The 2011 PlayStation®Network‘s attack

G. Ranieri - F. Albertini - F. Lafronza

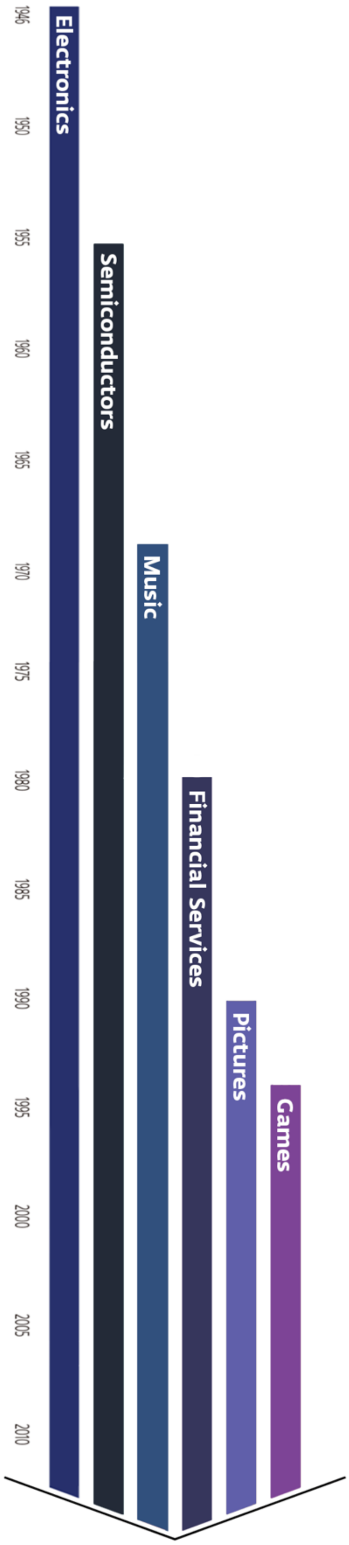
MsC in Cyber Risk Strategy & Governance

Technology Risk Governance

Critical incident report - The 2011 PlayStation Network's attack

Index:

1. Sony in 2011



Sony is a Japanese multinational corporation founded in 1946 in Tokyo, Japan, which specializes in consumer and professional electronics, gaming and entertainment. As of 2011, the company employed more than 70.000 people worldwide and registered consolidated sales and operating revenue of ¥6.493 billion (which rounds up to roughly €54 billion). The company owns the largest music entertainment business in the world, the largest video game console business and one of the largest video game publishing businesses. Sony is also one of the leading manufacturers of electronic products for the consumer and professional markets and a leading player in the film and television entertainment industry.

The history of the company is one of constant growth and success. It all started in 1946, one year after the end of World War II, when Masaru Ibuka and Akio Morita established Tokyo Telecommunications Engineering Corporation, out of a desire to use their technologies to contribute to society. In 1958, the company changed its name to the current Sony, a portmanteau of the Latin word “sonus”, a clear reference to the acquired importance of the audio components for the company, and “sonny”, a Japanese word used to refer to young men. In the 65 years since its founding, also thanks to some external acquisition (e.g. Columbia Pictures), Sony has evolved into a company with an ever-growing business portfolio that currently includes electronics, semiconductors (since 1955), music (1968), financial services (1979), motion pictures (1989), and games (1993) (Sony Annual Report, 2011).

The path to success of Sony has not been a straight line. Like many other technology companies, throughout the years, Sony has experienced various types of cyber-attacks to its products and services (e.g. 2014 Sony Pictures’ hack), some of which have become well-known to the public thanks to the attention of the media. The attack that the paper will delve into in the next paragraphs is the 2011 PlayStation™ Network’s attack, in which personal details from approximately 77 million accounts were compromised, and in order to better understand how the attack to one of the company’s main services came to be, the paper shall look at the state of affairs of Sony in 2011, with a particular focus on the Game & Network Services segment.

1.1. Competitors in the Game & Network Services

The year 2011 has proven to be a pivotal moment for most of the companies in the video gaming industry, mainly because of the upcoming transition from the seventh generation to the eighth generation of video game consoles. The sales of the seventh generation of video game consoles (PlayStation 3, Xbox 360 and Wii) were approaching their saturation levels and the respective developing companies were refining the new consoles to deliver them in the upcoming months. In this greatly complex and dynamic panorama, Sony enjoyed the position of market leader (11,44 mln units sold in fiscal year 2011) by a very small margin against its main competitor Microsoft (11,33 mln units) and followed closely by Nintendo (9,85 mln units), the third main player of the market (AFJV, 2013).

2011 marked the year of the transition to a new era of gaming consoles

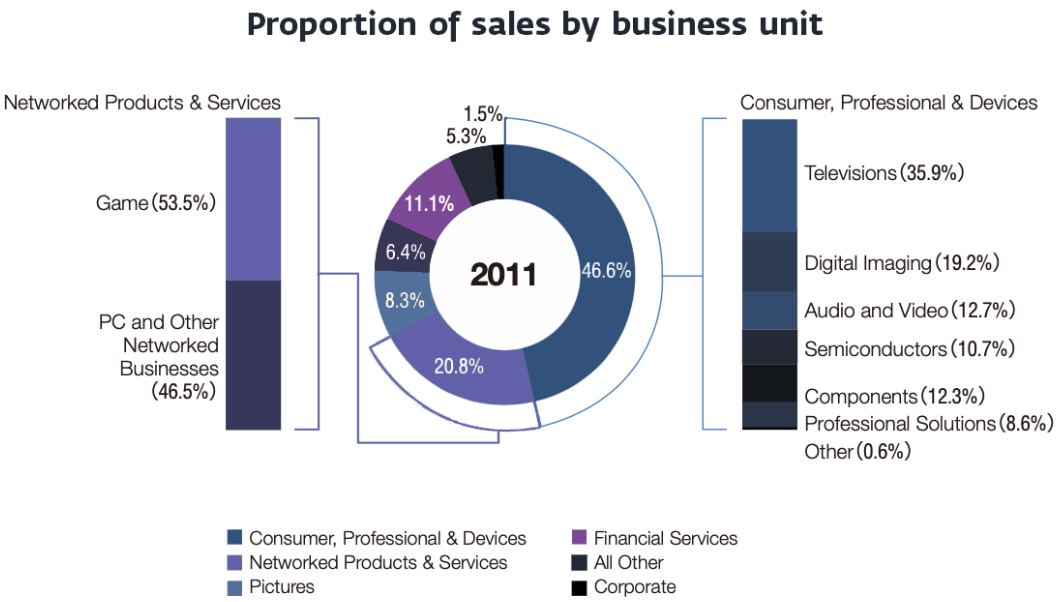
While, at that time, Sony was present on the market with both the PlayStation 2 and the PlayStation 3, Microsoft had already discontinued the Xbox and focused their effort exclusively on the new Xbox 360. Even if the performance of the two gaming consoles was reasonably similar, the Xbox 360, since the day of its release, has aimed to keep a lower price point than the PlayStation 3. The reason for this decision by Microsoft can be easily traced back to the pricing policy of their online services compared to Sony's. Both companies indeed offered their customers an online multiplayer gaming service. While Sony's PlayStation™ Network was free for all users, with the possibility to pay for the premium version (PlayStation Plus), Microsoft's Xbox Live was conceived, since its beginning, as a paid subscription service, starting at $50 a year. By taking this business decision, Microsoft likely chose to renounce at a higher return on the sale of the consoles in place of a steady income from its customers for its online services.

