Hacktivism: How to Respond and Build Around Hacker Communities

Eric Sembrat
IS 8300 - Disaster Recovery and Contingency Planning
Fall 2011
October 21, 2011

ABSTRACT

To understand the true nature of incident response (IR), disaster recovery (DR), and business continuity (BC), company case studies prove to be excellent examples of realistic in-practice processes. Sony Corporation, most popular for their electronics division, was beset by a series of digital break-ins and hacks in 2010 and 2011. Because of these series of hacks, this paper will define the hacks in regards to their severity and level, as well as establishing how Sony responded and revamped their operations.

1.INTRODUCTION

By its definition, hacktivism is merely a specific definition of the more widely used term hacker. A hacktivist is a user who engages in hacker activities for one goal: protesting corporate or political policy [15]. Unlike the generalized definition of the term hacker, however, hacktivists are have a goal in mind when hacking a person or interest on the web. In this case, these goals are negative and range from accessing and downloading data from corporate servers to defacing a public-facing website. For the sake of simplicity, this paper assigns hacktivism as being strictly confined to negatively-oriented goals, due to the legal and ethical implications that come from hijacking private information.

The roots of hacktivism go as far back as the late 1990s, with pioneer hacker collective group Electronic Disturbance Theater (EDT) countered Mexican government policies by virtual sit-ins, which took the form of distributed denial of service attacks (DDoS) attacks [25]. A DDoS, by definition, is a technique of multiple computers working in-sync to transmit traffic to and from a website repeatedly, which results in the servers hosting the website either crashing or failing to respond; thus, the 'denial of service' aspect [9].

The efforts of the EDT predate the unprecedented rise of the "flat world" (as coined by Thomas L. Friedman), where corporations suddenly had an opportunity to act, move, and respond globally as a consequence of widespread adoption of the Internet [30]. Suddenly, as Friedman states in his 2005 interview with magazine Wired, Indian and Chinese workers now could compete for work in a web-enabled collaborative playing field that disregarded the traditional barriers of geography, distance, and (in some cases) language. And as a consequence of the flat world, data storage became cheap, data communication exponentially grew, and some aspects of our physical world began to move towards being Internet-dependent. As the Internet-dependency spread, so did the impacts of digital attacks such as DDoSs.

2.ENTER: ANONYMOUS

The hacker collective group Anonymous came to international spotlight in 2008 as a response to anti-WikiLeaks backlash and the civil unrest in Egypt in Tunisia, spurred by the governments' efforts to silence its citizens by taking down its Internet connectivity [25]. However, the origins of the hacktivist collective are seeded in an Internet message board known simply as /b/. A purposefully-designated off-topic discussion board on the popular forum 4chan.org, /b/ is composed of thousands of anonymous self-claimed "/b/tards" posting discussion topics that correlate well with high-school bathroom stall graffiti: profane, crude, and obscene [35]. The New York Times article "The Trolls Among Us" profiles some of the /b/ community missions, from simple high-volume prank calls to the pointed and repeated harassment (both online and offline) of popular technical co-author Kathy Sierra.

/b/ branded the Anonymous image during their 2008 harassment of Scientology group leaders and members, encouraged by the church's "secretive and litigious nature" [5]. The newly formed members of Anonymous, banded together solely through an Internet discussion board, conducted DDoS attacks against Scientology websites, fax and email spams, all in an effort to disrupt the church's operation. Outside of the Internet, founding Anonymous members donned Guy Fawkes-style masks popularized in the popular graphic novel and movie 'V for Vendetta' and publicly protested local Scientology offices [6], thereby legitimatizing the Anonymous movement and rebranding the Guy Fawkes-style mask as a de facto logo.

Moving beyond /b/, Anonymous outgrew its parental home as its ranks expanded to over 1,000 loosely-knit members, commanded by no one and spurred only by what 22-year-old spokesperson 'Coldblood' referred to as "when the spirit moves them" [39]. As an unbounded and fluid loose organization of knowledgeable Internet hackers, their scope and scale can only be matched by the freedom their Internet anonymity allows them.

3.CRASHING THE PARTY: LULZSEC

Anonymous began an orchestrated attack on security consultants HBGary Federal in February 2011, as a response to the security company attempting to profile Anonymous members [16]. After Anonymous retrieved company records and emails from HBGary, the hacktivist group splintered. A small group of Anonymous leaders, most of whom orchestrated the HBGary hack, decided to start a second hacktivist group named LulzSec [23]. The name of the splinter group is derived from a portmanteau of the Internet-language acronym 'lol' (stylized as 'lulz') and security. As Samantha Murphy reported in her September 2011 NewScientist

article Agents provocateurs, LulzSec blasted right through the fine line between civil disobedience and criminality [25].

