University of Rome “La Sapienza”

MSc. in Cybersecurity

Ethical Hacking course

A.Y. 2018/2019

Governance, management and audit in Cybersecurity: The Heathland Payment System case study and analysis

by

Cristina Bottoni ID. 1632035

Abu Jafor Mohammad Saleh ID. 1469151

“It is only when they go wrong that machines remind you how powerful they are”

Clive James

Executive summary: The paper aims at analysing the Heartland Payment System’s case as one of the biggest and most relevant cases of data security breach and personal data breach. The work will initially describe the case providing some background history on the fact, in order to allow the reader to gain a clear understanding of the matter at hand. Secondly, the paper will identify the assets which have been compromised and the vulnerabilities that made the attack possible. By analysing the control weaknesses that have exposed the company to those above-mentioned vulnerabilities, the writers will provide some detailed response and prevention strategies using information security standards and frameworks (such as ISO and NIST). The report will finally debate on the pros and cons of such documents, highlighting their points of weakness and strength referring to the case of Heartland Payments System.

TABLE OF CONTENTS

1 Introduction

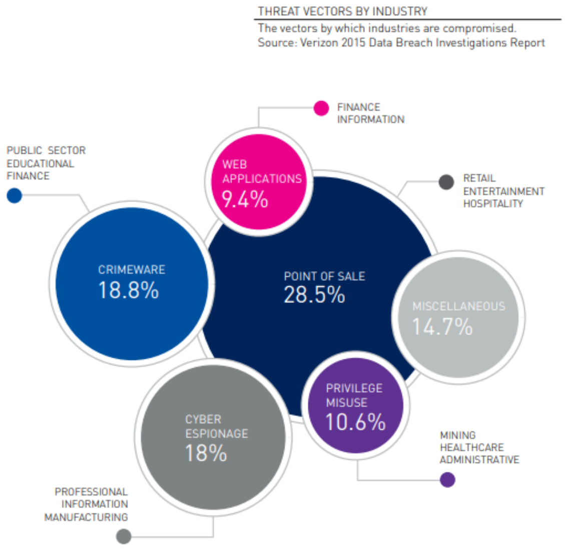
1.1 Cybersecurity in today's world

The concept of cybersecurity nowadays is spreading fast around the globe and with it also everything that the idea of new entails: fears, questions, doubts but also innovations, development and investments.

The meaning is it not very difficult to understand: it surely means "to stay secure, safe". But safe from what? What is this "cyber" that we need to stay safe from? Most people have a rough and general idea of what the cyber world is, but not many people really understand its specific meaning. Nowadays, everything is "cyber". Banks are online (and with them bank accounts as well), personal and professional information are online, newspapers are online, pictures are online, transactions are online, political ideas are online. In order to be able to fully manage this huge amount of crucial and delicate information, people need to be aware of the laws regulating the cyberworld, they must be aware of practices, of dangers, the dos and don'ts, and, in order not to be too pessimistic, of opportunities. Since almost half of the world's population is connected to the internet, and the dependence (and the interdependence) that everybody is experiencing thanks to this innovative, challenging and affordable cyberspace, the risk of people trying to exploit these factors is what is known nowadays as **cybercrime**.

Cybercrime takes place in actions such as stealing data and information, frauds or shutting down websites and service providers.

When the newspapers report of the last multinational company or bank robbery, of the cracking of thousands of passwords and credentials or of the disservices of a certain local or international service provider we are just referring to **lack of cybersecurity**: that is, in other words, "*a failure to protect computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation*".[1] The consequences, for this kind of "oversight", can result in significant financial or operational harm both from the company and its clients.



THREAT VECTORS BY INDUSTRY
The vectors by which industries are compromised.
Source: Verizon 2015 Data Breach Investigations Report

After this brief introduction, it is clear that cybersecurity nowadays cannot be considered as an option anymore. Cybersecurity, and its implementation, is something that must be fundamental when building or updating the skeleton of one company.

[1] https://economictimes.indiatimes.com/definition/cyber-security "Definition of Cybersecurity", The Economic Times.

1.2 Brief history on the Heartland Payments System case

Before starting to analyse the case at hand, it is fundamental to provide some background history on the Heartland Payments System as to have a better understanding of the company, its field of activities, its structural organization and its main components.

The Heartland Payments Systems Inc. is an international provider of technology and payment processing, as well as software solutions delivering, founded in 1997 in Princeton, New Jersey.[2] Currently, the company provides payments processing to more than 300,000 clients in the United States for a total of more than 11 million transactions per day which result in a total of 80 billion US dollars per year.[3]

There have been three fundamental years in the history of the Heartland Payments System:

1. The first one, **between December 2015 and April 2016**, the company was acquired by another payment processor, the Global Payments, at the price of 3.5 billion of dollars, and moved its headquarters in Edmond, Oklahoma,
2. The second one, **in 2014**, when the Nilson Report announced the Heartland to be the 6th largest payment processor in the United States by transaction count and the 8th payment processing company in the world for processed dollar volume,
3. The last one, unfortunately not as remarkable as the previous two, **in January 2009**, the Heartland was victim of one of the biggest cases of data security breaches in US history, with thousands of data and cardholders' information stolen.

In the following pages, we will talk more in depth about the last point, which will be the object of our analysis regarding the Heartland Payments System.

Before doing that, it is interesting to mention some relevant innovations that have seen the company as leader and promoter during the years.

In fact, on May 24, 2009, the Heartland launched their new technology called E3 solution, an end-to-end encryption model to safeguard credit and debit card account information in the very moment of the card swipe when paying. The Heartland has been one of the first companies in the US who put the first effort in planning the end-to-end encryption technology, followed by other processors such as Worldpay US and several First Data ISO's.

Therefore, in October 2013, the CEO of Heartland Bob Carr published an open letter denouncing the unethical and the dishonest pricing practices in the payment processing sector, in support for a transparent and fair way of processing transactions from international providers.

Finally, in May 2014, the Heartland Payments System launched the Heartland Secure initiative, aiming at providing merchants with more security and protection from stolen card data.

[2] https://www.heartlandpaymentsystems.com/about-us Heartland Payments System official website

[3] https://en.wikipedia.org/wiki/Heartland_Payment_Systems Heartland Payments System

1.3 Presentation and description of the case

As mentioned before, one of the fundamental moments for the Heartland Payments System has been the year 2009, when the company has been the victim of one of the most important data and personal cardholder information breaches of history. The breaches included also the digital information contained in the magnetic part of the debit and credit cards, which have been recorded and stolen in the very moment of the swipe of the card. Once gained this kind of information, thieves can simply copy this information on other prefabricated cards and freely use those cards as if they were the real owners. In terms of numbers, around 100 million cards were stolen, and more than 650 financial companies were compromised.