In this panorama Sony enjoyed the position of market leader

Even if the Wii was aimed at a different target of video game players (namely kids and families), Nintendo still provided its customers the possibility to play online through its online multiplayer gaming service called Nintendo Wi-Fi Connection. Just like Sony with its PlayStation™ Network, Nintendo opted to make the Nintendo Wi-Fi Connection available for free to its users, so that players could match up against people in different parts of the world and have a better overall experience (Nintendo website, 2019).

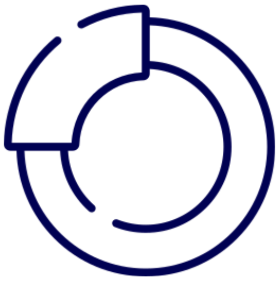
1.2. Company's business units

As mentioned in the previous paragraphs, Sony started selling electronic components but has gradually moved its focus on other businesses. In 2011 the U.S based Sony Music Entertainment, which had artists such as One Direction, Adele, and Beyoncé under contract, was the leader of the music recording business, recording sales around €3.9 billion. Meanwhile, at the dawn of the 4K era, the LCD television industry was about to reach its peak and Sony was able to hold a 10% share of the market, just behind Samsung (18,8%) and LG Electronics (12%). Most importantly, Sony Interactive Entertainment was regarded as the leader of the market video game console business and one of the largest companies in the video game publishing business.



Source: Sony's Annual Report 2011

Figure 1: Pie chart showing the proportion of sale by business unit in 2011.



The business unit with the gaming segment is the second most important for the company

Looking at the proportion of sales by business unit, the Consumer, Professional & Devices segment of the company, which included televisions, digital imaging, audio and video, semiconductors, and components as well as professional solutions, was the most important one (46.6% of the sales of Sony). While all the other business units taken singularly rarely reach more than 10% of the sales of the company, the Networked Products & Services business reaches 20.8% and is the second by importance for the Japanese conglomerate. This business unit comprehends the video game console, the video game publishing, and the online services business, which will be thoroughly examined in the next paragraphs of the paper (Sony Annual Report, 2011).

1.3. PlayStation™ Network (PSN)

Sony Computer Entertainment, the multinational video game and digital entertainment subsidiary owned by Sony Corporation, launched its digital media entertainment service in November 2006. The PlayStation™ Network allows PlayStation users to buy videogames on an online marketplace, to interact and play against other players on the network, and to access different music and movie streaming services. In order to access these services, when accessing the network the first time, the player is prompted to sign up by providing its personal information and a valid e-mail address to Sony (PlayStation website, 2019).

The PlayStation™ Network is one of the most important assets for the company

Starting from 2010, an optional premium subscription was made available to the public. A PlayStation™ Plus (often referred to as PS Plus) subscription provided access to complimentary games, exclusive content, and premium features for €49 a year. During the unveiling of the new PlayStation 4 in 2013, Sony announced that a PlayStation™ Plus subscription was going to be needed by the users to play online, assimilating its pricing strategy to Microsoft's Xbox Live (Sliva, Marty, 2016). This choice was driven by the fact that the new console's proclaimed main focus was going to be the online play and, according to Sony's management, the PlayStation 4 online gaming network was going to require a large investment of resources. The decision to make the PlayStation™ Plus account mandatory for anything that offers "real-time online play" marked without question a pivotal moment for Sony Corporation's history, following the realization of the importance of having a sturdy and impenetrable system (Loveridge, Sam, 2013).

2. Environmental conditions

The Sony data breach of 2011 is considered as one of the biggest security breaches of all times, due to the high number of information stolen from around 77 millions of different accounts all over the world (Baker and Finkle, 2011). Due to the high importance of the event, and to the number of actors involved, it is fundamental, while analyzing the causes and the consequences of the attack, to consider not only the company's faults or the techniques the hackers have utilized, but also the environmental conditions that set the stage for it. The goal of this paragraph is to give a brief introduction to four of the most important things that could have, directly or indirectly, contributed to the data breach. Those are:

1. The release of the Custom Firmware named Rebug;
2. Sony's sue to a famous hacker, George Hotz (nickname: "GeoHot");
3. Anonymous' DDoS attack to the corporation;
4. The appearance of a new hacker group, called LulzSec.

Some envirnomental conditions might be at the root of the attack

2.1. Rebug

In 2011 Sony Entertainment network released a new firmware for the PlayStation 3 console, whose code name was Rebug. It was considered as a revolution for the PS3 software because it had a new feature: the possibility to "transform" the console into a developer unit. This functionality was not intended to be accessible for normal users and, when started, it activated a set of features that were not accessible to the players. Yet, the most important thing about this new firmware, was the fact that, when the console was considered as a developer unit, it gained trusted access to Sony's internal developer network (Anthony, 2011). Once the internal server was reached, a lot of different potential hacks became available, because the server identified the user as a developer with a trusted access. At the time, one of the most credited theory stated that the customer's information database was easily accessible once the developer's permissions where held by an attacker.

Rebug enabled a way to get trusted access to Sony's network from the consoles

Even if, due to the new finding on the case, this hypothesis was discarded, this vulnerability of the developer's network could be one of the wrong paths followed by Sony's technicians that led to the long downtime of the PSN servers.

2.2. George Hotz sue

George Hotz was a hacker known to be the first person that executed a jailbreak of an iPhone. In 2009, two years before the data breach, he declared his intention to perform a security breach into a PlayStation 3 device. One year later, in 2010, he had his first theoretical achievement about this goal, but later in the same year he announced that he had stopped working on that case because the security system was too hard to exploit. However, the task was later accomplished by another hacking group, called "fail0verflow", that was well known for their ability on reverse engineering of security models. They were able to get the root signing and the encryption keys of the device. The trouble began in 2011 when George Hotz, whose nickname was "GeoHot", posted the root keys of the console on his website and created many tutorials on how to hack the PlayStation 3 console. The keys were immediately removed from his website due to a legal action carried out by Sony, but he continued to publish information about the possible exploits of the device. This resulted in a legal action against Hotz and the further request made by Sony to have access to all the IP addresses of people that visited GeoHot's website. After that, even PayPal guaranteed the access of Hotz's account to Sony and the parts reached an agreement to settle the lawsuit, in which it was stated that George Hotz would never try again any kind of hacking to a Sony product or server (Seybold, 2011).