LulzSec, rather than working slowly and focusing on singular targets, used a 50-day period to attack American state and local law enforcement agencies, security consultancy companies, and American corporations [23]. With a smaller team of hackers, the hacktivist group is able to coordinate fast-paced and frequent attacks and communicate quicker on social networks such as Twitter. LulzSec, as an example, was able to take down the public-facing sites of the Central Intelligence Agency (CIA) and Sony.

4.CASE ANALYSES

The three cases below outline the three major areas to which businesses must include in their business plans to counter any Internet-dependency risks and protect their private data, which is increasingly becoming a more valuable asset. Because of the interconnectivity between the global Internet and information management and technology, it is paramount that these analyses are used to enforce company information strongholds. Without this, the company data (and much of their company trustworthiness) is lost.

The three areas analyzed are: incident response, disaster recovery, and business continuity. Each of these three areas will be analyzed over one of Anonymous' and Lulzsec's most prolific and publicized hacks: Sony Corporation.

5.IR - UNLOCKING THE PS3

Anonymous' motivation for hacking Sony Corporation as a whole was centered around legal litigation against two small-time hardware hackers. In January of 2011, hackers George Hotz ("geohot") and "Bushing", alongside less-involved parties, discovered a backdoor loophole in the Sony Playstation 3 hardware that identified the 'root key' [12]. A root key is a long hexadecimal code that allows software code to be authorized ('signed') for usage on the console [32]. The risk here is that with the key, any programmer can now develop Sony Playstation 3-compatible code, encode it with the proper key, and run it on the video game console.

Sony was targeted by geohot and Bushing primarily due to the company removing the functionality of the Playstation 3 to boot Linux, which geohot initially targeted due to its ease-of-access to the lower level game system functionality [38]. As Keith Stuart of The Guardian notes, the removal of Linux on the Playstation 3 raised red flags with the home-brew (skilled computer users who develop tools and applications for consoles) community, and by association, the hacker communities. Thus, Sony's own efforts to secure their platform led to increased attention and hacking towards the console.

This is the first incident that Sony Corporation encountered, and the company's response was two-pronged: stop the hackers, and stop the information flow. However, the response took a full week (January 1 to January 7) to formulate and begin execution.

In order to stop the hackers from distributing the root key for the console, Sony Computer Entertainment lawyers approached a San Francisco District Court Judge in California to block the release of the code, citing "violations of the Digital Millennium Copyright Act (DMCA), the Computer Fraud and Abuse Act, plus breaches of California copyright law, breach of contract, and other violations" [12]. The DMCA law specifically outlines "anti-circumvention" provisions, where the loopholes of access controls and technical protection measures were deemed unlawful [8]. The root key's publication falls into the category of "anti-circumvention", as the key would easily be used to personally authorize software for the Playstation 3, bypassing Sony's internal guidelines for doing so.

Sony argued that the release of the root key would open the floodgates to illegally copied or pirate games, and that the root key was essential in keeping the PS3 functioning in a "safe and reliable manner" [13]. The reality of the situation confirmed Sony's fears, as software pirates were quickly using the rootkit tools to assign large numbers of trophies (digital achievement items attached to a user profile on the Sony portal network) to their profile, running modified versions of games, and pirating games onto the video game system [14].

After three months of heavy litigation and debate, Sony and the two key hackers reached a joint statement agreeing to a permanent injunction. The injunction prompted the two hackers to remove and destroy their PS3 hacking resources, including the root key, from their websites [26].

While Sony's legal response had stopped the faucet from leaking further in regards to technical hack discoveries, many loose ends still existed: other hackers were not named in the joint agreement, BitTorrent sites across the web continued to spread Playstation 3 hacking documentation, and the root key was still easily available from a search engine [27]. Thus, Sony's response then had to extend beyond the source to its constituents, as the information was now freely available throughout the Internet and still posed a great threat to the company's console and online services.

Sony, looking to diminish the number of users using the hacked tools and root key to run unauthorized software, released a statement in February 2011 that any software discovered while connected to the Sony Playstation Network (the Playstation 3's online portal) would be banned from the service permanently [26]. Each user would be issued a cease-and-desist order regarding the usage of unauthorized software; failure to comply with the cease-and-desist would result in the account being banned, prompting the user that the account "has been terminated permanently due to the use of unauthorized circumvention devices and unauthorized or pirated software on your PlayStation 3 system" [24].

Beyond stopping unauthorized software from being used on its portal service, there was not much Sony could do as an initial response. The root key and related software tools spread like fire through message boards, file sharing services ('bitlockers'), and BitTorrent communities. However, the company soon realized that the key to controlling the fallout was to engineer the Playstation 3 video game console to react to the tools and unauthorized software. Sony released a firmware update more than three weeks after the initial root key leak to "add a security patch", which prevented the root key from being used to run unauthorized software [14].

