A Virtue Ethics Analysis of the 2011 PlayStation Network Data Breach

STS Research Paper
Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia

By

Kyle Peter

April 10, 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____
Kyle Peter, B.S. Mechanical Engineering & Engineering Business Minor, University of Virginia Class of 2020

Approved: _____ Date _____
Benjamin J. Laugelli, Assistant Professor, Department of Engineering and Society

Introduction

In 2011 the Playstation Network (PSN) experienced one of the largest data breaches of the twenty first century. PSN is Sony's online gaming and video streaming service and can be accessed through Sony game consoles; the current console was the PlayStation 3 (PS3). At the time, the network used 130 server systems, 50 software programs, and had 77 million user accounts. On April 19, 2011, Sony engineers noticed six PSN servers rebooting themselves off schedule, prompting a week-long shutdown of PSN entirely for a thorough investigation. The shutdown meant that users could not play any Playstation games online. A week later, on April 26, Sony released an official statement that the PSN was hacked by an unknown individual and the personal information (names, addresses, possible credit card information) of all 77 million users had been compromised (Sherr, 2011). Sony reportedly spent upwards of 171 million USD to cover the costs of the massive security breach and has vehemently withheld information on the identity of the hacker and the manner in which its servers was hacked (Martinez, 2011).

The agent in question, Sony, has mainly been examined on its security measures and communication methods leading up to and after the breach. This approach to analyzing the breach fails to consider the characteristics of Sony that define its morality as an engineering collective. This underlines a widespread lack of understanding in the role and importance of morality in such cases. Through the ethical framework of virtue ethics, I argue that Sony acted immorally by failing to practice two necessary virtues of a morally responsible engineer: "expertise" and "openness to correction." The morality of the acting individual or acting body hinges upon the clear presence and implementation of these virtues, without which the individual or body is deemed immoral (Pritchard, 2001).

Background

In order to evaluate the shortcomings of Sony, it is necessary to outline key technologies in network-based systems. The most typical first line of defense against any sort of intrusion is a firewall: a network security device that both monitors incoming and outgoing online traffic and decides whether to allow or block said traffic within the confines of set guidelines. Firewalls are the barriers between the controllable and the uncontrollable, the trusted and the untrusted, or the internal network and the external internet (What is a firewall, n.d.). A web server houses information for a website and delivers it to users when called upon (What is a web server, n.d.). Web servers are almost like living systems because they can be updated, or patched, as time elapses to improve stability and prevent against technical vulnerabilities. Patches are integral to web server security because, according to the 2015 Verizon Data Breach Investigations Report, 70% of successful cyberattacks exploited known vulnerabilities (Why you should patch and update your PCs and server computers, n.d.).

Although the hacking individual/group and method are still unknown, a number of plausible theories drive the conversation on how PSN was breached. Jon Heimerl, director of strategic security for security service provider Solutionary, believed the breach could have started with a mistake. Heimerl suspected hackers entered the network by taking control of the personal computer of a Sony administrator, someone with restricted access to sensitive information on Sony's customers. This could have been executed by means of an email sent to this administrator with a malicious software disguised as a downloadable attachment (Rashid, 2011). Others believe the attack may have been a continuation of efforts from a large hacking conglomerate, Anonymous, by means of an SQL injection attack: a common cyber-attack method that uses malicious structured query language (SQL) code to manipulate backend

databases and retrieve information that was not intended to be displayed (SQL [structured query language] injection, n.d.). Another line of thought stems from the then recent release of a custom PS3 firmware (a set of instructions programmed on a hardware device) called Rebug, which effectively turned a user's PS3 into a developer unit, granting access to a plethora of features not intended for public use. Most importantly, the Rebug firmware gave the user trusted access to Sony's internal developer network (Anthony, 2011). Any individual theory or combination of theories can explain the PSN breach, but one can do no more than speculate because of Sony's secrecy in the matter.

Literature Review

The majority of researchers who study the breach of the Sony Playstation Network (PSN) tend to examine the effectiveness of user compensation and the government actions that should ensue. The existing works fail to examine the vulnerability of Sony's security technology and the morality of Sony in failing to address it. Sigi Goode and his colleagues present a novel study on how Sony reacted to this breach in regards to its customers and how those customers received this compensation. Through expectation confirmation research on users/consumers rather than broad market research, he developed three main conclusions: (i) compensation is a fitting and adequate response to data breach as long as it meets customers' expectations, (ii) overcompensation does not pay off, and (iii) a failure to understand consumer expectations can undermine the whole response effort. Goode et al. also go on to illustrate a greater need for a "broader theoretical view when examining security policies" that encompasses both actions to prevent and respond to such a breach (Goode et al., 2017).