Anonymous attacked Sony's network because of their behavior

2.3. Anonymous DDoS attack

The sue against George Hotz immediately backfired on Sony Computer Entertainment. Anonymous, a group of "hacktivist" (portmanteau of the word

Anonymous attacked Sony's network because of their behavior

"hack" and "activism"), born around 2003/2004, targeted the company because of its behavior. The group in fact was famous to actively fight for the freedom of speech and privacy on the internet. Sony's request to obtain access to the IP addresses of everyone who had visited George Hotz's website was against the principles of the organization, so the group decided to "declare war" to the company. Anonymous were also famous for their "modus operandi", performing Distributed Denial of Service (DDoS) attacks to the servers of the target in order to damage them. Two weeks before the data breach, Sony was victim of a DDoS attack, that was claimed by Anonymous. This, even if was completely unrelated to the following attack, had possibly made it even more difficult to detect the action of the cyber-thieves during the main attack. In fact, as it is stated in a letter sent by the company to the United States House of Representatives, Sony declared that the combined effect of the DDoS attack and the method used by the data-breachers made it very difficult for the technicians to detect what it was really happening (Rashid, 2011). Moreover, the proximity of the attacks made the company think that they were both carried out by the same organization, so they publicly accused Anonymous, identifying them as the responsible for the data breach. This public statement, when the real group of hackers claimed the attack, had a negative impact on the public image of the enterprise.

2.4. LulzSec

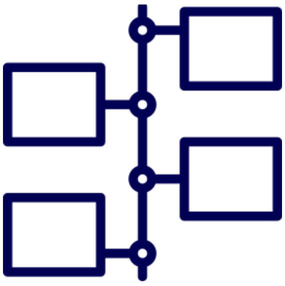
LulzSec performed attacks against a large number of companies and entities

The attack was indeed claimed by a group called LulzSec (portmanteau of "Lulz", the plural of "LoL" that stands for "Laughing Out Loud", and the word "Security"), a group that announced that they were in the business of stealing information and distributing it to the world just "for the lulz of it" (Pendergrass, 2012). So, their main goal was not to earn money through the cyber-theft and therefore Sony was not targeted for a specific reason. In fact, during their activity, they have performed various attacks against a large number of companies and entities, such as game servers of famous video games or even a A.T.M machine in the United Kingdom (Fox News, 2011). Their main goal was always to steal information and publish them on the internet but they have also performed DDoS attacks, sometimes also collaborating with Anonymous. Even if they had no monetary purposes their action had an enormous effect on the perception that people had of internet security. They were "loud", communicating every attack through Twitter and performing hacks not only to companies, but even to entities whose main objective was security, such as the CIA, the FBI, and the Arizona Law Enforcement.

3. Timeline of events

In this paragraph, the timeline of the events that involved Sony, between April and May 2011, will be presented. As previously said, in March 2010, Sony, for security reasons, updated the firmware to disable the possibility to run other operating systems (e.g. Linux) on the PS3. Then, at the end of 2010, the group fail0verflow discovered how to jailbreak PS3 and, at the beginning of 2011, GeoHot released a tutorial video to teach users how to run their own software on the console. For these reasons, on January 2011 Sony sued both the group and George Holtz for copyright infringement.

The court case attracted the attention of Anonymous group. The hackers announced that they would become operative to attempt to disrupt Sony's website if the company would not drop the charges against GeoHot.



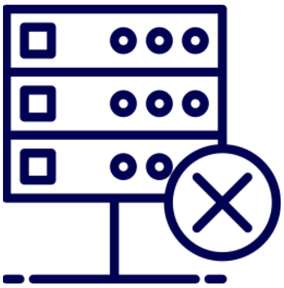
A timeline of the event is an essential ingredient for a deeper analysis of the case

The timeline of the events went as follows (To the Rails, 2011):

- April 11, 2011: Sony settles case with George Hotz, who closes his website with the info on how to jailbreak the PS3.
- April 13, 2011: Anonymous publishes a video declaring Sony as a public enemy, calling for a day of protest against the company and warns them on an incoming attack.
- **April 16-17, 2011 (Incident): Hackers break into PlayStation Network (PSN) and Sony Online Entertainment (SOE).**
- April 19, 2011: Sony detects the security breach and starts an internal investigation but does not send any message to their users to inform them about the situation of their personal information.
- April 20, 2011: Sony shuts down PSN declaring that the system was suffering from technical issues.
- April 22, 2011: Anonymous releases a statement denying any responsibility for the PSN outage.
- April 26, 2011 (PSN hacked): Sony admits the PSN has been hacked between April 17 and 20 blaming Anonymous group and enlists the aid of FBI. The breach concerns 77 Million names, date of birth, addresses, credentials and passwords, purchase history and probably financial information.
- April 28, 2011: A gamer sues Sony because the company "failed to provide prompt and adequate warnings of security breaches, and unreasonably delayed in bringing the PSN service back on line" (Richard Chirgwin, 2011).

On April 16-17, 2011 hackers broke into the PlayStation Network

- May 1, 2011 (SOE hacked): Sony executives apologize for the data breach and the outage of PSN. Meanwhile the company discovers that the servers of SOE have been breached and decides to shut them down.
- May 2, 2011: Sony unveils SOE breach details to public. They declare that 24.6 Million customers birthdates, email and phone info were breached, including around thirteen thousand non-US credit or debit card information.
- May 4, 2011: The Chairman of Sony says to the congress that they found a folder called "Anonymous" with a document containing the statement "We Are Legion", which is also the hacker group's motto. After Anonymous declined any responsibility, the company claimed that the group, with their activity, made it easier for other attackers to breach into Sony systems.
- May 5, 2011: Once again Anonymous denies credit card theft.



Sony missed its first self-imposed deadline

- May 5, 2011: Sony brings in forensic experts on data breaches (Data Forte, Guidance Software, and Protiviti).
- May 5, 2011: Sony releases statement that say the company is testing its new network and that the PSN will return "in the coming days".
- May 7, 2011: Sony misses its self-imposed deadline of service restoration due to the sophistication of the hack (subsequently in this work we will conclude that the attack was not sophisticate as Sony declares and the problem was the level of the security measures).
- May 7, 2011 (incident): Sony suffers another leak. The breach includes around two thousand names and addresses of 2001 Sony's database (Chester Wisniewski, 2011).
- May 9, 2011: Sony declares that the services will go back online by the end of the month.
- May 14, 2011: Sony starts to put accounts back online keeping some services still inactive (e.g. PlayStation Store). All SOE games and services were down for 24 days.
- May 15, 2011: Firmware update and for users became mandatory to reset their passwords, once changed users can access to their accounts.

The aforementioned timeline presents a brief introduction to Sony's case. Soon after the resume of the PSN and the other services, Sony stated that they had indeed fixed their network and ensured users about the safety of their information. Nevertheless, starting from May 17, a lot of other vulnerabilities would then be exploited by hackers. On May 17, a vulnerability that led an attacker to change user password using only account's email and date of birth (breached information) was discovered.

