and consumer data. Any failure to adequately enforce these protective measures could result in protracted and costly litigation.

Figure 3: Paragraph of the Form 10K where Heartland precisely describe what the consequences of a data breach will be. (Page 30)

3 The Data Breach

This section contains a detailed technical analysis of the event occurred during the attack, specifying which was the vulnerabilities and how they were exploited. The majority of the reported information comes from the FBI advisory[7] released after the three important breaches happened between 2007 and 2008[1] and, although the advisory was not specific for the Heartland, there are plenty of reasons to believe that the example attack presented in the document is very similar to the one used in this case study.
The breach was a very slow moving event. It started in 2007 when the hackers exploited, for the first time in the company history, a SQL injection in a web login page which was developed eight years before[16].

*** Joint USSS/FBI Advisory ***

PREVENTIVE MEASURES

Over the past year, there has been a considerable spike in cyber attacks against the financial services and the online retail industry. There are a number of actions a firm can take in order to prevent or thwart the specific attacks and techniques used by these intruders. The following steps can be taken to reduce the likelihood of a similar compromise while improving an organization's ability to detect and respond to similar incidents quickly and thoroughly.

Figure 4: Introduction of the FBI Advisory[7]

They used an extended procedure called **"xp_cmdshell"**[2], which is installed by default on Microsoft SQL Server (MSSQL), to download their hacker tools inside the compromised server. With this method, an attacker is able to execute any command in the server with the same permissions of the user that is currently running the database software. The most believable version of Microsoft SQL Server running in Heartland' system at the time is "2000". Major hints come from the fact that the web site had been developed eight-year before and the *"xp_cmdshell"* feature was disabled by default in version "2005". In addition on the "2000" version, this procedure is only available if the database software runs with sysadmin rights which makes the attackers able to perform a lot of more harmful actions.
During this period hackers were confined into the company's corporate network, which, as required by PCI-DSS policies, is separate from the process-payment system.

[1] In detail the Heartland, 7-Eleven Inc., Hannaford Brothers Co.[13]
[2] Official documentation : https://docs.microsoft.com/enus/sql/relationaldatabases/systemstoredprocedures/xp-cmdshelltransactsql?view=sqlserver2017

Although at the time when the breach was announced (May 2008) Heartland knew how the corporate network had been exploited, it was unaware the hackers were still present on its system for months conducting reconnaissance. As a matter of fact, on April 30, Heartland hired Trustwave, a computer security firm, that conducted an audit and deemed it compliant with PCI DSS.
After many investigations led by U.S. Secret Services and by two breach forensics teams[3] it was found that the hackers have moved from corporate to process-payment network with the help of valid Windows credential obtained using tools like **fgdump**[3] or similar. Such tools have been employed to extract NTLM password hashes from Windows Security Account Manager(SAM). In details, NTML is a suite of Microsoft security protocols intended to provide authentication, integrity, and confidentiality to users. Hackers had probably cracked hashes due to the usage of weak passwords inside the company.
When they were inside the process-payment network hackers installed what is called a **"network sniffers"** which are able to catch any packet that passes through the network, including card data and all the systems transaction. Sniffers are typically not identified by network security tools due to the fact that they are passive auditors and therefore do not execute any particular action that could reveal their presence.
Subsequently the attackers managed to install back-doors able to communicate periodically with their servers in order to secretly and persistently gain access to the compromised network.
Once they obtained regular access to the system hackers start to target Hardware Security Modules (**HSMs**), which are physical computing devices that safeguards and manages digital keys for authentication and provides cryptoprocessing. They trying to attack applications and brute-force HSMs in order to obtain some credit card data. To conclude the stolen data were transferred to a server owned by the attacker, which in the end captured card account numbers, expiration dates and, in 20 percent of cases, the customer's name as well[2].

OVERT ACTS

18. In furtherance of the conspiracy, and to effect its unlawful object, the coconspirators committed and caused to be committed the following overt acts, among others, in the District of New Jersey and elsewhere:

a. On or about November 6, 2007, GONZALEZ transferred a computer file to the Ukranian Server named "sqlz.txt" that contained information stolen from Company A's computer network.

b. On or about November 6, 2007, GONZALEZ transferred a computer file to the Ukranian Server named "injector.exe" that matched malware placed on both Heartland and Company A's servers during the hacks of those companies.