Lance Bonner outlines the events of the data breach and Zurich's successful effort to file for a release of any duty to indemnify Sony in the context of the corresponding claims. The study

then goes on to explore the landscape of cyber risk-related insurance and how the insurance offered to major corporations dealing with data were severely outdated and not comprehensive enough to cope with and/or cover the losses experienced during a data breach. Bonner ends by urging the federal and state government to encourage the expansion of cyber insurance risk adoption among business and organizations in the US (Bonner, 2012). Both Goode et al. and Bonner focus on the consequences and reactions of the data breach, but fail to address its root cause.

While the discussed viewpoints offer valuable lenses with which to evaluate the breach and its aftermath, there is an ethical and technical void that has gone unmentioned regarding Sony's software. To address this void, I will use the virtue ethics framework to evaluate the actions of Sony.

Conceptual Framework

To assess the morality of Sony in the PSN data breach, I will employ the ethical framework of virtue ethics. More specifically, I will draw upon two of Michael Pritchard's virtues for morally responsible engineers: "expertise" and "openness to correction." Virtue ethics is an ethical theory driven by human development; an individual's characteristics can be shaped and nurtured through both education and the examples set by his or her surroundings. In developing the theory, Aristotle focused on the actor and his or her characteristics for a basis of moral judgement. The morality in question relies on the quality of the acting individual rather than the action or the subsequent consequences. To live a "good life" and act in a moral manner in accordance with the framework of virtue ethics, one must strive for or possess, at minimum, a set of good or desirable characteristics otherwise known as virtues. This virtuous and "good" life

can be found as a middle course between two extremes. For example, courage is the middle course between the extremes of cowardice and recklessness (van de Poel & Royakkers, 2011).

There are a number of general virtues such as reliability, honesty, courage, and justice. However, many industries have their own virtues that take into account the specificities of the nature of work done. In my employment of virtue ethics, I consider the acting individual to be Sony Corporation. Pritchard's list of virtues, shown below in Figure 1, is tailored specifically for "morally responsible engineers," providing an apt moral baseline in this case since the cause of the data breach was technical and related to software.

1. Expertise
2. Clear and informative communication
3. Cooperativeness
4. Willingness to compromise
5. Perseverance
6. Habit of documenting work thoroughly and clearly
7. Commitment to quality
8. Openness to correction
9. Being imaginative
10. Seeing the "big picture" as well as the details of smaller domains

Figure 1: Pritchard's List of Virtues for Morally Responsible Engineers

Although comprehensive, the list is not all-encompassing as there can be more virtues both general or specific. However, Pritchard emphasizes that lacking even one of the included virtues displays a lack of "responsible engineering practice" (Pritchard, 2001). In Sony's case, it lacked more than one of these virtues, which provides grounds with which to question its morality.

Analysis

For the argument of this paper, I will treat Sony as a collective of engineers due to the fact that individual employees act in unison under the values and vision of the larger, holistic company. Of the many values Sony expresses on its official website, the most notable ones are "Integrity & Sincerity" as it strives to "earn the trust for the Sony brand through *ethical and responsible conduct*" (Sony's purpose & values, n.d.). Ironically in the aftermath of the PSN data

breach, Sony lost a great deal of trust among its customers as a consequence of its arguably unethical and irresponsible conduct. According to Pritchard, the absence of just one virtue undermines the morality of the acting agent; Sony lacked both expertise and openness to correction.

Expertise

In evaluating the 2011 PSN data breach, Sony failed to exhibit a key virtue of "expertise" that the morally responsible engineer should hold paramount. Cambridge Dictionary defines expertise as "a high level of skill or knowledge" (Meaning of expertise in english, n.d.). Given Sony was founded over 60 years ago and has had such a significant grip on the tech industry in at least the last 20 years, one can reasonably expect a high level of skill or knowledge to be built into every product and service provided by the company. More specifically, a PSN user in 2011 could have expected that Sony would employ its expertise to develop, implement, and maintain a sophisticated security mechanism around the network. Unfortunately, 77 million PSN users fell victim to Sony's failure to uphold this particular virtue.

Given the importance to firewalls to cyber security, it would seem obvious that Sony would protect the PSN with at least one form of firewall. Yet, for unknown or unexplored reasons, Sony chose not to use firewalls of any kind to protect the PSN in the years leading up to 2011. To make matters worse, Sony was using "outdated versions of the Apache Web server with no patches applied on the PSN" (Wang et al., 2015). The choice of web server was not the issue as the Apache Web server powers 46% of websites around the world today (G., 2019); the issue was rooted in the clear lack of both a firewall and patches to said server. As a consequence, Sony fell prey to such an attack. Firewalls and web server patches are incredibly commonplace

in the network security world and an omission of either, let alone both, points to an egregious lack of expertise.