Subsequently, phishing site were found on Sony's server, which exploited vulnerabilities of Sony Music Indonesia (by k4L0ng666), Sony Greece's website was hacked via SQL Injection breaching 8,500 usernames, email, phone and password hashes (by b4d_vipera).

The following months would see Sony attacked by different actors (the most powerful was LulzSec group) sometimes known, sometimes unknown. During those months, Sony claimed many times over to have done everything in their power to patch vulnerabilities, although it seemed that the hacker community wanted to prove Sony's incompetence and lack of security measures.

4. Model based in-depth analysis

Different type of models have been used to analyze the event

In order to correctly analyze the failures of the system and the active errors that lead to the 2011 PlayStation's Network data breach, this paper is going to follow a precise path. The first thing will be the analysis of the event using the TRIPOD Beta method, in order to discover and explain the active and latent errors of the system and the failures that lead to the data breach. Then the paper will present another type of analysis developed by Olaniran *et al.* using the Anticipatory Model of Crisis Management (AMCM).This second analysis will be useful in order to have a broader view of the event and will be used to develop a Bow Tie Model for the company in order to try to prevent similar outages.

4.1. TRIPOD Beta Tree Analysis

The TRIPOD Beta tree for the analysis is built following three main steps. Each step has the aim to answer a specific question about the accident. The first one asks the question "What happened?", the second "How did it happen?" and the last one "Why did it happen?". It is mainly focused on human errors that can be related both to direct errors or to design errors of the system.

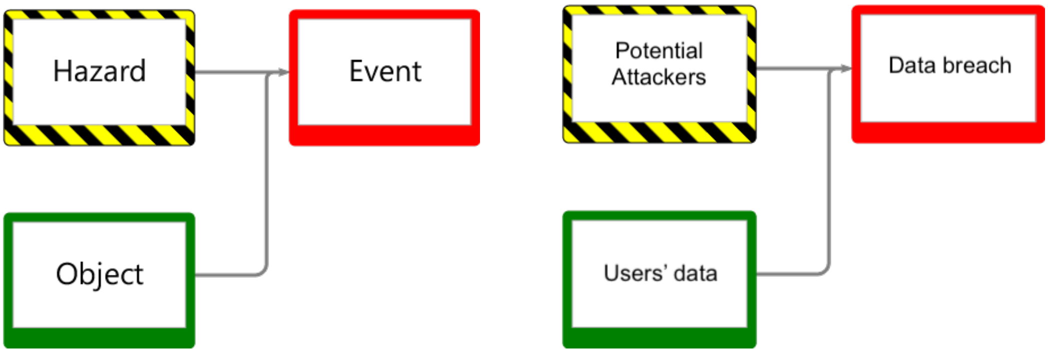


Figure 2: First step of the TRIPOD Beta, general and applied version.

The first step of the three is built as it is shown in the following image, on the left, there is the standard structure for the TRIPOD Beta, while on the right side the structure applied to the PlayStation Network data breach (Figure 2).

The TRIPOD analysis follows three main steps

It is important to describe in detail every single part of the three that is being built:

- **Users' data (Object):** The sensible data of the users of the PlayStation Network is the core of our analysis. This was the target of the attackers and, also, it is one of the company's most sensible information. In fact, ensuring the security of user's data must be the priority of a company that works on the internet. If the potential customers feel unsafe about the protection of their data while purchasing something, they probably will not go through with the purchase. This means that losing sensitive information implies losing credibility and trust among customers.
- **Potential attackers (Hazard/Agent):** When a company works with a considerable amount of data and sensible information, the potential hazard for the company is the potential malicious agents. The aims of the attackers are as various as the many possible attacks that they can perform, meaning that organization must always take into consideration their potential impact.
- **Data breach (Event):** The data breach of the PlayStation Network is the main event on this TRIPOD analysis. It is possible to describe it in general terms as the Hazard that is able to reach the Object that the company must preserve, and this is what happened during the data breach. The attackers, violating the security protocols of the company were able to access the sensitive information stored into the servers of the PlayStation Network. This caused enormous damage to the company in terms of economic loss, in fact, their servers suffered an enormous downtime, and damage for the users, because their data were stolen.

Sensitive data was stored in plain and human-readable text

The second step of the analysis is focused on the "How". What are the security protocols that have failed or that were missing during the attack that lead to the final event? While performing this analysis, we will consider two important types of barriers that the company needs to have to protect sensitive information. The first one has to protect the Object, the users' data, from the possible Hazard, potential attackers. In this case, it is the cryptography algorithm for the users' data that, according to the statements of LulzSec was completely missing. This means that the sensitive data was stored in plain and human-readable text. After accessing the database the group could just copy the data without even needing to try to decrypt the text. The second one has to prevent the Hazard to be exposed and try to harm company. In the case considered this barrier was represented by the authentication of the servers. According to the same statements of LulzSec, they were able to bypass that protection using a simple SQL injection. This means that the so-called “SQL countermeasures”, used in coding to prevent SQL injection attacks were completely missing. The usual countermeasures that are utilized to prevent this type of attack belong to two important categories:

- **Parse first principle:** means that it is possible to use parameterized SQL-queries (that are also called prepared statements) that are generally offered by the database.
- **Perform input validation:** means to not allow users to insert every possible character as input, especially ones that can create problems to the database, such as “”. Another possibility is to rewrite these characters into ones that do not give problems to the databases.

The protection layer was bypassed with a simple SQL injection

In the event of the PSN data breach, the first barrier can be considered as missing, because there was not any kind of cryptography. The second one must be considered as a failed barrier because the authentication has the purpose of keeping the unauthorized users out of the system and this goal was not reached.

The third step of the analysis will be related to the question “Why?”. What are the preconditions existing into the company that caused the data breach to happen? In the image below it is possible to see the schema that will be used for the analysis. On top there is the one that represents the general structure for this TRIPOD Beta analysis, below there is the application of the case (Figure 3).