Figure 5: Court Sentence[13] where hackers moves are describer

[3] Official website: https://sectools.org/tool/fgdump/

3.1 Timeline

2006	Heartland created the "*Merchant Bill of Rights*" which the company describes as "an industry standard for fairness, honesty and transparency in credit and debit card processing[1].
2007	A *security assurance* was stipulated before the data breach occurred. Heartland made the following affirmative representations concerning its security measures: "Our internal network configuration provides multiple layers of security to isolate our databases from unauthorized access and implements detailed security rules to limit access to all critical systems."[4].
December 2007	Attackers exploited a vulnerability and *gain access to the network*, although they were confined into the company's corporate network.[2]
2007/2008	*Heartland caught the breach* of the corporate network, but was unaware the hackers were sitting on its system for months conducting reconnaissance.[2]
30 April 2008	Trustwave conduct an audit of Heartland and say it was *compliant with PCI*. [2]
May 2008	The hackers had *jumped to the processing* network[2]
October 2008	Visa first alerted Heartland about "*suspicious activities* surrounding certain cardholder accounts" - nearly one year later the attack
November 4, 2008	Carr's comments confirm that the PCI standards are minimal, and that the actual industry standard for security is much higher, complaint says.
2008/2009	Heartland called U.S. Secret Service and hired *two breach forensics teams to investigate*. [3]
January 12, 2009	Investigation led to the discovery of "suspicious files".
January 13, 2009	Heartland uncovered "malicious software that apparently had created those files."
January 20, 2009	Heartland's public disclosure, President Obama's inauguration day.
March 14, 2009	Visa removed Heartland from its published list of PCI-DSS compliant service providers.
March 19, 2009	Speech at the Global Security Summit hosted by Visa in Washington D.C, said that the Heartland data breach would not have occurred had the company had been vigilant about maintaining its PCI compliance.
April 2009	Heartland was re-certified as PCI compliant by an auditor.
August 4 2009	Carr stated that the company's end-to-end encryption project will offer merchants "the highest level of beta security in the marketplace. [6]
June 2012	The attackers were arrested in Sweden.
2015	Both attacker were extradited in the USA.

4 Risks and control weaknesses identified

During out analysis we have tried to retrieve all possible document, spacing from technical[7] to business reports[4]. After a careful analysis we started to make hypothesis about what went wrong at the time, how and who is/are the main responsible(s) of this event.
At the beginning, before reading the entire reportage, we were sure that only problem was the initial SQL injection vulnerability present in the old web page. However by carefully following the time-line is clear that employees would had enough time (about 5 months) to spot unusual network activity also by considering that the attackers had tried, for the entire period, to access the payment's network (probably with many attempts). In addition when they have detected the breach in the corporate network the attacker already had gained access to the payment's network.
It is obvious that something beyond the login page vulnerability have simplified the attackers work making their criminal plan to succeeded.
In this section we have tried to identify and aggregate major weakness and errors that could have prevented the data breach. Although a lot of disparate action might have blocked the attacker plan, we have selected and grouped the major problems that affected the company before and during the attack.

- **Lack of vulnerability check** : As described in the previous section, the attack started from a SQL injection, which still nowadays represent one of the most famous and exploited. Although the web login page targeted by the hackers was probably developed around 2001, at that time SQL injection was already well known to the world, so a process-payment company such as Heartland could not disregard it.
  By considering the size of the company, it would have been quite useful to use automated vulnerabilities scanning tools that could aware Heartland of code mistakes made on networks, web pages and all others software developed years before; because a serious policy should pay particular attention to old systems because is a well known fact that most of the cyber attacks start from the weakest part of the chain.
  In addition to automated tools would have been useful also hire some specialized auditor or penetration test teams to check weaknesses of company's system developed in the past, that probably were underestimated by Heartland as an access point for cyber attacks.
  Focusing on those weaknesses it is right to consider also the lack of a proper error checking mechanism. As a matter of fact during the entire attack many actions conducted by the hackers should have generated a large number of error messages, therefore it is quite impossible (as is written below in the logging system weakness paragraph) that no alarm was triggered when they tried to break the web page and the boundary of process-payment network.
  A working approach to mitigate this weakness that could be helpful consists of better training for the entire IT team. In fact to prevent this kind of code mistakes employees must be trained to use secure protocols, mechanisms, procedures and templates which are already widely tested and studied.

- **Network Monitoring** : Company clearly specified in the "Network Security" section of 2008's Form 10K that "*Our internal network configuration provides multiple layers of security to isolate our databases from unauthorized access and implements detailed security rules to limit access to all critical systems*". At first glance, this policy is reflected in the company's network separation between internal and payment processing networks. This makes attackers work more complicated because they need to overcome network boundaries in order to access critical services. In the end, this separation was very effective since hackers spent about five months trying to bypass defenses and avoiding anti-virus detection until they finally jumped into the processing network.
  While solution worked as intended network segmentation should not be used alone but supported with Intrusion Detection System (IDS) and strong firewall policies. Official documents do not explain how the attacker managed to break the security functionality, but the only useful information for this analysis is that company became aware that someone was able to access the network only on 13 November of 2009, approximately two years from the first time the web login vulnerability was exploited. By putting aside the malfunctioning logging process the main problem here was the fact that any of the present security software was able (or was not configured) to generate an alert to the network admin.
  Although the attackers studied various method to avoid detection, during the entire period when they were present in the network they used a backdoor that "beacon" periodically to their command and control servers (C&C), allowing easy access to the compromised networks. While the sniffer software was passive and therefore nearly impossible to spot with network monitor tool, unusual traffic either directed to the network boundaries or to the C&C external server should have been spotted by network security solutions.
  Consequently, since the company specified that they regularly performed software and anti-virus definition updates[5] probably the network monitor software was inadequate or was not configured properly to alert the security responsible.
  To conclude even though is extremely difficult to create an impenetrable boundary, possible attack can be immediately detected with the appropriate tool and then countermeasures could be taken.