The main responsible of these activities was an American computer hacker, Albert Gonzalez, who gained, thanks to his illicit activities, 20 years of jail starting from 2010. According to SC magazine, it was the longest penalty ever given for cybercrime. For the Heartland side, the company declared to have lost a total of 12.5 million dollars, in terms of clients, financial loss and legal fees.[4] The Hacker Albert Gonzalez was also responsible for other attacks on other companies such as TJX, Hannaford, a grocery store chain, and 7-Eleven, a convenience store chain. In the TJX case, Gonzalez was able to crack data from 45.6 million debit and credit cards' numbers in around one year and a half.

As soon as Heartland found out that there had been a SQL injection in their systems and that the malware was causing problems to both private clients and companies, in terms of not allowed or never executed payments, they immediately contacted the US Secret Services and the Department of Justice, in order to keep the damage contained. The interesting fact was that no merchant data or cardholder Social Security numbers, unencrypted personal identification numbers (PIN), addresses or telephone numbers were involved in the breach.[5]

2 Analysis of the case

After having provided the reader with some basic knowledge about the history of the attacked company and the case under study, it is important to take an active part in the analysis of the case by going deeper in the understanding of the actions of the company that made the attack possible.

In the second chapter, we will try to give a more technical insight on which choices led to certain disastrous consequences for the Heartland Payments System and on how sometimes the lack of control that may seem a trivial issue can bring much more problems than expected.

[4] https://en.wikipedia.org/wiki/Albert_Gonzalez#Heartland_Payment_Systems Albert Gonzalez

[5] https://www.bankinfosecurity.com/heartland-payment-systems-forcht-bank-discover-data-breaches-a-1168 "Heartland Payment Systems, Forcht Bank Discover Data Breaches" Linda McGlasson, January 21, 2009

First, we will give a second reading on the case, no more only by stating facts as in the previous chapter but also by separating positive facts from negative facts, in order to build a more critical analysis on one of the biggest cyber attacks of the history.
Second, we are going to analyse which have been the main compromised assets and processes during and after the attack, and which have been the most impacted sectors of the company, in terms of loss of money, credibility, trust and availability of services.
Thirdly, the second chapter will deal with the identification of the cybersecurity control weaknesses present in the company that made the attack possible. The analysis will then go further with providing some solutions for Heartland but also for all private and public bodies from each sector and continent of the world which can also be subject to future attacks. The evidence of these proposed solutions will be found in some international information security standards, frameworks or best practices that we are going to present in the chapter such as the ones of the International Organization for Standardization IS0 27001 and 27002 and the National Institute of Standards and Technology.
The chapter will finally provide a comparative analysis on the pros and cons of each chosen framework, to understand which one would be applied in the best way and where.

2.1 Critical analysis of the event

After having read and understood the main developments of the case of data and information breach of the Heartland Payments System, it is important, before starting to count the compromised assets and processes, to understand which of the facts happened to the company during the year 2008 and 2009 can be counted as positive and which facts should be considered as the cause of this attack.
It is important, when carrying out a detailed and critical analysis of a case, not to limit your comprehension of the case only to a general understanding of the events, because in this way it will not be possible to have a clear and detail picture of the situation, but only a partial image, that may lead to a loss of some important information on the development of the events. In most cases, this can have catastrophic consequences, especially when you are trying to solve an important case and you cannot allow yourself to make mistakes: many lives depend on the outcome of the analysis, particularly when you cover a role that entails many responsibilities. In carrying out the analysis of this case, we imagined to be a team of experts in the Information Security department of the United Nation, a role that we aim to reach in our future career. In fact, when covering positions of great decisional power, you cannot allow yourself and your team to make evaluation mistakes in terms of money, assets, human resources, external people affected.
In order to be as complete as possible, we decided to spend a few lines of our work in classifying the facts that happened to the company in negative and positive elements, as to understand deeply the ex-ante conditions which may have led or have facilitated the attack.

Ineffective things:

1. **Security based only on the firewall**: firewalls are no longer an adequate protection in the modern age when attacks are evolving and with them also the techniques in which the same attacks can be carried on. In today's world, working remotely is necessary in order not to love productivity when being away from the office or while traveling. Firewalls do not provide enough protection when connecting from other endpoints such as airports or cafes. Even though in your company you enlarge the range of endpoints from which the connections can be secured, always new threats are going to arise to mine your business. Nowadays, it is very unwise to rely on your security only on firewalls, when hackers are already specialized to get around these kinds of traditional network security.[6]

2. **"Knowledge of security threats should not be viewed as a competitive advantage"**: when a firm is well aware of security threats it should not use it to outperform its competitors, it should be otherwise used to building awareness inside the company and also outside in order to be able to formulate adequate response plans and ad hoc security measures.

3. **No *incident response plan***: "an incident response plan is a systematic and documented method of approaching and managing situations resulting from IT security incidents or breaches. It is used in enterprise IT environments and facilities to identify, respond, limit and counteract security incidents as they occur."[7] It is fundamental to include a good incident response plan in the framework of the company because it assures that different types of breaches are either resolved or counteracted with minimum time and resources possible, minimizing costs and losses.[8] At the time of the data breach, Heartland did not have an incident response plan ready to enter in force as a countermeasure of the attack.

4. **Human error:** humans are subjected to error constantly in life, because it is intrinsic in being humans. It is very common to occur in employees who can perform, during the period of work in a company, not at the maximum of their capacities and duties. This is normal but must be controlled and limited in order not to have an extensive branch of the company to be compromised. Strategies for reducing human error can go from taking disciplinary action directly on the person but also to the design the equipment, of the job, of the procedures and of training. Finally, it is important to reduce and even eliminate error occurrence and consequences.[9]

5. **Incorrect Responsibility management in Cyber Attack case**: in every company it is very important to separate competences and responsibilities in order to manage

[6] https://www.globalquestinc.com/a-firewall-isnt-enough-protecting-yourself-against-the-threats-you-cant-see "A Firewall Isn't Enough: Protecting Yourself Against the Threats You Can't See", Globalquest Solutions.

[7] https://www.techopedia.com/definition/16513/incident-response-plan Incident Response Plan

[8] https://www.techopedia.com/definition/16513/incident-response-plan Incident Response Plan

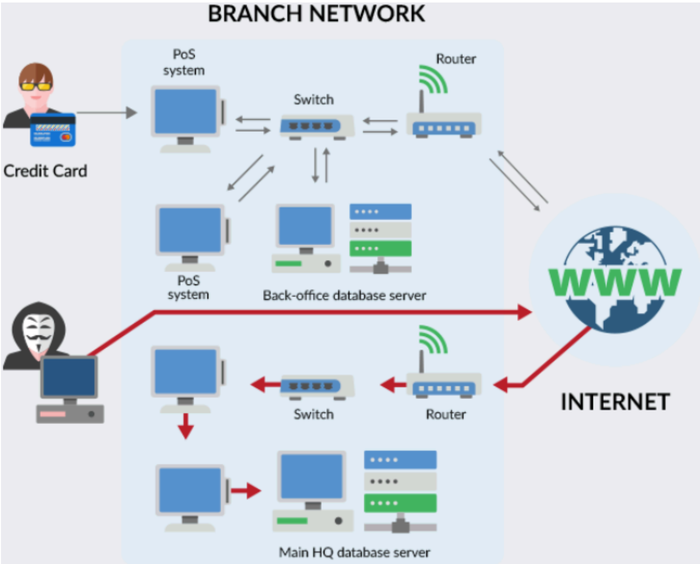
[9] http://www.hrdp-idrm.in/e5783/e17327/e28013/e28930/ "Strategies for reducing human error", Disaster Management Institute – DMI

every sector and prevent it from being compromised. At the time of the attack, Heartland had an incorrect responsibility management which led to internal fragmentation and consequently made the attack easier.