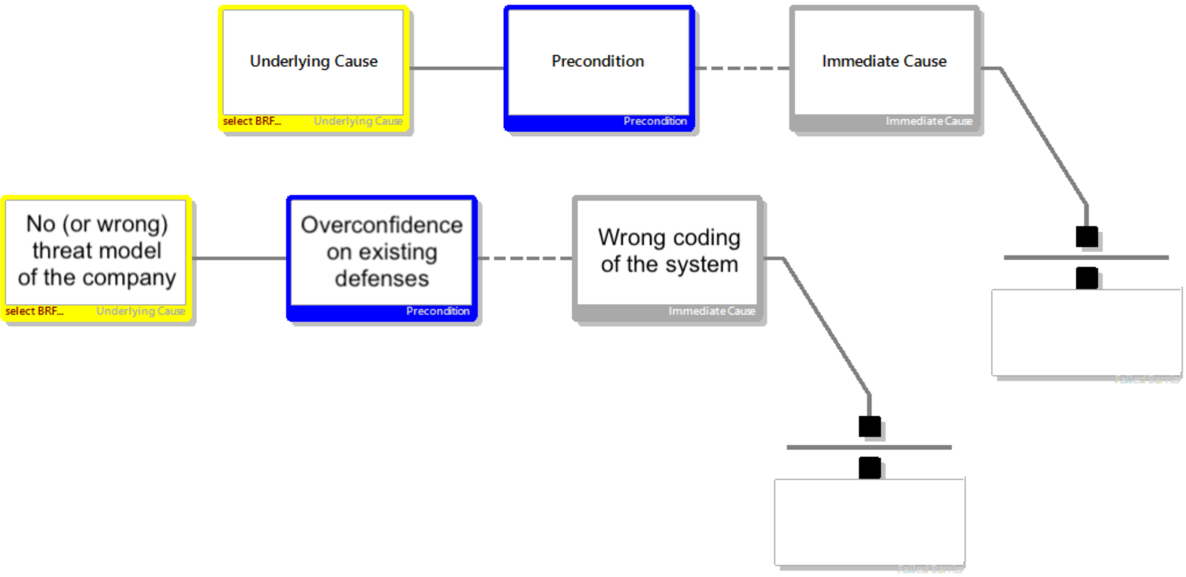
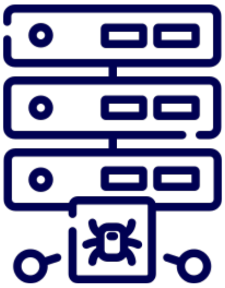


Figure 3: Basic and applied structure of the third step of TRIPOD analysis.

Starting from latent errors to the immediate cause, it is possible to underline the various error of the company while creating its system:

- **No (or wrong) threat model of the company (Underlying cause):** The latent error is related to the threat modeling performed by the society. The absence of a cryptography algorithm means that the company at that time performed a wrong threat modeling. So, there was no correct identification of the possible attackers and mostly there was no identification of the possible core assets of the company and the risk related to a possible data breach.
- **Overconfidence on existing defenses (Precondition):** This level is related to the existing environmental conditions and it can be considered as one of the most important mistakes done by Sony. In fact, after the sue to the famous hacker George Hotz and the Anonymous' DDoS attack, there was the necessity to focus more on the defenses of the company against the possible informatic attacks.
- **Wrong coding of the system (Immediate cause):** The immediate cause that created the condition for the Hazard to reach the Object is related to the wrong coding of the entire system. As was stated before the attack was carried out by a simple SQL injection, something that must not happen in an organization such as Sony. They have been always working in the technology sector and they should have been prepared to face even the most complicated cyber-attacks, especially for the importance of the data that has been stored in their databases. This means that the system was developed in a wrong or shallow way and this led to the data breach of 2011.



The data was not encrypted exposing it to a big threat

After a brief description of all the steps that were followed to perform the TRIPOD Beta analysis, here is shown a visual representation of the entire Tree (Figure 4):

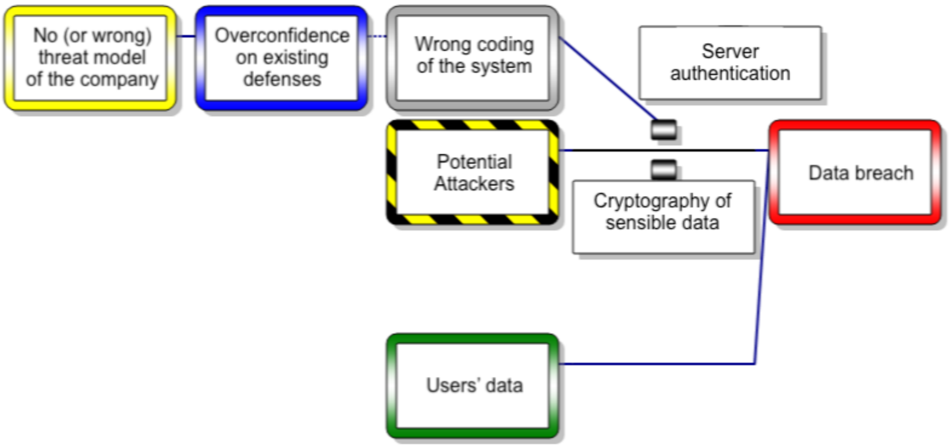

No (or wrong) threat model of the company
Overconfidence on existing defenses
Wrong coding of the system
Server authentication
Potential Attackers
Cryptography of sensible data
Data breach
Users' data

Figure 4: TRIPOD Beta analysis of the PlayStation Network data breach.

4.2. Anticipatory Model for Crisis Management (AMCM)

A crisis is a big event that threatens to harm an organization

Crises are an inevitable part of an organization's life and when they happen every institution has to be prepared in order to limit the consequences as much as possible. In our work, we decided to present the framework of the Anticipatory Model of Crisis Management applied to Sony's hack, a useful tool to better understand the outcomes of the actions taken by Sony's management to reduce the impact of the crisis.

A crisis is a major, unpredictable event that threatens to harm an organization and its stakeholders. Although crisis events are unpredictable, they are not unexpected (Coombs W.T., 1999). This type of event can seriously affect the reputation of a company if it directly compromises, for example, the safety of systems, customers, environment, or employees.

Crisis management is the process used to deal with these disruptive and unexpected events. Effective crisis management implies a proactive approach of the company. The Anticipatory Model of Crisis Management was created to support the entity during this process, especially during the pre-crisis phase. The AMCM focuses on the prevention of crisis, developing programs to identify possible crisis triggers and creating plans to manage crisis scenarios across all the organization's departments. The prevention phase is crucial because, in addition to safeguarding the system's health, it also suggests to the customer, and more in general to all the stakeholders, that the company is very committed to ensuring the quality of products, and the transparency of its business practices. The anticipatory model requires the support of communication to create an open dialogue within the organization and the public, this dialogue is very important to maintain, evaluate and improve the best practices of the company.

The AMCM requires the support of communication to create an open dialogue

The AMCM is based on three main components: *expectations, enactment,* and *control*.

- **Expectation**: includes the assumptions that people make about events when they happen. It is very important because is well known that assumptions via expectation can lead to a self-fulfilling prophecy.
- **Enactment**: is based on the assumption which suggests that the very action that enables the interaction of people and organizations can also lead to destruction. Enactment is focused on the process that leads to the completion of a given action and on its consequences.
- **Control**: correspond to the degree of power at the disposal of the organization to address the event.

These three components interact with each other, more precisely, expectations determine enactments (actions), which represent the control over the situations. AMCM needs to consider the interactions and interdependencies of the three components.

To sum up, the prevention of a crisis requires a deep knowledge of the relationships with all the stakeholders, both internal and external. Enactment corresponds to the specific actions that the company may take, expectation about something determines which type of measures will be taken in the enactment process. These measures will also determine the degree of control of the company to manage the crisis event. Altogether these factors and their relationships are the backbones of the anticipatory process of crisis prevention, which foresees the occurrence of an adverse and unexpected event and tries to reduce at minimum the repercussions of the crisis.