- **Weak Password Policy** : Weak passwords are probably the major responsible of company breaches and therefore are a curse in computer security. Even the most impenetrable company may be in danger if one of their employees use an easily guessable password. In fact, a weak password leaves an open door to the internal network, making the boundaries protection useless.
  In this case study, FBI Advisory [7] declared that "*Hackers obtained valid Windows credentials by using fgdump or a similar tool*". As stated in the previous section they extracted NTML hashes and started to crack them in order to obtain some valid credentials. Since hashes are designed to be impossible to invert (in other words discover the password), cracking a single one would require an unsustainable amount of time. The only applicable option is to build up a dictionary containing

the most common password and try each of them.
As a result only what is considered n the previous section they extracted NTML hashes and started to crack them in order to obtain some valid credentials. Since hashes are designed to be impossible to invert (in other words discover the password), cracking a single one would require an unsustainable amount of time. The only applicable option is to build up a dictionary containing the most common password and try each of them. As a result only what is considered "weak passwords" can be cracked in short time. Obviously since the attackers managed to obtain credentials, probably at the time Heartland did not enforce a comprehensive password policy.
One of the simple countermeasure to this phenomena consists in maintaining a blacklist of most common password, like the one drafted by the National Cyber Security Centre (NCSC)[4], in order to avoid their usage. Even though blacklist seems effective, they are not a reliable solution. For example, a secretary may use their child, pet name or a combination of them, which is very likely to not be present in the list but anyway is simply guessable with a bit of social engineering. Therefore one of the main weapons against password guessing is employees training. Only when they gain awareness of the importance of password as a security mechanism effective policies can be applied, otherwise, nobody is going to follow them.

- **Inadequate company services and infrastructures awareness** : This section slightly differs from the "Lack of vulnerability check" (4), while the latter is related to security scans and audits of software this one focuses on code review and on system patches and maintenance processes. PCI-DSS compliance extensively cover the recommended guidelines for software security in requirement number 6, under the name "*Develop and maintain secure systems and applications*"[10].
  According to what is written in the introduction is likely to believe that Heartland ran a "Microsoft SQL Server 2000" at the time. It is known that this version allows the execution of "xp_cmdshell" only if the server runs with administrative privilege. Point 6.2 of PCI states that all software should install all vendor security update within one month. Despite newer version of SQL Server were released by Microsoft (2003, 2005, 2008) no critical CVE was present[5] on that version before the July of 2008 which is in accordance with the audit performed by Trustwave in April.
  Moreover the PCI documents only refer to the "*least-privilege*" principles only in human terms and exclusively when cardholder data are involved[6], which justifies why the auditors did not warn about the fact that the database software runs with administrative privilege.
  On the other hand, when looking at the web-login page, the PCI clearly states on the point 6.6 that "*For public-facing web applications, ... reviewing applications via manual or automated application vulnerability security assessment tools or methods, at least annually, ... Installing an automated technical solution that detects and prevents web-based attacks"*. In this case, the policy was not applied since a simple review would have spotted the lack of sanitation on user input and migrated to a modern solution (like SQL prepared statements). Furthermore (from what is publicly available) no sort of "web application firewall" (WAF) was present at the time. Such software is great to filter dangerous user input and can also be configured to alert the system administrator if suspicious activity occurs.
  To conclude, while the choice of maintaining an old (but still supported) software may be comprehensible, whereas the absence of a periodic software review and the lack of a WAF significantly facilitate the attacker works.
- **Absence of a reliable and complete logging system and log-review process** : Logging systems are a key component of the company infrastructure since they provide a comprehensive description of events that occurred and therefore may help to troubleshoot. In addition, an exhaustive log file can be used for various activities, in particular for security incident response and forensics, so presumably, at the time Heartland's logs were not so well-designed since employees were not capable of understanding how the attackers got into the network until an external forensic team was engaged.
  The PCI-DSS standard includes a logging policy in the "*Requirement 10*"[10] which instruct about what information must be logged, where logs should be stored and even requires a regular log review process executed either by personnel or automated. In particular for each event related to a system component "*user identification, type of event, date and time, success or failure indication,*