6. **Encrypting cardholder data from end to end - from the POS terminal to the end of the payment process**: in May 24, 2009, Heartland launched a new initiative, the E3 solution, and end-to-end encryption model to safeguard credit and debit card account information in the very moment of the card swipe when paying. Heartland has been one of the first companies to introduce this new technology, but it resulted to be ineffective because it did not protect the data flowing inside the company, which were in clear text. This made possible for the attacker to steal all the information.

Positive things:

1. **More secure POS terminal for its merchants with encrypting hardware built-in**: Heartland developed a stricter policy on secure POS terminal. The Point of Sale System (POS) security prevents the unauthorized access by third parties who look from security gaps to sneak inside the cardholder information and steal data in order to use the card according to their malicious intent.[10]



[Source: https://securebox.comodo.com/pos-system/pos-security/ Comodo Group Inc, Secure Box]

2. **New group within FS-ISAC to promote information sharing**: the partnership with the Financial Services Information Sharing and Analysis Center (FS-ISAC), responsible for the spreading of information about security threats among different providers of services. Together with FS-ISAC, Heartland created the Payments Processing Information Sharing Council (PPISC), in order to share confidential information about "*new and emerging types of security threats and risk mitigation techniques*"[11].

[10] https://digitalguardian.com/blog/what-pos-security-protecting-data-pos-environments "What is POS security? Protecting Data in POS Environments" by Nate Lord, September 11, 2018, Digital Guardian

[11] https://core.ac.uk/download/pdf/6245917.pdf "Heartland Payment Systems: Lessons Learned from a Data Breach" Julia S. Cheney, January 2010

2.2 Compromised assets and processes

In the previous paragraph, we discussed the events that eased the breach and made the attack possible, and on the other hand the positive things that Heartland Payments System did in order to strengthen its shield against attacks and the countermeasures.
This new paragraph will deal with the ex-post conditions, the result of the attack in terms of assets and processes compromised, in order to carry on a quantitative but also a qualitative analysis on the general loss of the company after the breach.

This kind of analysis is very important to:

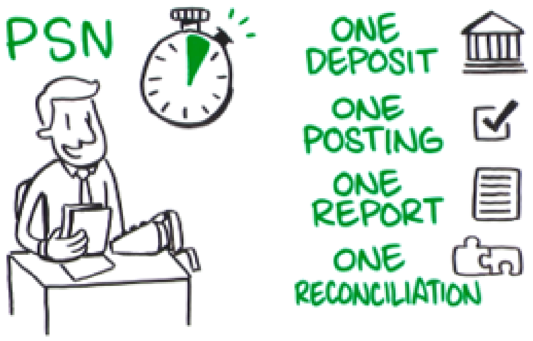
- Understand the gravity of the attack,
- Identify the compromised assets and processes,
- Identify if there has been entire sectors' impairment,
- Estimate the range of impact, in terms of financial, human, resource impact,
- Create an adequate risk assessment, by identifying and assessing risks,
- Identify control measures,
- Build an effective and efficient response plan,
- Build a cybersecurity program,
- Check the performance.

All these actions depend on the identification of the affected areas of the company, the compromised assets and processes which the company or organization must potentiate and control in order to avoid future breaches.
In the case of Heartland, we would like to provide a detailed analysis and identification of the processes and the assets that have been impacted and/or compromised during the attack of 2009.

1. **Web server**: the web server is the first most important asset that was compromised. The web server is a software application which can manage the requests of transfer of a client's web pages. The web server is mainly used to respond to clients' requests and allow the visualization of web pages. The web server has dedicated ports through which every client can connect. The job of the web server is to listen to these clients trying to connect and able them to browse. For a web server, it is fundamental to be able to talk to many kinds of devices like tablet, smartphone, laptops. Its role is very crucial in a company like Heartland, with a worldwide leading role especially in online transaction and payments processing. The web server of Heartland has been the first thing to be compromised in order to shut down all the connections among clients and between these same clients and the company itself.

2. **Corporate Network**: the aim of a corporate network is to connect people occupied in different buildings, departments, and organizational structures around the world. A corporate network needs to bring them all together, help them communicate and share resources, and protect and advance the interests of the corporate entity. It is defined as an enterprise's communications backbone that helps connect computers and related devices across departments and workgroup networks, facilitating insight and data accessibility.[12] A corporate network is about keeping both machines and people connected, in order to pursue shared business objectives and increase their competitiveness.[13]

3. **Payment Network**: the payment network surrounds us every day, whenever we pay with a credit card or we withdraw cash from an ATM. It assures that our everyday transactions are completed safely and accurately. The payment network is the intermediary among all the elements of a transaction, especially the link between the issuer of the transaction and the terminal or ATM of the service.[14] This can be a very crucial asset to compromise especially in a company like Heartland, which bases its own activities on this kind of network, with millions of dollars managed in payments processing every day. Compromising the payment network for a payment processor company means to compromise all its main activities which results in a huge loss in terms of money, availability and efficiency of the services.



[Source: https://www.info.paymentservicenetwork.com/]

4. **POS**: one of the technologies supported by the payment network, is the POS. As we mentioned before, Payments of Service System assures secure transactions and prevents unauthorized access in the very moment of swiping the card when the transactions take place. Even if Heartland developed a more secure strategies in protecting unauthorized access during the use of the POS terminal, during the attack the POS system was one of the first things to be compromised and it represented a good percentage of the attack because most of the data stolen was taken in the swiping of the card during the payment.

[12] https://www.techopedia.com/the-it-professionals-guide-to-corporate-networks/2/25665 "The IT Professional's Guide To Corporate Networks" David Scott Brown, September 18, 2017.

[13] https://www.igi-global.com/dictionary/corporate-network/5965 "Encyclopedia of Networked and Virtual Organizations" Goran D. Putnik and Maria Manuela Cruz-Cunha, March 2008.

[14] https://www.vantiv.com/about/newsroom/article-payments-networks-101 Payment Network 101, Rob Rankin.

5. **Database**: the databases of a company are its source of information on clients, on recorded transactions during different periods of time, on the financial situation of the company, on the current and past employees, on partners… databases are the container of basically all the information oh the company and its activities. Most of the information contained in databases are confidential and should not be shared with unauthorized third parties. With data breaches we mean the leaking and the disclosing of confidential information from an unauthorized person. The hacker will be able to consult, copy, share, transmit, and even manipulate[15] these data. Sometimes, it takes time from the wronged party to notice that the information of the databases has been compromised.