The analysis requires knowledge of the relationship with all the stakeholder

We decided to use AMCM to assess Sony's behavior during the data breach of the PlayStation's Network, searching for errors made by the company during the management of the hacking crisis. This process is useful to understand the missteps taken by the organization, and then identify some best practices for organizations to better handle these types of situations in the future.

During the spring of 2011, Sony committed several errors trying to manage one of the biggest data breaches of history. First of all, when they discovered the intrusion in their systems, they decided to not alert the customers until a week later. In addition to delays in communication, they did not tell to their customers that most likely many credit card information had been stolen. Instead, Sony declared that any financial data records were stolen. Secondly, when Sony figured out the security breach did not immediately shut down the network. Then, they wrongly blamed the Anonymous hacker group without hard evidence. The last Sony’s misstep analyzed is the failure to observe the self-imposed deadline to restore the network.

At first, Sony decided to not alert its customers of the ongoing intrusion

The first aspect of Sony's PlayStation Network hack deals with expectations and enactment components. It goes without saying that expectations play a key role in the analysis of the crisis. When customers are purchasing something using their credit card, they expect that the company will do whatever it takes to safeguards their credit card information. Sony failed to satisfy this expectation when its database, which contained more than 12 million credit cards, was stolen and hackers announced the intention to sell it. In this regard, Sony also failed to meet the expectations of the user concerning the security of the network. In fact, Sony announced the breach only after a week and only when they were sure that credit card information was stolen. To sum up, Sony waited until it was aware of the theft of the credit card information to announce the hack. This means that for a week customers could not protect themselves in any way because they had not been warned. The communication failure is very clear, given the fact that customers expect any sort of notification even if there is a small possibility that something has happened because they trust the company.

In this crisis, the communication failure is clear

After the discovery of the breach, Sony committed another big error by not shutting down the PlayStation Network immediately. Sony was the only one in this situation that had control over the security of its own network and customers always expect the best security. Unfortunately, during the attack, Sony could not act because they had chosen beforehand security measures which later proved to be insufficient (e.g. data were not encrypted and the server was vulnerable to simple SQL injections). As we can see, in this part of the analysis we can observe all of the elements of AMCM. Similar to the first aspect, Sony failed to inform players and did close the network after the discovery, this time not by choice, but because Sony's security had not noticed the intrusion. Many organizations during crisis management decide to not alarm the public, but this choice only reveals incompetence because, as we said before, customers trust the company and hiding what is happening to their data can lead customers to lose their trust. In addition to these considerations, we have to think about what would have happened if Sony had shut down the network immediately. Probably smaller information would have been stolen, but the most important thing is that a notification about what happened would have given customers the chance to take certain actions on their own (e.g. removing credit card information). The consumer always expects that the company has control over its environment and that it can take all the countermeasures to avoid any sort of threat. In this regard, Sony failed again to meet customers' expectations. One element of AMCM is control, this means that Sony needed to control the hackers? Of course not. The notion of control here refers to the possibility that Sony had to check if their security was the best available, and the lack of security measures for intrusion detection compromises the security of an entire system. LulzSec, the group responsible for the intrusion, declared that they did not want to appear as "master hackers" because they owned Sony with a very simple SQL injection. So, it is clear that Sony did not implement the best security available, but did Sony have any sort of protection? In fact, Sony did not apply any sort of encryption security neither on financial information. Again, Sony did not encounter the customers' expectations.

Sony's third problem, from the AMCM perspective, was the accusation of the Anonymous group. The company decided to blame the hacking group because Sony found a text file named "Anonymous" containing their motto ("We are a legion"). Anonymous promptly denied any responsibility with the breach claiming that they are not interested in stealing customers' personal information. While consumers were waiting for a response, Sony blamed the wrong group, disappointing expectations. The wrong accusation made people begin to consider that Sony wasn't willing to accept its own responsibility for the crisis.

The Anonymous' motto is "We are legion"

Next, Sony released a statement that said that the company was testing its new network and that the PSN would return "in the coming days". Unfortunately, the company missed the self-imposed deadline. When a tech company has any sort of problem linked to its network or products, consumers expect that the company is capable to understand how to restore or fix its architecture. So, when Sony declared that they would restore the network during the following days, and then failed to meet the deadline, it proved that they did not really understand how to fix the PlayStation Network. This situation deteriorated consumers' perception of Sony, which showed its lack of understanding of how to avoid further intrusions. After missing the self-imposed deadline Sony showed a lack of control over the functioning and security of its own network.

A swift hack turned into a multi-million dollar loss for the company

Sony at the time did not implement any anticipatory model of crisis management, and as their actions demonstrated, they did not have a clear idea of stakeholders' expectations. In AMCM the definition of stakeholders' reactions and expectations in a crisis is fundamental to avoid public relation errors that could be very costly in terms of image and revenues. In the case of Sony, the initial network crisis evolved into a wide-company crisis that cost Sony hundreds of millions of dollars. Sony did not understand the psychology of its consumers, not considering the dedication, trustworthiness, technological expectation, and emotional reaction of the players' community. Sony followed the traditional procedures of crisis management which have proved to be fallacious in handling this type of situation. These procedures completely ignored the new trend of preferences which coincides with instant-access to social and information technologies. This trend reveals another important factor: corporations must presume that their stakeholder base is the entire world. Communities around the world communicate with each other at an unprecedented speed using multiple types of devices and networks. So, when corporations are facing a crisis, they must communicate considering the entire world-based community that influences the expectations and preferences of the consumers.

Wrong perceptions of the company can impact on its history, image, and revenues for a long time, due to the persistence of world-wide discussions on community forums. Sony through its marketing campaigns communicates its reliability and technological superiority compared to Microsoft or Nintendo. So, when these perceptions created by Sony were challenged by the data breach the result was seen from the community as a betrayal of trust. Sony did not seem to be empathic with its customer when decided to not disclose the data breach at the moment they found it, then, decided to not disclose in a first moment the robbery of millions of credit card information, in addition to that, Sony always said that they were implementing the best security available and then what emerged is that they were exploited by a simple SQL injection and that they did not use any kind of encryption for their customer sensible information. Sony will suffer for many years the consequences of the failure in the management of the 2011 crisis, and this because they were following an issue-based traditional crisis management strategy, which assumes a specific event-response relationship. But the world has changed and with it also how consumers formulate their expectations on the corporations, under which they entrust their personal and sensible information. Traditional crisis management completely ignores the possibility of a flexible strategy modelled on the randomness and emotional responses of human nature. In this situation, Sony ignored too many times the human component of the crisis, focusing its effort on the technical part of the crisis and overlooking the public relations, that have a very important role since customers' information had been stolen.

An AMCM approach
requires a significant
effort for the company

An AMCM approach requires significant organizational and financial effort because, in addition to the past strategies, AMCM includes the analysis of human psychology which explains how people formulate their own perceptions, expectations, and conclusions. Sony in the management of the crisis situation completely failed to address the human nature of its stakeholder base. Also, from the technical point of view, Sony committed a lot of mistakes, although consumers could have another perception if the company would have been honest and immediately admitted the existence and the entity of the data breach.