[4] NCSC Common password report: https://www.ncsc.gov.uk/news/mosthacked-passwordsrevealedasukcybersurveyexposesgapsinonlinesecurity
[5] MSSQL 2000 CVE: https://www.cvedetails.com/vulnerabilitylist/vendor_id26/product_id251/version_id-57840/MicrosoftSqlServer2000.html
[6] Requirements 7: "*Restrict access to cardholder data by business need to know*"

origination of event, and identity or name of affected data, system component or resource"[10] have to be stored.
During the entire period of the attack when the hackers worked undisturbed inside the company infrastructure a security team with a PCI-compliant log should have been capable of noticing some strange events in the periodic log review process.
It is not clear why despite Heartland was PCI compliant nobody inside the company realized what it was happening. One possible explanation is that the work was left to an automated process which failed to detect the breach.
However, the seriousness of the situation concerns the company event response. While the hackers managed to jump into the processing network, Heartland finally discovered the breach of the corporate network but "*was unaware the hackers were sitting on its system for months conducting reconnaissance.*"[2]. employees were not able to spot the thieves presence even though by the network activity log should contain some evidence. Since no further investigation was performed, the attackers jumped into the processing network and, only after VISA alerted (one year after the initial attack) about some "suspicious activity" the company finally managed to engage two forensics team.
If some sort of logging review process were performed periodically at the time, probably unusual activities, like the ones generated by the malicious software or in general by the two hackers, would have been discovered and some action might have been taken in place (like temporarily suspend payments until a complete audit).

- **Lack of encryption on sensitive data** : Inside the Form 10K, the company explicitly stated that "cardholder numbers that are stored in our databases are encrypted using triple-DES protocols" and in this sense the company made a valid choice considering that at the time the used cipher was the highest commercially available standard for encryption. This policy definitely prevented the attacker from exfiltrating more sensitive data that could have caused a serious data breach that the one happened.
  The company has correctly applied the "*encryption at rest*" however for some reason they forgot to protect some important data that used to transit in the payment processing network. After the attackers have studied packets dump generated by the sniffer they discovered that digital information encoded onto the magnetic present on the backs of credit and debit cards transited in clear text.
  With such data, criminals can forge counterfeit credit cards by simply impressing on them the stolen information. Nowadays the technology of credit card makes difficult to forge a valid card with those information[8], but at the time the illegal market of counterfeit cards was very profitable, according to the Nilson Report[9] worldwide losses from card fraud was about $8 billion in 2010. So the problem to highlight here is the lack of "*encryption in transit*". It is not possible to say without knowing the company's infrastructure if other sensitive information transit through the network protected with encryption, therefore is difficult to determine if the policy is only focused on data at rest. By examining the PCI guidelines (6) it is possible to see that data like the one inserted into the magnetic stripes and customers PIN cannot be stored anywhere for security reason. Though since no PINs code were stolen this means that they probably travel on another network or was just encrypted. Definitively the only indisputable statement is that the company failed to enforce their sensitive information policy, allowing unencrypted flow of critical data across the internal network. In our opinion, a simple inventory of the company data flow (like what information applications exchange) would have been enough to spot the implementation weakness. Others action like external audit was not sufficient because of the amount of network traffic data that expert had (probably) analyzed. In this sense even a powerful network logging software which is able to. determine if sensitive data transit might spot the issue, but this solution is probably more expensive than having a clear and complete data flow report.

- **Absence of an explicit and clear cyber security policy** : It is almost clear that Heartland, although were PCI-DSS compliant and inside Form 10K claimed that they carried out an annual SAS-70 review, they did not have a specific and complete Cyber Security policy.
  This clearly was the main problem that lead the company to such impressive breach. All of the weaknesses described above are just pixels of a big picture that form a more complete policy able to detect, protect, prevent and mitigate the damage produced by the breach.
  Having a Cyber Security policy means that Heartland had to check its networks, encryption mechanisms and log systems, check if all the software installed were properly updated or if unusual traffic inside its networks appears.

Guidelines for Cardholder Data Elements

	Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
Sensitive Authentication Data[1]	Full Track Data[2]	No	Cannot store per Requirement 3.2
	CAV2/CVC2/CVV2/CID[3]	No	Cannot store per Requirement 3.2
	PIN/PIN Block[4]	No	Cannot store per Requirement 3.2

[1] Sensitive authentication data must not be stored after authorization (even if encrypted)
[2] Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.
[3] The three- or four-digit value printed on the front or back of a payment card
[4] Personal Identification Number entered by cardholder during a transaction, and/or encrypted PIN block present within the transaction message

Figure 6: PCI-DSS specificaton for storing sensitive data

After analyzing all the available documents we understood that Heartland were conscious about risks of a cyber attack but nonetheless, they did not built a concrete plan to prevent and mitigate the attack. As a matter of fact it only became aware of the breach after eight months and exclusively after Visa alerted it of suspicious payment activities.
In addition to the weaknesses already described, an improper application of the principles of "*least privilege*", which constitute one of the fundamental principle of software and organization security, was present. Furthermore the absence of either external or internal penetration tests could have been aware Heartland of vulnerabilities such as the SQL injection or the absence of a complete logging system.
To conclude another important company behavior that favored the huge amount of data leak was the, not taken, decision to temporary stop their system for further investigation on the event. Though this would have caused some financial loss, the consequences would have been far less catastrophic than the current one. Hence a better risk management policy that requires to halt system on security breaches would have surely limited the damages.