6. **Human Resources**: human resources were not the final target of the attack. In this case, the final objective of the attack was to rely on the possibility of human error of the employees of the Heartland in order to make them spread the malware inside the network. The employees have been an intermediate target to reach the final aim of the attack, to steal information and spread the malware inside the company.

2.3 Cybersecurity control weaknesses which have exposed the organization to the vulnerabilities exploited in the attack

After having discussed about the impacted sectors and the compromised assets of Heartland Payments System who made the company famous around the globe for one of the biggest data breaches of the history, we will going to dive deeper in the analysis of the case by identifying the cybersecurity control weaknesses which have exposed the company to the vulnerabilities exploited in the attack. The job of the hackers is to constantly look for the smallest and finest vulnerabilities to exploit in order to carry on the attack. Even though it seems that your system is completely secured and protected against any unwanted intrusion, there are always going to be some vulnerabilities that you were not aware about but that can be exploited by the hacker. This was the case of Heartland: in fact, even though the company was sure about its data protection and intrusion detection plan, we have identified some control weaknesses which made the hacker able to carry on the attack.

In this paragraph, we will focus on these weaknesses with the aim to understand their range of impact and the consequences which have been caused.

1. **Input sanitization**: the first weakness we want to focus on is the lack of control on the input sanitization. This is a very important control weakness because the lack of control on the input of the functions can lead to disastrous consequences: for instance, the Cross-Site Scripting (XSS) vulnerability that has as main target exactly those dynamic websites which do not have enough control on the input of the forms. It mainly consists in including html code inside a webpage in order to carry on malicious operations. The

[15] https://www.bit4law.com/data-breach/ "Cos'è il data breach?"

hackers can use the SQL injection attack for example to manipulate confidential information, to modify data contained in servers, altering the dynamic behaviour or web pages.[16]
The SQL injection is an attack which can take place thanks to a lack of control on the input, which was exactly what happened to Heartland. SQL injection is a code injection technique, used to attack database management systems. The SQL injection exploits the security vulnerabilities of the code of one application, for example when the user input is not correctly filtered as in the input sanitization. The SQL is used through inserting strings of SQL malicious code inside the input fields and then making these strings to be executed.

2. **Database control**: Another important control is the database control: in fact, it is very important to have control and inventories on the sensitive data of a company or an organization. It is also true that most companies have more or less a clear idea of the data that are on the system and on the publicly available information on the company itself and on all its components, but one thing is to have an idea, another thing is to have these data to be efficiently controlled and locally administered.[17] If the company does not have a good classification of data and a good policy to control and protect such data, it is very likely that hackers can access it and manipulate, copy, even change it.

3. **Network and backdoors control**: The network controls are another very important control that has to take place in order to keep your company or organization safe and under control. A network control is a procedure to improve the efficiency of the security control on the network. It is important to have all the IP addresses which are included in the network, to check their movements and the packets exchange that take place in the network.
A lack of network control can result in leaving open some ports in the system. This is a fatal mistake because in this way the hacker can identify open ports in the network which he can exploit in order to redirect the traffic and in this way sniff the information. This problem can be detected by checking the route of the packets and the time in which the traffic passes through the door, for example during the night hours where all the working activities do not take place.

4. **Potentially privilege escalation**: Not enough control on the permissions when dealing with the management of applications and programs can be also a factor to make the job of the hacker easier. In fact, it is very important to execute programs with the least privileges, only the ones necessary for the correct functioning of the program. In fact, if some of the programs that have more or higher permissions of the minimal required for

[16] https://www.html.it/articoli/xss-attacchi-avanzati/ "XSS: attacchi avanzati" Gianluca Brindisi, March 27th, 2012.

[17] https://www.csoonline.com/article/2935814/lessons-from-the-heartland-payment-systems-data-breach-redux.html "Lessons from the Heartland Payment Systems data breach, redux" Tony Martin-Vegue

the functioning of the application (for example, the ones at the admin level), could be exploited to execute malicious code that otherwise could not be executed only with user privileges.

5. **Network segregation subjected to human error**: At the time of the attack, Heartland's network was divided into two parts. These two parts did not communicate among each other and it was divided in this way: one part of the network was the one in which there was contained all the sensitive information on the company and the other part of the network did not contain any sensitive information. When the malware injected by the hacker entered in contact with the part of the network without sensitive data, this did not create a big problem because the malware was kept inside that network partition. Until here everything seems fine, but because of human error (like for example through USB, ethernet cable or any other type of cabled connection) the malware passed from the safe partition to the one which contained all the sensitive data of the company.

6. **No Cryptography**: The cryptography issue is strictly related to the network segregation issue. When the malware reached the network partition with all the sensitive data of the company, all that information was not encrypted. In fact, Heartland used end-to-end encryption according to which only the data flowing from inside the company towards outside were encrypted but not the data circulating inside the company. The sensitive data and information inside the company were in clear text. This was a crucial control weakness because when the malware entered the network partition with all the sensitive data, it was able to see all the card information.

7. **Missed Training and Education of Personnel**: The capacity building of a company is a crucial step to increase efficiency and protection from potential threats. In fact, the company must take care of the employees with courses, training workshops or professional knowledge. This is very important in order to manage and even foresee imminent and future threats that can affect the company in order to limit the impact of these threats and sometimes even avoid it. A well trained and aware personnel is fundamental especially nowadays, when companies are launching new technologies almost every day in order to make them able to keep up with the advancing progress and innovations. Untrained personnel will not be able to deal with threats and consequences and face the advancement of new technologies which will decrease the productivity and the efficiency of the company.

8. **Lack of incident plan**: an incident response plan is a set of instructions that help IT staff detect, respond to, and recover from network security incidents.[18] All IT companies must have an incident response plan because it plays an essential role when dealing with IT critical issues like threats, vulnerabilities, cybercrime, data loss. When a company, like Heartland, does not have an incident response plan, it jeopardises the

[18] https://www.cisco.com/c/en/us/products/security/incident-response-plan.html "What is an incident response plan of IT?"

capability of that company to function well, when facing the above-mentioned issues. In the case of Heartland, the missing plan did not allow the company to be prepared to face this malicious attack and respond rapidly and efficiently.

9. **Incorrect Auditing PCI/DSS**: The Payment Card Industry (PCI) Security Standards Council designed the Data Security Standard (DSS) in order to conduct assessment and on-site auditing to assure compliance of merchants and service providers to common shared standards about securing cardholder data.[19] It is developed in four steps: 1) Complete a Self-Assessment Questionnaire 2) Find a Qualified Security Assessor 3) Assess Your Compliance 4) Remediate.
   This assessment aims at enhancing the current security and compliance program of any company and organization, through improved infrastructure, awareness training, policies, procedures and network standards. A non-correct compliance and assessing of these standards from the company means to put all of this at risk.