In conclusion, we can say that the main mistakes committed by Sony when handling the crisis were four. Sony failed to disclose the breach until the following week after the incident and failed to inform the consumers that, in addition to their personal information, also their financial information might have been stolen. Sony did not immediately close the network. Sony decided to blame the wrong hacker group. Then, Sony claimed to re-open the network but failed its self-imposed deadline.

5. New threat model (Bow-tie model)

The Bow-Tie Model is very useful to visualize the risk correlated to an event in a concise way. The diagram, which has the form of a bow tie, helps the analyst to differentiate between proactive and reactive risk management by identifying the possible causes (on the left) and the possible consequences (on the right) of the event. For each possible cause, some barriers that might prevent this unwanted scenario from unfolding gets identified, while for each possible consequence, some other barriers that are aimed at recovering from or mitigating a loss of control before more serious consequences occur.

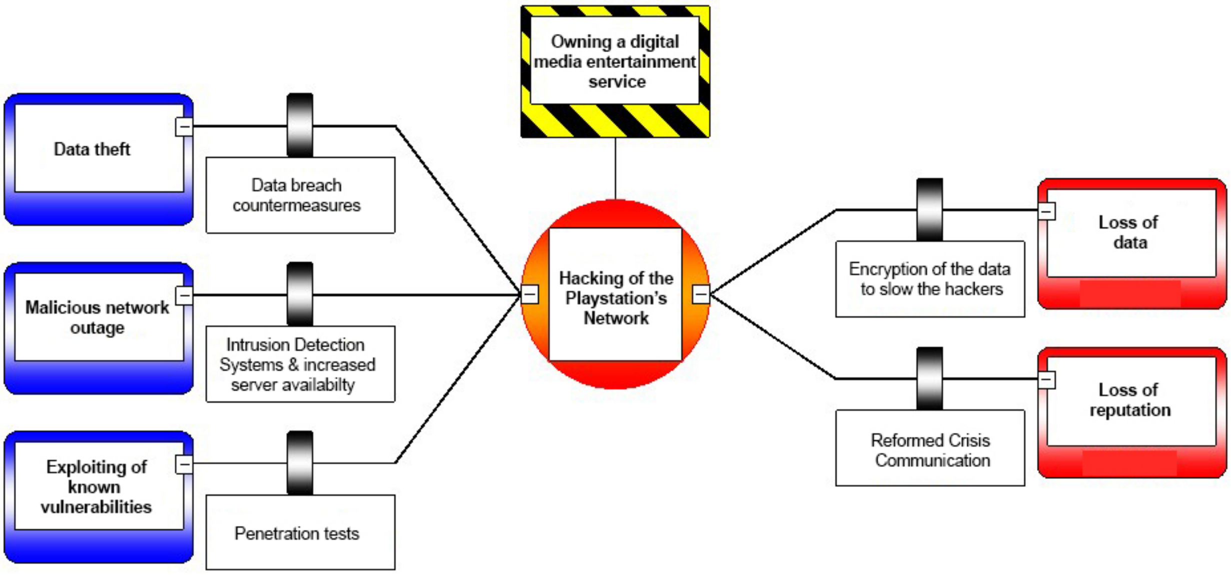
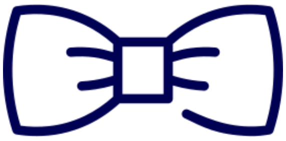

Owning a digital media entertainment service
Data theft
Data breach countermeasures
Malicious network outage
Intrusion Detection Systems & increased server availabilty
Exploiting of known vulnerabilities
Penetration tests
Hacking of the Playstation's Network
Encryption of the data to slow the hackers
Loss of data
Reformed Crisis Communication
Loss of reputation

Figure 5: Bow-tie Model of a future possible hack of the PlayStation Network.

Given the nature of the model, which aims at analyzing the risk correlated to a possible future event, it's a very good framework to see what Sony should have learned from the 2011 hack and what barriers to prevent and mitigate the event should already have been put into place by the company. Before starting the analysis, it is paramount to identify the hazard, meaning the part of the organization which has the potential to cause damage. In this case, the hazard is the mere fact of owning a digital media entertainment service, which obviously is not a hazardous aspect of an organization per se, but it has the potential to cause any sort of very bad consequences that we have seen in the previous paragraphs of this paper. This hazard is indeed the underlying cause of the main event, which is, once again, the hacking of the PlayStation™ Network, one of the company's most important asset. The first part of the analysis is aimed at finding what are the possible underlying threats and motivations that might lead a hacker to attack Sony's digital media entertainment service. Data theft is of course the first threat that should be taken into consideration given the broad spectrum that this type of attack can assume. A hacker might be interested to steal the data stored by the company for a number of reasons (to resell them, to expose the company, etc.) and Sony needs to put in place all the economically feasible countermeasures possible. An example of them would be to protect its databases from an SQL injection, which characterized the 2011 hack, by using prepared statements (with parametrized queries), which help avoiding to insert the values directly into the command, thus prevent the backend from running malicious queries that are harmful to the database (Table Plus, 2018). Another type of threat to consider would be a hacker causing an outage of the PlayStation™ Network, which, depending on the scale of the attack, would cause all sorts of damage to the public image of the company. This type of attack needs to be avoided because, especially nowadays, the customers/players' discontent will resonate through social networks and might result very hard to contain. A proper Intrusion Detection System (IDS), paired with a solution to grant the network availability at all time, would be a good countermeasure to this type of attack. Lastly, we should consider the more general threat of exploiting known vulnerabilities from hackers driven by a different purpose rather than money. This was the case of the original attack to the PlayStation™ Network, when hackers targeted specifically Sony for various reasons. One of the barriers that need to put in place to prevent this type of threat is definitely to perform various penetration test, aiming at different part of the system in order to find, time by time, the weakest ink of the network and work toward fixing the problems that affects it.



The Bow-tie model helps visualize the risk and the consequences of an event

The second part of the analysis focuses instead on the possible outcomes of the event and the repercussions that they might have on the company's objectives. Two of the main consequences identified, should a new hack of the PlayStation Network occur, are the loss of data and reputation among customers and investors. As far as the loss of data, it's a fairly straightforward problem, which, once occurred, there are very few things you can do, and most of them need to be done before the event itself. Learning from their experience, we believe that Sony has now put in place an encryption system for the data they are storing to make it harder for hackers to decrypt it, should they ever get ahold of it. The loss of reputation is a much harder and broader topic to deal with because it includes many facets of crisis handling. To avoid such naïve mistakes that have been made in 2011, it is reasonable to think that the company has reformed its Crisis Communication management while informing all of the people involved about how they should act properly in the case of a future crisis.