5 Framworks Analysis

5.1 NIST Framework

The NIST framework is a collection of computer security policies directed to a private organization which aims to improve their countermeasure against cyber attacks. The framework is composed by three parts, namely the "*Core*", which contains a set of various aspects and approaches to cyber-security, the "*Profile*", which basically is the list of outcomes chose by the organization based on their needs and, finally, the "*Tiers*", which specifies organization's view of cyber-security risks and how they approach them. The following analysis is focused on the "Core" since the other two parts are related to a business decision and would not be so valuable for the purposes of this

Figure 7: NIST Five functions

work.

The core is again divided into five functions and, as stated in the official documentation, "*They act as the backbone of the Framework Core that all other elements are organized around*"[7]. The functions are[8]:

- **Identify**: managing cyber-security risk to systems, people, assets, data, and capabilities.
- **Protect**: plans appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect**: defines the appropriate activities to identify the occurrence of a cyber-security event.
- **Respond**: includes appropriate activities to take action regarding a detected cyber-security incident.
- **Recover**: identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security incident.

Our choice fell on this framework due to its characteristic of having, for each element, an extensive reference to a variety of other frameworks (like ISO-27001) , allowing for a better comparison with the next one (SANS-CIS).
In addition, we have discovered that the official Italian cyber-security framework was inspired by the NIST[9] so this seems to us the most educative choice.

5.1.1 How could have *prevented* hackers breach?

The NIST framework study is started by listing some controls that might have prevented the breach in various ways, from the identification of software to incident response. Despite those controls alone would have only slowed down the attackers, a whole and correct application of them would have hardened Heartland's infrastructure.

ID	**Summary**.
ID.AM-2	Software platforms and applications within the organization are inventoried.
ID.RA-1	Asset vulnerabilities are identified and documented.
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles.
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
DE.DP-2	Detection activities comply with all applicable requirements.
DE.CM-4	Malicious code is detected.
DE.CM-8	Vulnerability scans are performed.
RS.AN-2	The impact of the incident is understood.
RS.MI-2	Incidents are mitigated.

To begin with, the outcomes that belong to the "Identify" function is presented. The fact that the company still used a near decade-old software is already described in the weakness section(4). By combining `ID:AM-2` with `ID.RA-1` Heartland would have been created a detailed ledger of installed application with their relative know vulnerabilities listed, which might have worried some executive.

[7] Official Training: https://www.nist.gov/cyberframework/onlinelearning/fivefunctions
[8] Description are taken from the official training
[9] Italian Cybersecurity Framework website: https://www.cybersecurityframework.it/

From a more technical perspective, despite the presence of a vulnerability in the web login form, hackers would not have caused so much damage if the database software did not run with administrative privilege. That is why a policy that enforced the usage of PR.IP-1, with a particular attention to the principle of "least functionality" (PR.AC-4 and PR-PT-3), would have limited intruder capabilities.

After that the controls that would have "contained" the breach after the Heartland discovered the intrusion for the first time between 2007 and 2008[2].
First of all, once the breach was detected, employees believed that hackers were confined into the internal network while in reality they already gained access to the payment network. In this case, if company members were specifically trained to deal with this situation, like the policy RS.AN-2 requires, the network would have been immediately halted consequently causing mitigated damage in accordance with RS.MI-2.

To conclude, when the breach was initially discovered, an effective application of DE.CM-4 and DE.CM-8 would have spotted both the presence of intruders in the payment network and the weakness that they had exploited. Instead, external security auditors were engaged and (unsurprisingly) failed to observe any strange event.

5.1.2 How could have *detected* the breach?

Obviously, this section heavily relies on the "Detect" function, even though two elements belonging to "Protect" and "Respond" were chosen.
The heartland lack of a reliable logging system has been already discussed earlier (4) just like the ineffective network monitoring tool (4). In the following table, we have selected the most fitting outcomes that would have detected the data breach.

ID	Summary.
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.
DE.AE-2	Detected events are analyzed to understand attack targets and methods.
DE.CM-1	The network is monitored to detect potential cyber-security events.
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
DE.DP-2	Detection activities comply with all applicable requirements.
RS.MI-1	Incidents are contained.

By analyzing the event according to their temporal order, applying the DE.CM-1 and DE.AE-10 policies would have drastically changed the attack result. When the web login page was exploited the first time, a network monitor would have immediately detected the injection and then, considering that requirement PR.PT-1 imposes well-designed logging system, the event would have been rapidly studied to identify and (subsequently) patch the vulnerability. At the same time once a cyber-security breach is detected, following the RS.MI-1 would have required the company to temporarily halt their system until further investigation ensures that every exploited vulnerability has been patched and that no backdoor is present. In our case study, a premature detection would for sure changed the course of the event since Heartland's executive might consequently have improved their security policies (DE.DP-2).
If the criminals managed to elude the network monitor on the exploitation of the web vulnerability, other alarms should have been triggered. When the attackers conducted reconnaissance on the internal network a monitor which follows the requirements of DE.CM-7 would immediately detect something like a port scanning coming from database host.
Lastly, a clear and detailed set of allowed network operation specific for each connection, devices or software

(as specified in DE.AE-1) would, without doubt, immediately expose flaw which allowed sensitive cardholder data to flew in clear-text across the payment processing network.