In the eyes of Alan Paller, research director of the SANS Institute, Sony did not pay enough attention when developing its software. Under pressure to innovate rapidly and release cutting-edge technology ahead of competitors, companies like Sony sometimes allow security to "take a back seat." Paller states that new software almost always has errors, creating a window of opportunity for hackers in the absence of sufficient security measures (Baker & Finkle, 2011). The fact that large tech companies must innovate rapidly should not be a surprise to anyone, but that should put an even greater emphasis on security to safeguard what is being released and used by the public. The motivation to do so is driven by the virtue of expertise, one that Sony failed to exhibit in its actions leading up to the breach.

Openness to Correction

Another virtue Sony failed to adhere to within virtue ethics was "openness to correction," which added to its apparent immorality in the 2011 PSN data breach. Correction, in an engineering capacity, can come in many forms and is an invaluable tool to improve a product or service and provide outside insights that the engineer is unaware of. In order to leverage correction or criticism as an invaluable tool, the engineer must first be willing to listen to what is being said and implement changes if necessary. The correction Sony received in the months leading up to the PSN data breach took different and rather unorthodox forms but still held great potential value to the company and its engineers. Instead of absorbing and addressing the criticism, however, Sony displayed a demonstrable lack of openness to correction and eventually suffered the associated consequences.

The first example of Sony's failure to demonstrate an openness to correction concerns the actions of Anonymous, one of the world's largest decentralized "hacktivist" groups known for its high profile distributed denial of service (DDoS) attacks. In January 2011, PlayStation 3 hacker George Hotz broke into the PSN and pirated games that he then distributed to the public. Sony responded by attempting to take legal action against Hotz, but the case was settled. Since Hotz was a "fellow hacker," Anonymous caught wind of the incident and issued a public threat to Sony on April 4, 2011 in which it called Sony's responsive actions "wholly unforgivable." The statement went on to warn, "now you will experience the wrath of Anonymous. You must face the consequences of your actions, Anonymous style" (Phillips, 2016). The threat from Anonymous intimates that Sony overstepped a boundary and the company must be punished in a way that suits Anonymous' expertise. Given Anonymous' previous, extremely notable DDoS attacks on very prominent, global players (eg. MasterCard, PayPal, the U.S. military, and the federal governments of Australia, Egypt, Iran, and Zimbabwe), the group's threat gave a reasonable expectation that the "consequences" would take the form of a DDoS attack (What is Anonymous, 2013). The success of Hotz was a very clear criticism of the frailty of the PSN network security and the threat of Anonymous was an even more clear caution for Sony to address that frailty. According to Pritchard, a morally responsible engineer would exhibit the virtue of "openness to correction" and, although the correction was of hostile nature, address the message and act upon it (Pritchard, 2001). However, Sony made no changes to its security protocol in the face of this criticism and, therefore, demonstrated immoral character.

As I have argued, Sony failed to attend to information that could have helped strengthen its network security and prevent the breach, pointing to its lack of openness to correction. However, the CEO of Lieberman Software, Philip Lieberman, contends that the failure, not

immorality, lies in the auditors who neglected to acknowledge the risk that Sony was taking with its outdated technology (Rashid, 2011). While this can be contested, it is important to note that Sony was already made aware of this outdated technology by the previously mentioned threat by Anonymous as well as security forums monitored by Sony employees. The source of this correction was Gene Spafford, a cyber security expert and Computer Science professor at Purdue University. In an oral testimony to the House Subcommittee on Commerce, Manufacturing, and Trade on May 4, 2011, Spafford revealed that the security vulnerabilities of the PSN were flagged on security forums two to three months prior to the breach. These forums were monitored by Sony employees (Ogg, 2011). Evidently, Sony was made aware of its security issues *months before* the PSN and its 77 million users were affected but the company failed to address the issues, underlining the company's lack of openness to correction. Thus, the immorality heavily lies in the hands of Sony and not in those of the auditors.

The fact that they were flagged over online forums should not detract from the validity of the warning. A number of Sony employees deliberately and closely followed the discussions on these security forums, meaning the company placed some sort of value on what was being said. With knowledge of these vulnerabilities in hand, Sony failed to fortify its security technology and consequently kept the information of its customers at risk. Pritchard argues that the omission of one virtue for morally responsible engineers deems an engineer immoral, and Sony can be deemed immoral on those grounds in two scenarios leading up to the eventual PSN breach due to its lack of openness to correction. Evidently, Sony let its immoral characteristics take the forefront in the months leading to the PSN breach due to its inherent lack of two key virtues for morally responsible engineers: expertise and openness to correction.