3 How to mitigate control weaknesses by using information security standards

In the second chapter we have proved that sometimes, even if the company thinks to have a very good security system but actually, analysing more in depth the skeleton of the organization, we can find many holes in the system.

This third and last chapter will take all this as the basis to go a little bit further and conclude our analysis by finding remediation policies when receiving an attack like the one of the Heartland.

This part of the paper will be fundamental because it deals with control. Controls nowadays are very important when carrying on any kind of activity, but it becomes a crucial issue when dealing with activities that involve sensitive data like the ones of credit and debit cards that require a giant cyber architecture behind it. Controlling the cyberworld is a hard and almost impossible task, because of new threats, new challenges and new evolutions that are evolving every day. Sometimes, we spend years fighting one malware and we are so happy when we defeat it, that we do not think about the enormous quantity of new one that are just behind the corner, waiting for a vulnerability of the system to access it.

That is why it is very important to understand which weaknesses are present in our system and where, in order to prevent, or at least minimize, the chances of someone sneaking inside it.

This is why, in the next paragraphs, we will deal with some of the main information security standards which set standards for cyber security and information security, aiming at harmonize the level of all the organizations, companies, public and private businesses of

[19] https://smallbusiness.chron.com/pci-dss-audit-procedures-4891.html PCI DSS Audit Procedures

the world, limit and prevent control weaknesses to be the major attack territory of all hackers all around the world.

In the next pages, we will mainly deal with ISO – International Organization for Standardization and NIST – National Institute of Standards and Technology and how these standards are helpful in managing control weaknesses and implementing new policies and strategies to adapt businesses and organizations from all around the world to the same cyber security standards' level.

3.1 ISO – International Organization for Standardization

ISO is the main organization, at a global level, who deals with the developing and publishing of every kind of international standards and technical norms. The ISO standards deal basically with everything: from environmental control to languages, from business guidelines to air conditions. Of particular importance for the informatics world, is the section that goes from ISO 27000 to 27999, those standards dealing with Information technology security techniques or, as we like to say in other world, cybersecurity. This set of standards is serving as a reference point of all those businesses, companies, organizations who are dealing with cybersecurity or simply want to implement that sector among their activities.

In this paragraph, we will analyse ISO 27001 and 27002 referencing the Heartland Payments System case, in order to understand which of these controls would have mitigated the cybersecurity control weaknesses explained in the paragraph 2.3.

The ISO 27001 is a standard which deals with information security. It is very important because it belongs to the ISO 27000 family, which has as main aim to "help the organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties"[20]. In particular, ISO 27001 is of relevant importance because it provides requirements for the so-called information security management system (ISMS). The ISMS is "a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process"[21]. It is very important because it can help all kinds of businesses to keep information assets secure. In particular, the Plan-Do-Check-Act cycle refers to the ISMS and sets the guidelines to establish and implement it inside your system.

- ***"Plan (establishing the ISMS)***
  Establish the policy, the ISMS objectives, processes and procedures related to risk management and the improvement of information security to provide results in line with the global policies and objectives of the organization.
- ***Do (implementing and workings of the ISMS)***

[20] https://www.iso.org/isoiec-27001-information-security.html ISO/IEC 27000 family - Information security management systems

[21] https://www.iso.org/isoiec-27001-information-security.html ISO/IEC 27000 family - Information security management systems

Implement and exploit the ISMS policy, controls, processes and procedures.

- ***Check (monitoring and review of the ISMS)***
  Assess and, if applicable, measure the performances of the processes against the policy, objectives and practical experience and report results to management for review.
- ***Act (update and improvement of the ISMS)***
  Undertake corrective and preventive actions, on the basis of the results of the ISMS internal audit and management review, or other relevant information to continually improve the said system."[22]

Without the presence of an ISMS, controls tend to be disorganized and not effective, they do not really aim at enforcing solutions, but they serve more as a convention.
According to ISO 27001, the management must:

- *"Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;*
- *Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and*
- *Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis."*[23]

For what concerns ISO 27002, it provides best practice recommendations on information security controls in order to initiate, implement and maintain the Information Security Management Systems (ISMS). How to do it? We have to follow the C-I-A principle: assuring confidentiality, integrity and accessibility of information. For confidentiality it is intended that the information has to be accessible only from those authorized users, while availability means to keep that information available for the ones you are authorized to access it. Finally, integrity means that, during the communication between the client and the company, the information has not been modified by anybody. ISO 27002 deals specifically with physical and environmental security, with human resources security and standards and most importantly, sets the standards for the ways and means the access to cyber infrastructures has to be managed and controlled.

After having understood in general what are ISO 27001 and 27002 dealing with and their main areas of influence, we will go more in depth by analysing specifically how and why each requirement of the standards could have mitigated the control weaknesses of Heartland Payments System:

[22] http://iso-17799.safemode.org/indexecce.html?page=PDCA_Cycle PDCA Cycle
[23] https://en.wikipedia.org/wiki/ISO/IEC_27001 ISO/IEC 27001

1. **A.7.2.1 Management responsibilities:**
    1. **How**: make sure that all the employees are aware of the consequences of their actions and make the qualifications and skills appropriate to all employees with respect to the role they cover.
    2. **Why**: a good management of the responsibility in the company would have reduced the chances of human error.
2. **A.9.1.2 Access to network services:**
    1. **How**: monitor access to the network, and efficiently manage the network access procedures. In particular, things to check are the source and the destination of packets via various tools. One of the best tools is Wireshark that provides administrators a lot of information about them. If for instance, unknown IP addresses are detected, administrators might be alerted.
    2. **Why**: a stricter control on who, how and when access the network, surely reduces the chances of unauthorized access in the network. In particular, an APT via backdoor can be discovered and mitigated.
3. **A.9.2.3 Management of privileges:**
    1. **How**: minimize access rights to various process resources on the network, record all privileges allocated and verify the competence according to the privileges they have, by implementing a least privilege policy.
    2. **Why**: stricter and more defined privileges on applications would make more difficult privilege escalation to avoid unauthorized users to gain the admin privilege and allow the person to carry on important operations and changes inside the system. In addition, the attacker cannot use higher privilege services to remote code execution.
4. **A.9.4.1 Information access restriction:**
    1. **How**: controlling and providing physical access control in order to keep isolated sensitive applications, application data or system.
    2. **Why**: to make more difficult the movement from a network to another and be sure that the unauthorized users cannot access sensitive data. This also implies the reduction of human error by employees.
5. **A.9.4.4 Use of privileged utility programs:**
    1. **How**: first of all, it is important to state that privileged programs must be used only by trusted, dedicated staff members and administrators, in order to establish a minimum practical number of trusted logging users through a white list and define and document who has the authorization to which program, in order to track all safe accesses and target the malicious ones. This might be implemented in various ways: for instance, by physical implementation such as not giving privilege on employee's badge to access all part of the building or limiting the use of USB pen drives, signing which pen drive can be read by the servers and PCs.

b. **Why**: to make more difficult the movement from a network to another and be sure that the unauthorized users cannot access sensitive data. If the two networks are truly separated even in case of an attack, no data breach can take place because the attacker will not be able to reach the sensitive data.