5.2 How could have *protected* the stolen data?

This section, which is entirely composed by outcomes belonging to the "Protection" function, focuses on ways that Heartland could have used to keep critical data safe.

ID	Summary.
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
PR.DS-2	Data-in-transit is protected.
PR.DS-5	Protections against data leaks are implemented.
PR.AT-1	All users are informed and trained.

Firstly the weak authentication policy is studied. In the "Weak Password Policy" section (4) is explained that the hackers managed to obtain valid credential only because some system had used a weak password. By studying the PCI-DSS compliance it is noticed that only an obscene password security policy is present. The very last version of the standard [10] states[10] that a password must be "*at minimum length of at least seven characters*" which could be cracked in few hours by a modern computer. [11]). In addition it also specifies that password must be changed at least once every 90 days, while nowadays this is considered very bad practice since often the new password is easily-guessable.[12] With such password policies, it is clear how hackers succeed in finding valid credential.
In contrast, NIST framework takes credentials very seriously. Firstly the policy PR.AT-1 requires that employees must be trained on security best-practices, such as password complexity rules, while on PR.AC-7 is suggested to strengthen the authentication mechanism according to the user privileges and roles (like implementing multi-factor authentication). The final policy regarding password is PR.AC-1 that put strict control on identities by forcing them to be issued, verified and revoked for various entities, such as devices, users and even processes.

After that the approach of NIST against sensitive communication is analyzed. As written above (4) the lack of a precise assets data flow scheme was the main responsible for the transit of un-encrypted data through the internal network. In addition, the PCI-DSS instruct about weak security protection which focuses on segmenting the network[10][13] where cardholder data transit but say nothing about encryption[14]. This security approach is entirely based on the assumption that an attacker would not have been able to access the process-payment network and was very likely to be the big mistake the company has done. Any serious security audit (apart from the PCI-DSS compliance) would have been reported a critical flaw like this one. Also, in this case, NIST framework would have corrected the problems. With the PR.DS-5 even if hackers managed to steal sensitive data they would not have been able to retrieve them since external connection would not be allowed in the restricted network. For example, a simple whitelist of allowed IPs address would have stopped them from using their own server to store malware and data[13]. Despite these various techniques exists to exfiltrate data out of a protected network. Instead, the real policy that would have completely stopped the thieves is R.DS-2, which demands that all the data in transit should be encrypted.

[10] In section 8.2.3, 8.2.4
[11] According to this site which also considers the computational power in 2007: https://www.betterbuys.com/estimating-password-cracking-times/
[12] Government Article link
[13] In "*Network Segmentation*" paragraph
[14] The only required encryption is when data transit over public network (Requirement 4).

5.3 SANS Framework - CIS Controls

The "Critical Security Controls for Effective Cyber Defense" (CIS Controls)[15] is claimed to be a leading framework used in cyber security assessments.
The CIS Controls are a prioritized set of actions that collectively form defense-in-depth guidelines of best practices that mitigate the most common attacks against systems and networks. One of the main characteristics of the CIS Controls is they are developed by experts based on their first-hand experience in the security field and are derived from actual threat data from a variety of public and private sources. Also, in addition to being prioritized and relevant, they are regularly updated to stay in step with the cybersecurity's ever-changing threat environment.
What should be understood about CIS Controls is that is not a one-size-fits-all solution, in either content or priority.
Who decides to follow this set of rules has to understand what is critical to its business, data, systems, networks, and infrastructures, and it has to consider the adversary actions that could impact its business. This means that by following these criteria we started filtering each subcategory of the 20 controls listed, choosing which controls suited better to Heartland case.

5.3.1 How could have *prevented* hackers breach?

"Prevent" means keeping something from occurring, so results quite obvious that CIS Controls chosen for this section have the aim of taking actions and adopt behaviors before something bad happens.
As we properly analyzed in Risk and control weaknesses section (4) to prevent the breach Heartland should have implemented a complete cyber-security policy achieving consequently a better knowledge of their entire infrastructure.
In the table below CIS Controls that better describe the actions and decisions that should have been made to prevent the breach are presented.

ID	**Summary**.
2.8	Implement Application Whitelisting of Libraries.
2.9	Implement Application Whitelisting of Scripts.
3.1	Run Automated Vulnerability Scanning Tools.
16.3	Require Multi-factor Authentication.
18.2	Ensure Explicit Error Checking is Performed for All In-house Developed Software.
18.6	Ensure Software Development Personnel are Trained in Secure Coding.
18.10	Deploy Web Application Firewalls.
18.11	Use Standard Hardening Configuration Templates for Databases.
20.2	Conduct Regular External and Internal Penetration Tests.