Conclusion

Although Sony has kept many details of the breach secret, there is sufficient information to develop a judgement on the morality of its corporate character. By failing to exhibit two virtues paramount to morally responsible engineers, expertise and openness to correction, I have argued that the character of Sony was immoral. Sony continuously ran outdated software and upon being made aware of this deficiency did not enact any changes to improve the security of its technology.

Amidst a technical failure such as a data breach, it is acceptable and sufficient to evaluate the technical and non-human deficiencies that opened the door to infiltration. However, to understand the character and morality of the acting individual is to go one step further past what is sufficient. This gap in understanding is critical to acknowledge and explore because the morality behind acting individuals play integral roles in events such as this. Technology companies now possess an immense amount of information on their users and a constant, close eye on the morality of these companies can be a key factor in ensuring both the safety of our information and the implementation of appropriate security measures to protect it.

References

Anthony, S. (2011, April 27). How the PlayStation network was hacked. ExtremeTech. Retrieved from https://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked

Baker, L. B., & Finkle, J. (2011, April 26). Sony PlayStation suffers massive data breach. *Reuters.* Retrieved from https://www.reuters.com/article/us-sony-stoldendata/sony-playstation-suffers-massive-data-breach-idUSTRE73P6WB20110427

Bonner, L. (2012). Cyber risk: How the 2011 Sony data breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches. *Washington University Journal of Law & Policy, 30*(257), 257–277.

G, D. (2019, November 25). What is apache? An in-depth overview of apache web server. Retrieved February 28, 2020, from https://www.hostinger.com/tutorials/what-is-apache

Goode, S. A., Hoehle, H. A., Venkatesh, V. A., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly, 40*(3).

Martinez, E. (2011, May 24). PlayStation network breach has cost Sony $171 million. *CBS News.* Retrieved from https://www.cbsnews.com/news/playstation-network-breach-has-cost-sony-171-million/

Meaning of expertise in english. (n.d.). Retrieved February 28, 2020, from https://dictionary.cambridge.org/us/dictionary/english/expertise

Ogg, E. (2011, May 3). The PlayStation Network breach (FAQ). Cnet. Retrieved from https://www.cnet.com/news/the-playstation-network-breach-faq/

Phillips, T. (2016, April 26). Five years ago today, Sony admitted the great PSN hack.

Eurogamer. Retrieved from https://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today

Pritchard, M. (2001). Responsible engineering: The importance of character and imagination. *Science and Engineering Ethics, 7*(3), 391–402.

Rashid, F. Y. (2011, May 6). Sony networks lacked firewall, ran obsolete software: testimony. EWeek. Retrieved from https://www.eweek.com/security/sony-networks-lacked-firewall-ran-obsolete-software-testimony

Sherr, I., & Wingfield, N. (2011, May 7). Play by play: Sony's struggles on breach. *The Wall Street Journal.* Retrieved from https://global-factiva-com.proxy01.its.virginia.edu/ha/default.aspx#./!?&_suid=158290758776704301718131402661

Sony's purpose & values. (n.d.). Retrieved February 28, 2020, from https://www.sony.net/SonyInfo/CorporateInfo/purpose_and_values/

SQL (structured query language) injection. (n.d.). Retrieved February 28, 2020, from https://www.imperva.com/learn/application-security/sql-injection-sqli/

van de Poel, I., & Royakkers, L. (2011). Ethics, technology, and engineering: An introduction. Hoboken, NJ: *Blackwell Publishing Ltd.*

Wang, P., Ali, A., & Kelly, W. (2015). *d*ata *s*ecurity and *t*hreat *m*odeling for smart city infrastructure. 2015 international conference on cyber security of smart cities, industrial control system and communications (SSIC).

What is a firewall? (n.d.). Retrieved February 28, 2020, from https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

What is a web server? (n.d.). Retrieved February 28, 2020, from

https://www.nginx.com/resources/glossary/web-server/

What is Anonymous? (2013). Retrieved February 28, 2020, from http://www.nbcnews.com/id/41895501/ns/technology_and_science-security/t/what-anonymous/#.XlmEg5NKgWp

Why you should patch and update your PCs and server computers. (n.d.). Retrieved February 28, 2020, from https://www.spiceworks.com/it-articles/patch-and-update-pc-and-server-computers/