6. Conclusions

The reason behind the analysis of the Sony 2011 attack is that this can be considered one of the most important cyber-related events of the decade. The company was the leader in the sector and the attack caused an enormous loss in term of monetary gain and image of the company. Moreover, an attack directed to a technological giant gave to all the potential users the idea that not even data utilized in the mainstream platforms its completely secure. This inevitably incentivized the companies to invest more in the protection of sensible data.

The main model utilized in this paper was TRIPOD, useful in order to identify mostly human errors that caused attacks. The reason behind the choice of the model was the fact that most of the causes of the event were related to the wrong configuration of the system (e.g. no SQL countermeasures taken) or not implementation of some important security barriers (e.g. no cryptography on users' data).

However, due to the complexity of the event, it is necessary to focus also on the consequences of the event, in order to evaluate not only the defenses that Sony had to implement before the event, but also its reaction and its ability to manage the crisis. That is why it was also necessary to analyze the unfolding of the event using the Anticipatory Model for Crisis Management (AMCM), used to underline errors done by the company in all the phases that came after the data breach. In fact, it is really important to have a good crisis management in order to not increase possible damages to the company's assets, such as its reputation.

By analizing the crisis, a company can learn to improve its operations

The most important problem that emerged after the two analysis was the incorrect (or missing) threat modeling for the company. In this paper there is a proposal of a new Bow-Tie model for the enterprise that takes in account some of the aspects that were probably missing before the 2011 data breach. The importance of a correct threat modeling is clear while analyzing this event. In fact, not having any clue about the possible weak points of the company or the important assets to protect, not only leads to possible attacks, but also causes the impossibility to manage all the consequences correctly. This has a severe impact on the ability of the enterprise to ensure business continuity, an aspect that is fundamental for all the organization, especially for a society that provided an online gaming platform as a service. A long downtime period causes an enormous economic loss and also could lead users to abandon the services provided by the company allowing competitors to gain important market shares.

7. References

- Sony Corporation. “Annual Report 2011”. 31 March 2011, <https://www.sony.net/SonyInfo/IR/library/ar/SonyAR11-E.pdf>
- “Nintendo Wi-Fi Connection.” Nintendo of Europe GmbH, <https://www.nintendo.co.uk/Wii/Get-Connected/Nintendo-Wi-Fi-Connection/Nintendo-Wi-Fi-Connection-626434.html>
- AFJV. “Global console unit sales from 2012 to 2016, by type (in millions) [Graph]”. In Statista. <https://www.statista.com/statistics/255194/global-console-unit-sales-by-type/>
- “PlayStation®Network.” PlayStation, <https://www.playstation.com/en-ae/explore/playstation-network/>
- Sliva, Marty. “E3 2013: PlayStation Plus Required for PS4 Online Play.” IGN, IGN, 13 July 2016, <https://www.ign.com/articles/2013/06/11/e3-2013-playstation-plus-required-for-ps4-online-play>
- Loveridge, Sam. “Sony Explains PlayStation Plus Requirement for PS4 Online.” Trusted Reviews, Trusted Reviews, 27 June 2013, <https://www.trustedreviews.com/news/sony-explains-playstation-plus-requirement-for-ps4-online-2905669>
- Fox News (2011). “A Brief History of the LulzSec Hackers”. <https://www.foxnews.com/tech/a-brief-history-of-the-lulzsec-hackers>
- Baker, L. B. and Finkle, J. (2011). “Sony PlayStation suffers massive data breach”. <https://www.reuters.com/article/us-sony-stoldendata/sony-playstation-suffers-massive-data-breach-idUSTRE73P6WB20110427> [Last visit: December 7th 2019]
- Anthony, S. (2011) “How the PlayStation Network was Hacked”. < https://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked> [Last visit: December 7th 2019]
- Seybold, P. (2011) “Settlement in George Hotz Case”. <https://blog.us.playstation.com/2011/04/11/settlement-in-george-hotz-case/> [Last visit: December 7th 2019]
- Rashid, F.Y. (2011) “Sony Data Breach Was Camouflaged by Anonymous DDoS Attack”. <https://www.eweek.com/security/sony-data-breach-was-camouflaged-by-anonymous-ddos-attack>
- “Absolute Sownage: A concise history of recent Sony hacks” <http://attrition.org/security/rant/sony_aka_sownage.html>
- “PlayStation Network Hack Timeline” <http://totherails.blogspot.com/2011/05/playstation-network-hack-timeline.html>
- Williams, Martyn. “PlayStation Network Hack Timeline.” CSO Online, CSO, 27 Apr. 2011, <https://www.csoonline.com/article/2128353/playstation-network-hack-timeline.html>
- Anderson, Nate, and Utc. “‘Anonymous’ Attacks Sony to Protest PS3 Hacker Lawsuit.” Ars Technica, 4 Apr. 2011, <https://arstechnica.com/tech-policy/2011/04/anonymous-attacks-sony-to-protest-ps3-hacker-lawsuit/#>
- Chirgwin, Richard. “PSN Hack Triggers Lawsuit.” • The Register, The Register, 28 Apr. 2011, <https://www.theregister.co.uk/2011/04/28/sony_psn_sued/>
- Wisniewski, Chester, et al. “Sony Succumbs to Another Hack Leaking 2,500 ‘Old Records.’” Naked Security, 7 May 2011, <https://nakedsecurity.sophos.com/2011/05/07/sony-succumbs-to-another-hack-leaking-2500-old-records/>

- Williams, Martyn. “Sony Resuming PlayStation Network, Qriocity Services.” Computerworld, IDG News Service, 14 May 2011, <https://www.computerworld.com/article/2508060/sony-resuming-playstation-network--qriocity-services.html>
- Seybold, Patrick, et al. “Update on PSN Password Reset Process.” PlayStation.Blog, 18 May 2011, <https://blog.us.playstation.com/2011/05/18/update-on-psn-password-reset-process/>
- Panzarino, Matthew. “Not so Fast: Sony's PlayStation Network Hacked Again - TNW Industry.” The Next Web, 18 May 2011, <https://thenextweb.com/insider/2011/05/18/not-so-fast-sonys-playstation-network-hacked-again/>
- Sony Ericsson Got Hacked by Idahc - Lebanese Hacker.” The Hacker News, 22 June 2011, <https://thehackernews.com/2011/05/sony-erricson-got-hacked-by-idahca.html>
- Fogarty, Kevin. “Latest Hack Shows Sony Didn't Plug Holes.” PCWorld, ITworld, 5 June 2011, <https://www.pcworld.com/article/229421/latest_hack_shows_sony_didnt_plug_holes.html>
- Olaniran, Bolanle A., et al. “A Gamers Nightmare: An Analysis of the Sony PlayStation Hacking Crisis.” Journal of Risk Analysis and Crisis Response, vol. 4, no. 3, 2014, p. 151., <doi:10.2991/jrarc.2014.4.3.4>
- “8 Best Practices to Prevent SQL Injection Attacks.” *TablePlus*, 19 Aug. 2018, <https://tableplus.com/blog/2018/08/best-practices-to-prevent-sql-injection-attacks.html.>