6. **A.10.1.1 Policy on the use of cryptographic controls:**
This was a very crucial aspect because at the time of the attack Heartland did not have a good policy on data encryption and cryptographic controls. In fact, the end-to-end encryption was not enough to block an attacker from stealing credit cards information because the attack was from the inside where there was no encryption.
   a. **How**: make sure that the data inside the company are encrypted following the right policies of data encryption both in databases and inside the network. Make sure those policies are well implemented with periodical control and enforcement procedures. There are different ways to encrypt data between hosts e.g. with symmetric cryptography or asymmetric cryptography and all the sensitive information stored in the database must be hashed, the most used hashing algorithms are SHA-512 and bcrypt.
   b. **Why**: to make impossible the reading of information from non-authorized users and employees, which may have malicious aims. Even in cases in which an attacker succeeds in stealing data he will need several years before successfully decrypting all the information which is humanly impossible, so the data is still protected.

7. **A.12.2.1 Controls against malware:**
   a. **How**: in order to prevent malware from sneaking inside the system needs to be checked periodically. The first thing to do is reduce the vulnerabilities by doing vulnerability scanning. It can be done by establishing whitelists and by scanning all web pages and all files periodically to check whether there are vulnerabilities and to implement policies to eradicate them. White listing is a way to prevent malware attacks. The most used vulnerability scanning are OpenVas and Nessus which provide a deep analysis of the system and the potential danger of every service and software running along with the CVE of the vulnerability.
   b. **Why**: the first aim is to prevent future attacks, which is very unlikely to happen because new threats are always behind the corner. A more realistic idea could be to identify the malware and develop good and efficient response strategies as soon as possible.

8. **A. 12.4.1 Event Logging:**
   a. **How**: sequential and chronological registrations of all the operations that take place in the system from users or from administrators. These registers

should be then memorized and accessed every time it is needed to analyse data and events.

b. **Why**: to identify the actions taken by the malware, track the malicious activities and have records of their movements. If the malicious activities take place, it will leave a record in the event logging so it can be detected and subsequently eradicated. By checking the logs, you are always aware of the anomalies present in the system; this allows you to act and react accordingly: i.e. in an effective and efficient manner in the event of an attack.

9. A. 12.5.1 Installation of software on operational systems:

a. **How**: be sure that installations of the software are done exclusively from administrators' accounts. It is important to highlight that this procedure can be done only by administrators and not by other employees.

b. **Why**: administrators surely have more control of security management and have enough competences and knowledge to make sure the installation is done in the right and safe way. Normal employees might not have the complete knowledge of the servers, the service running on those and the network structure, so a misconfiguration might develop an unintentional vulnerability to be exploited by an attacker.

10. A. 12.6.1 Management of technical vulnerabilities:

a. **How**: the best outcome would be a complete lack of system vulnerabilities, but this can be achieved only by continuous checks and implementations on the system. This, of course, implies the development of good vulnerabilities detection and eradication policies.

b. **Why**: when your system is not subjected to vulnerabilities, it is very unlikely to have unauthorized access and most importantly, as the case of Heartland, to avoid attacks such as SQL injection or XSS (mentioned in the previous chapters).

11. A. 13.1.1: Network controls:

a. **How**: develop policies to manage and control the network under many aspects: from the list of all IP addresses logging in the network, information on the open and closed ports on which the traffic can be retransmitted, check of all the activities (who does what and especially if it is during working hours or not). In this situation a port scanner like Nmap and a traffic analyser like Wireshark come in handy.

b. **Why**: the reason is trivial: of course, a well-managed network is more difficult to attack, because the detection of unauthorized access is very efficient and precise. Through an open port an attacker can communicate with the server and might exploit the services running on it, with Wireshark we can detect the traffic flow, its anomalies and attacks.

12. **A. 14.2.1: Secure development policy:**
    a. **How**: develop control policies based on security, for the development of all types of applications, particularly web ones. This means that all the fields on the web page must be sanitized in order to eradicate XSS and SQL-Injection vulnerabilities; in case of software, follow the best practices to avoid basic vulnerabilities like "buffer overflow" and "string format vulnerability".
    b. **Why**: avoid bug disclosure and illegal accesses, which will result in less chances to be exploited, data breach and company loss.

13. **A. 16.1.1: Responsibilities and procedures:**
    a. **How**: development of procedures for incident response monitoring and logging.
    b. **Why**: to reduce the likelihood or impact of future incidents.

3.2 NIST – National Institute of Standards and Technology

After having provided the point of view of ISO on how to mitigate the control weaknesses of the company before, during and after the attack, we will continue the analysis by bringing the example of another information security framework: The National Institute of Standards and Technology – NIST.
NIST is an agency of the United States government, specifically the Department of Commerce, whose main task is the management of technologies, promoting innovations and industrial competitiveness.[24]
In this paragraph, we will go through the NIST requirements in order to understand which ones of the control strategies would have mitigated the weaknesses present in Heartland's systems and how.

1. PM-13 INFORMATION SECURITY WORKFORCE

The organization establishes an information security workforce development and improvement program.

The first control we want to focus on is about the information security workforce program. We decided to put this as the first control strategy because we think it is a fundamental step which presuppose also all the other ones. By establishing an information security workforce plan aimed at the development and the improvement of the working body, the company aims at keeping the personnel at a certain level for it to have the required skills and knowledge to face cybersecurity threats and manage risks. A company can do this by establishing training courses, building capacity and knowledge building activities.

[24] https://www.nist.gov/ NIST - National Institute of Standards and Technology U.S. Department of Commerce

2. AT-2(1) SECURITY AWARENESS | PRACTICAL EXERCISES

The organization includes practical exercises in security awareness training that simulate actual cyber-attacks.

The second control strategy is very linked to the first one. It just aims at defining which kind of activities can be done inside the company to make all the personnel, the clients and even the partners aware in practical terms of what is like to be under attack. This can be achieved by organizing some weeks during the year when all the people involved in the company can gather together in different groups in order to make people aware of the risks of cyber-attacks. The company can also organize group exercises and activities in order to test the ability of the member to collaborate and harmonize in response strategies to face cyber threats.

3. SC-8(4) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL/RANDOMISE COMMUNICATION

The information system implements cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected.

At the time of the attack, Heartland did not have a good encryption policy inside the company. In fact, once the malware reached the network partition with the sensitive information, since they were encrypted with end-to-end encryption, the data travelling inside the company were not encrypted. Once the hacker was able to sneak inside the system, he could read all the sensitive data in clear text. This is why it is crucial to have a good encryption implemented inside your company. It can be implemented with some simulation to check if the data are actually protected.