`Control 2.8` and `2.9` are widespread techniques used to limit the diffusion of malware inside a network and single devices due to the fact that only the execution of trusted scripts and libraries is allowed, preventing malicious code from performing harmful actions. On the other hand `Control 3.1, 18.6, 18.11` could have prevented the initial SQL injection which started the entire attack. In addition to that, it could also be considered useful the `control 20.2` because almost surely a well-done and comprehensive penetration test, maybe led by some external team, could have notified Heartland about the various already discussed weaknesses that afflict the entire system. `Control 18.10` instead might have blocked the SQL injection exploitation since WAFs are instructed to spot and deny unusual request, such as the one

[15] Offical description of the framework is taken from https://www.defensis.it/ecms/file/CISControlsVersion7.pdf

generated during a SQL injection, along with high traffic load.
To conclude, `control 16.3` would have been secured assets login, preventing hackers from gaining access to the system just by cracking passwords, in fact with such mechanism an additional authentication layer is necessary to gain access.

5.3.2 How could have *detected* the breach?

As was done for the NIST framework in this section the CIS Controls that could have detected the hacker's intrusion inside the system have been chosen, and all the other problems arisen from this are briefly described.

ID	**Summary**.
6.3	Enable Detailed Logging.
6.7	Regularly Review Logs.
9.2	Ensure Only Approved Ports, Protocols and Services Are Running.
9.4	Apply Host-based Firewalls or Port Filtering.
12.2	Scan for Unauthorized Connections.
12.5	Configure Monitoring Systems to Record Network Packets.
12.8	Deploy NetFlow Collection on Networking Boundary Devices.
13.3	Monitor and Block Unauthorized Network Traffic.
16.13	Alert on Account Login Behavior Deviation.

`Control 6.3 and 6.7` belong to the absence of a complete logging system (4) and suggest to include detailed information such as an event source, date, source and destination address within the log of each host of the network. It is emphasized also to check regularly the logs generated to detect if there were any malicious attempt to enter inside the system and corrupt it. As a matter of fact, CIS Controls guidelines suggest to configure servers inside the network in order to create access control logs when a user attempts to access resources without the appropriate privileges.
Usually, attackers search for remotely accessible network services that are vulnerable to exploitation. `Control 9.2 and 9.4` highlight the importance to take note of which ports and protocols are really necessary to make the system work and to apply a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. Always within network weaknesses `control 12.2, 12.5 and 12.8` focus their attention on boundaries, which usually are the Achilles heel of network infrastructures. Therefore check and log the traffic on boundaries could have prevented and detected the attack especially when the hackers tried to pass from one network to the other.
Even if the asset of `control 13.3` is "data" and not even more "network" also this one emphasized the importance of examining packets that pass through network perimeters, maybe by developing an automated tool that blocks traffic of sensitive data and alerts immediately when this happens. Indeed it is important that an organization, such as Heartland, understand what its sensitive information is, where it resides, and who needs access to it. Although once the hackers were inside the network many actions could have done to obfuscate the data stolen, adopting `control 13.3 and 16.13` together would have made the life of the attackers really hard. As a matter of fact, monitoring the behavior of logged account would have notified an abnormal time-of-day or workstation location and duration of user activities controlled by the hackers.

5.3.3 How could have *protected* the stolen data?

In case that the attackers managed to enter anyway inside Heartland systems even with all the previous controls properly implemented, CIS Controls suggests the correct behaviour in order to protect data from malicious entities.

ID	Summary.
4.4	Use Unique Passwords.
14.4	Encrypt All Sensitive Information in Transit.

As a matter of fact `control 4.4` could have been useful as an alternative of multi-factor authentication where this was not supported. Adopt "unique" password means do not use the same password for all the services and resources of the system, which is one of the most widespread advice in the field of cybersecurity.
Definitely seen how the attack actually happened and how the data was stolen the `control 14.4` surely has mitigated the damage of the breach. Although the information in transit during payment processes might have been stolen in any case, the use of a proper encryption algorithm always raises the level of security of an entire system. As mentioned above PCI DSS standard does not say anything about data encryption leaving a big hole in the security of a system.

6 Framework Comparison

After using both frameworks on the Heartland case we have identified major benefits and drawback of each one.
The NIST framework is widely developed and applied all over the world by huge corporation[16] and therefore results more complete and specific; appropriate for large companies that can afford an entire security team. In fact, due to its length and verbosity, a medium/small company who chose to adopt it may start a very time-consuming and resource-intensive review application process.
Despite it is divided into five macro-categories, which may seem to make it clearer, subcategories do not contain a brief explanation but instead, a lot of references to other standards (like SANS, ISO27001) are provided, making the decision process very tedious. Detailed description are contained in an external document (NIST SP 800-53[17]) which precisely describe every aspect and action to carry on in order to accomplish the standard.