4. SI-4(13) INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS

The organization: (a) Analyzes communications traffic/'event patterns for the information system: (b) Develops profiles representing common traffic patterns and/or events: and (c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.

This information security control on system monitoring is very important in order to understand communication traffic patterns, to keep track of the use of the network all the users of the company do.

5. SI-4(20) INFORMATION SYSTEM MONITORING | PRIVILEGED USER

The organization implements organization-defined additional monitoring of privileged users.

Privilege escalation is a very important problem that a company and/or an organization can face. If there is not enough control on how privileges on web applications are managed, it is very likely that someone can exploit this and pass from user to admin permissions. This is extremely risky because administrators have very important tasks like acquire, install or upgrade computer components and software, maintain security policies, configure computer systems and servers. These kinds of activities can be done only by extremely reliable people, so it is very unsafe to allow people with malicious intents to gain the permissions to carry on such tasks.

6. SI-4(22) INFORMATION SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES

The information system detects network services that have not been authorized or approved by organization-defined authorization or approval processes and audits.

If good network controls take place, it is very easy to detect unauthorized access from unauthorized users, to understand if there have been open ports left on which the traffic can be redirected and so information can be stolen. This can be checked by the event log, registrations of all the operations that take place in the system from users or from administrators. The event log is used to detect if data redirecting on open doors takes place, or for instance unauthorized access in not working hours.

7. SI-4(24) INFORMATION SYSTEM MONITORING | INDICATORS OF COMPROMISE

The information system discovers, collects, distributes, and uses indicators of compromise
The check on indicators of compromise allow the company to have a clear idea on whether the system has been compromised and how. The best way to carry on this practice is precisely and clearly collect these indicators in order to have a defined idea on which assets have been compromised and how. It may lead to a more target-oriented strategy to repair and prevent these assets or entire sectors to be compromised again in the future.

8. RA-5 VULNERABILITY SCANNING

Scans for vulnerabilities in the information system and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported

The continuous check of vulnerabilities present inside the system of the company is a fundamental control practice that has to take place when carrying on any kind of activity. When the company is aware of its vulnerabilities, these can be fixed so that in the future the system will never incur the same weaknesses. A continuous check is the only possible way to manage vulnerabilities, because new threats arise continuously in the cyber world and with them also new ways in which the systems can be attacked.

9. IR-4 INCIDENT HANDLING

Control: The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery

b. Coordinates incident handling activities with contingency planning activities

c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures. training. and testing/exercises and implements the resulting changes accordingly.

10. IR-8 INCIDENT RESPONSE PLAN

Control: The organization:

Develops an incident response plan that:

a. Provides the organization with a roadmap for implementing its incident response capability;

b. Distributes copies of the incident response plan

c. Reviews the incident response

d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing

e. Communicates incident response plan changes

f. Protects the incident response plan from unauthorized disclosure and modification.

The last two control strategies are very similar. They both deal with the management and the handling of security incidents. A company always has to take into account the possibility of incidents to happen and that they cannot be prevented. If incidents cannot be prevented, at least it is fundamental to have a good incident handling policy and a good incident response plan implemented inside the company. These two strategies allow a fast incident detection and an efficient recovery and response phase. At the time of the attack, Heartland did not have an incident response plan, and this made its recovery slow and resource consuming.

3.3 Pros and cons of information security frameworks ISO and NIST

To complete our analysis, the last paragraph of the chapter will deal with a comparison between the information security frameworks we presented previously and, for each point, the pros and cons of adopting one strategy with respect to the other one and vice versa.

Description	ISO	NIST	Pros	Cons

Management responsibilities	**A.7.2.1**	**PM-13**	For what concerns this point, the two frameworks are on the same level because both of them provide an adequate and complete policy on how to build capacity inside the company and for the personnel.	
Access to network services	**A.9.1.2**	**SI-4(22)**	On the access to network services, ISO provides a more detailed policy, dedicating one section only to regulate the access to the network.	In this case, NIST is weaker because it is not effective in regulating all kinds of weaknesses, since it provides only one general strategy dealing with network weaknesses, which is not adequate enough to deal with all kinds of problems.
Management of privileges	**A.9.2.3**	**SI-4(20)**	On the management of privileges, ISO is stronger because it provides a more detailed policy on the management of privileges.	For what concerns the management of privileges, NIST is weaker because it provides only one general policy on how to deal with privilege escalation, while ISO is more specific.
Information access restriction	**A.9.4.1**	**SI-4(22)**	On the information access restriction, ISO provides a more detailed policy, dedicating one section only to regulate the access to the network.	In this case, NIST is weaker because it is not effective in regulating all kinds of weaknesses, since it provides only one general strategy dealing with network weaknesses, which is not adequate enough to deal with all kinds of problems.

Use of privileged utility programs	**A.9.4.4**	**SI-4(20)**	ISO is very specific when dealing with privilege escalation controls, because it dedicates an entire section on how to use web applications preventing privileges escalation.	For what concerns the management of privileges, NIST is weaker because it provides only one general policy on how to deal with privilege escalation, while ISO is more specific.
Cryptographic controls	**A.10.1.1**	**SC-8(4)**	On the encryption methods, the two frameworks are equally precise and accurate, because they both provide a specific strategy on how to deal with cryptographic measures inside the company.	
Controls against malware	**A.12.2.1**	**AT-2(1)**	Both frameworks have a good policy on controls against malware, but both of them give a different perspective. ISO is more technical while NIST is more about governance.	
Event Logging	**A.12.4.1**	**SI-4(13)**	When dealing with traffic detection, the two frameworks are equally precise, because both of them have a dedicated section on how to detect traffic movements.	
Installation of software on operational systems	**A.12.5.1**	**SI-4(20)**	ISO is very specific when dealing with privileges controls, because it dedicates an entire section on how to use web applications and good practices on how to deal with the	For what concerns the installation of software, NIST is weaker because it provides only one general policy on how to deal with privileges management and how to deal with specific admin permissions, while ISO is more specific.

			installation of software.	
Management of technical vulnerabilities	**A.12.6.1**	**RA-5** **SI-4(24)**	For what concerns the detecting and management of technical vulnerabilities, NIST provides a more detailed strategy, by dedicating even two controls on detecting vulnerabilities and checking indicators of compromised assets.	On the vulnerabilities of the system, ISO is a weaker framework because it provides a strategy on the management of vulnerabilities, but in a more general way with respect to NIST.
Network controls	**A.13.1.1**	**SI-4(22)**	On network controls, ISO provides a more detailed policy, dedicating one section only to regulate and control the network.	In this case, NIST is weaker because it is not effective in regulating all kinds of weaknesses, since it provides only one general strategy dealing with network weaknesses, which is not adequate enough to deal with all kinds of problems.
Secure development policy	**A.14.2.1**	**IR-4** **IR-8**	NIST has the best section regarding the secure development policies because it has even two strategies to control secure development inside the companies.	ISO has a good policy on implementing secure development policies, but it provides only the technicalities while NIST is very complete also under the governance aspect.
Responsibilities and procedures	**A.16.1.1**	**AT-2(1)** **IR-4** **IR-8**	NIST dedicates even three controls in defining the responsibilities and procedures to follow in case of incident responses.	Even though the ISO section on responsibilities and procedures is present and important in the framework, it is too poor to deal with all types of incident responses.

4 Conclusions

We have reached the end of our analysis.

We have used the case of Heartland Payments System, who has been the protagonist victim of one of the biggest data breaches of history, to talk about compromised sectors, positive and negative actions, system control weaknesses, control strategies, information security frameworks and the pros and cons of control strategies.
All this analysis led us to this final chapter of the work, when we are going to sum up our findings and try to go a little bit further by providing general suggestion and guidelines on how to check whether a company is aligned to the international standards on information security and is correctly implementing the policies in order to be protected against any type of intrusion in the system.

This kind of analysis is very important because it is very complete, and it helps the company to deeply build awareness on the weaknesses of their system and understand which kind of strategies can be applied to fill the security gaps and develop an adequate risk assessment and an incident response plan.

The cyber world, characterized by the constant development of new challenges, new threats and new innovations, is still an evolving space. For this reason, being completely safe from all the dangers is almost impossible. The chances of being attacked are big and the number of vulnerabilities which can be exploited even bigger. When you are dealing with sensitive information, like in the case of Heartland, the chances of being attacked is multiplied by the ways in which your company can be attacked and summarized with the impacted assets. The result can lead to disastrous consequences such as the loss of trust from clients and partners, the unavailability of information and also, last but not least, loss of money and/or profits.

Being aligned with international standards and developing good control strategies means that the chances of disastrous consequences will definitely decrease.

In order to do this, a cybersecurity expert managing technical vulnerabilities is not enough. We need the joint work and harmonized response strategies from many different professional figures: the cybersecurity technical expert, as mentioned before, covers a fundamental role in dealing with such issues but it is not enough. In addition, we need motivated stakeholders, which are the main source of money to develop new strategies and new technologies. We need an economist, able to deal with the management of monetary resources, we need even an anthropologist, which can analyse the human errors of employees and the human factors inside the hackers' minds. We need auditors, to determine whether an information system safeguards assets, maintains integrity, achieves organizational goals effectively and consumes resources efficiently".[25] We need risk management experts, to understand the threats, the likelihood and the impact of risks.[26]

As you can see, cybersecurity is a complex and open system made of many components and many agents interacting among each other in order to reach a common goal. All the components are crucial for the success of the battle against hackers. All the components are fundamental to the implementation of cybersecurity that, as said before, is an horizon, so even if we can never fully reach it, we can learn how to manage.

[25] Slides of the course "Governance, Management and Auditing of Cybersecurity – Theory and Practice in International Organizations". HOW TO AUDIT and FORMALLY CERTIFY A CYBERSECURITY PROGRAM, Slide n. 8.

[26] Slides of the course "Governance, Management and Auditing of Cybersecurity – Theory and Practice in International Organizations". HOW TO AUDIT and FORMALLY CERTIFY A CYBERSECURITY PROGRAM, Slide n. 10.

5 Bibliography and Sitography

1. Slides of the course “Governance, Management and Auditing of Cybersecurity – Theory and Practice in International Organizations”.
2. UNITED STATES DISTRICT COURT DISTRICT OF NEW JERSEY, UNITED STATES OF AMERICA v. ALBERT GONZALEZ.
3. https://www.secureworks.com/blog/general-pci-compliance-data-security-case-study-heartland “A Famous Data Security Breach & PCI Case Study: Four Years Later”, Thursday, October 25, 2012, by SECUREWORKS
4. https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf “Cybersecurity Threats Challenges Opportunities”, ACS – The Professional Association for Australia's ICT sector, November 2016.
5. https://economictimes.indiatimes.com/definition/cyber-security “Definition of Cybersecurity”, The Economic Times.
6. https://en.wikipedia.org/wiki/Heartland_Payment_Systems Heartland Payments System
7. https://www.heartlandpaymentsystems.com/about-us Heartland Payments System official website
8. https://en.wikipedia.org/wiki/Albert_Gonzalez#Heartland_Payment_Systems Albert Gonzalez
9. https://www.bankinfosecurity.com/heartland-payment-systems-forcht-bank-discover-data-breaches-a-1168 “Heartland Payment Systems, Forcht Bank Discover Data Breaches” Linda McGlasson, January 21, 2009
10. https://www.globalquestinc.com/a-firewall-isnt-enough-protecting-yourself-against-the-threats-you-cant-see “A Firewall Isn’t Enough: Protecting Yourself Against the Threats You Can’t See”, Globalquest Solutions.

11. https://www.techopedia.com/definition/16513/incident-response-plan Incident Response Plan
12. http://www.hrdp-idrm.in/e5783/e17327/e28013/e28930/ "Strategies for reducing human error", Disaster Management Institute
13. https://securebox.comodo.com/pos-system/pos-security/ Comodo Group Inc, Secure Box
14. https://digitalguardian.com/blog/what-pos-security-protecting-data-pos-environments "What is POS security? Protecting Data in POS Environments" by Nate Lord, September 11, 2018, Digital Guardian
15. https://core.ac.uk/download/pdf/6245917.pdf "Heartland Payment Systems: Lessons Learned from a Data Breach" Julia S. Cheney, January 2010
16. https://www.techopedia.com/the-it-professionals-guide-to-corporate-networks/2/25665 "The IT Professional's Guide To Corporate Networks" David Scott Brown, September 18, 2017.
17. https://www.igi-global.com/dictionary/corporate-network/5965 "Encyclopedia of Networked and Virtual Organizations" Goran D. Putnik and Maria Manuela Cruz-Cunha, March 2008.
18. https://www.vantiv.com/about/newsroom/article-payments-networks-101 Payment Network 101, Rob Rankin.
19. https://www.html.it/articoli/xss-attacchi-avanzati/ "XSS: attacchi avanzati" Gianluca Brindisi, March 27th, 2012.
20. https://www.csoonline.com/article/2935814/lessons-from-the-heartland-payment-systems-data-breach-redux.html "Lessons from the Heartland Payment Systems data breach, redux" Tony Martin-Vegue
21. https://www.cisco.com/c/en/us/products/security/incident-response-plan.html "What is an incident response plan of IT?"
22. https://smallbusiness.chron.com/pci-dss-audit-procedures-4891.html PCI DSS Audit Procedures
23. https://www.iso.org/isoiec-27001-information-security.html ISO/IEC 27000 family - Information security management systems
24. http://iso-17799.safemode.org/indexecce.html?page=PDCA_Cycle PDCA Cycle
25. https://en.wikipedia.org/wiki/ISO/IEC_27001 ISO/IEC 27001

26. https://www.nist.gov/ NIST - National Institute of Standards and Technology U.S. Department of Commerce