On the other hand, the CIS Controls framework is divided into twenty specific categories that contain various "*sub-controls*". For each of them, the relative asset is made explicit along with its security function and a short description. Differently from the previous one, at the end of each category, there is a "Procedure and Tools" section which explains, without being too technical, how to accomplish the control. This makes it easier to understand and implement without too much effort, which suits-well for those who cannot afford a specialized cyber-security team.

To conclude as far as we concerned both frameworks would have been helpful for Heartland case at the time. The reality is that the company lacked of a concrete cyber-security policy and were only aware of the possible risks involved. This catches the executives unprepared and unable to take the correct decision which would have either prevent or mitigate the breach.

[16] NIST Success stories https://www.nist.gov/cyberframework/successstories
[17] Official Link: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.80053r4.pdf

7 Conclusion

Heartland data breach is probably one of the largest leak of credit card data ever, but at the same time is also a valid example of how security policy should be implemented. The huge mistake that caused the event was believing that a standard like the PCI-DSS, which is not intended to provide an extensive cybersecurity prevention platform. Instead, applying a well-designed framework as the one studied (5) would have definitely improved the situation.
After the 2008, incident the company started to take security very seriously. They have been re-listed in VISA PCI compliant service providers and even calling standard for encryption within the payment industry[6]. However, on 8 May 2015, they suffered a break-in at the company's offices in Santa Ana, California. This time no sensitive data was officially stolen and Heartland responded quickly to the customers with a clear advisory[14]. To conclude, although the presented facts may seem an old story, nowadays the cybersecurity world is still affected by what happened about 10 years ago.
Recently a huge dump of credentials which counts nearly 2.2 billion entries started to circulate on the dark web forum and expert states that some of the data is related to the Heartland breach of 2008[15], which demonstrate how consequences of a data breach could persist for a long time.

References

[1] Linda McGlasson Heartland Breach: Inside Look at the Plaintiffs' Case URL: https://www.bankinfosecurity.com/heartlandbreachinsidelookatplaintiffscasea1844 October 8, 2009

[2] Kim ZetterKim Zetter TJX Hacker Charged With Heartland, Hannaford Breaches URL: https://www.wired.com/2009/08/tjx-hacker-charged-with-heartland/ August 17, 2009

[3] Brian Krebs Payment Processor Breach May Be Largest Ever URL: *http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html?hpid=topnews* January 20, 2009

[4] HEARTLAND PAYMENT SYSTEMS, INC. FORM 10-K URL: https://last10k.com/sec-filings/1144354/000119312508051380/d10k.htm.pdf

[5] HEARTLAND PAYMENT SYSTEMS, INC. FORM 10-K - Network Security URL: https://last10k.com/sec-filings/1144354/000119312508051380/d10k.htm.pdf Page 23

[6] Linda McGlasson Heartland Data Breach: Is End-to-End Encryption the Answer? URL: *https://www.bankinfosecurity.com/heartland-data-breach-end-to-end-encryption-answer-a-1455* May 11, 2009

[7] Joint USSS/FBI Advisory URL: "*20090212-usss_fbi_advisory.pdf*"

[8] Matthew Cochrane Why U.S. Counterfeit Credit Card Fraud Is Down 75% URL: https://www.fool.com/investing/2018/09/16/why-us-counterfeit-credit-card-fraud-is-down-75.aspx

[9] Nilson Report Card Fraud Worldwide URL : *https://nilsonreport.com/content_promo.phpid_promo=8* Direct Download: *https://www.nilsonreport.com/upload/content_promo/The_Nilson_Report_1017-2016.pdf*

[10] PCI DSS PCI-DSS v3.2.1 URL: *https://www.pcisecuritystandards.org/documents/PCI_DSSQRG-v3_2_1.pdf*

[11] Jaikumar Vijayan Heartland breach expenses pegged at $140M – so far URL: *https://www.computerworld.com/article/2518328/heartland-breach-expenses-pegged-at–140m—-so-far.html*

[12] NIST NIST SP 800-63B-3 URL: *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf*

[13] UNITED STATES DISTRICT COURTDISTRICT OF NEW JERSEY 18 U.S.C. § 371 URL: https://www.wired.com/images_blogs/threatlevel/2009/08/gonzalez.pdf

[14] Heartland URL: https://oag.ca.gov/system/files/Heartland%20Payment%20Systems%20Ad%20r1fin_0.pdf

[15] Scott Ikeda The Data Dump of 2.2 Billion Breached Accounts: What You Need to Know URL: https://www.cpomagazine.com/cyber-security/the-data-dump-of-2-2-billion-breached-accounts-what-you-need-to-know 9 Feb 2019

[16] Kevin Judge The Heartland Breach: A Cautionary Tale for E-Commerce URL: https://blog.comodo.com/e-commerce/theheartlandbreachacautionarytaleforecommerce/ 15 Oct 2013