Though hackers were able to dissect the security patch and release the firmware-added keys, Sony had a short-term tug of war battle that gave the company the leading edge. Sony could, for the foreseeable future, continue to roll out firmware updates for "security updates" that did nothing but blacklist vulnerabilities and unauthorized key usage. Because the Sony Playstation 3, much like the Microsoft XBOX 360, require that users check for and install firmware updates before using its online services, Sony had the short-term and long-term solution packed into one. In the short-term, the firmware updates would be utilized to continuously keep pace with hacker group releases. Long-term,

firmware updates allow Sony an avenue for updating the console with stricter anti-circumvention measures.

While Sony was able to respond appropriately to the software hacking of the Playstation 3, hacker groups began to focus their attention to Sony in the wake of what the groups saw as corporate crackdowns. Anonymous, in an April 4th 2011 press release, referred to Sony's actions as an "[abuse of] the judicial system in an attempt to censor information". At the end of the press release, Anonymous made their future intentions known, citing that "now [Sony] will experience the wrath of Anonymous" [20].

Anonymous' first response to Sony was coordinated DDoS attacks against public-facing Sony websites [37]. While this is inconvenient, Sony can do little to determine which Internet traffic is legitimate and which are the result of a hacker community. In addition, a DDoS is short-term - eventually the DDoS loses its potency through a decrease in actors engaging in the denial-of-service. Sony's only options are to devote more network connectivity to their public-facing sites, or place regional redirects to forward users of a particular region to a separate physical server, in order to minimize the damage of a over-saturated network.

Over time, the 'distributed' aspect of the Sony DDoS loses its luster and the denial-of-service is rendered less-effective (if not ineffective). However, the next step in the attack was prompted not by Anonymous, but rather the smaller (and more dangerous) group LulzSec.

6.IR - SQL INJECTIONS

LulzSec discovered that a simple SQL injection attack could give the hackers access to the company's servers (and thus gain access to Sony's internal information). LulzSec is quoted as saying the SQL injection attack was executed in just under three days in June 2011 [22]. SQL is a popular database storage solution for websites and web applications and does not inherently have a flaw in its design [33]. The flaws exist in the website pages themselves, as Ian Paul of PCWorld magazine explains, where an online form can be manhandled to allow unrestricted access to a database [28]. Once gaining access, LulzSec could download, alter, and even corrupt the entire database system.

Using that single flaw in SQL, LulzSec uncovered one million passwords, 3.7 million "music coupon" codes, 21,000 email addresses, and 75,000 "music codes" on the database [34]. The most troubling aspect of the data uncovered was that the one million passwords were unencrypted - that is, the passwords were stored in their plain form rather than using an encryption algorithm to scramble the password. With this information, LulzSec could use the passwords alongside user profile information (usernames, locations, date of births, etc.) to social engineer their way into other popular services such as Google and Facebook that the user accounts may be using, due to the usage of a single password in multiple locations. This information was published on BitTorrent trackers such as The Pirate Bay, allowing any user with knowledge of the BitTorrent protocol to download, view, and use the database information gathered [22].

To recover from this giant breach of data and information, Sony enacted yet another two-pronged approach: fixing middle-man website forms, and encrypting data. The web forms, being the source of the intrusions due to their faulty initial design, simply needed better design to prevent large amounts of text from being entered. By doing this, hackers would no longer be able to include SQL commands and rogue code into the form through the form fields. In addition, stronger data encryption results in information taking longer to decode per entry or even impossible to decode, dependent on the encryption method.

7.DR - DATABASE DIVING

Months earlier in April, Anonymous engaged in pursuing a different aspect of Sony's business and accessed more data than just usernames and passwords. A rogue subsection of Anonymous members, branding themselves solely as the Anonymous group, was able to access the Sony Playstation Network customer information database over a four-hour period on April 21st [17]. As soon as Sony discovered the breach in its AT&T Sand Diego data center [36], the company disconnected the Playstation Network entirely, leaving over 75 million customers without access to their Playstation games and online multiplayer [41]. Without access to the Sony Playstation Network servers, users of the Playstation Portable and Playstation 3 were unable to log in to the portal network and engage in online multiplayer.

Sony took just under a week from closing the Playstation 3 network database to inform its customers that their personal and credit card information had been stolen. Customers were initially informed that "there was nothing to report, [and at the same time] thanking them for their patience" for the six day period [17]. Once Sony was able to confirm the depth of the hack, the company revealed that user names, addresses, countries of origin, email address, birth-dates, and Playstation Network login information had been acquired. In addition, Sony was unsure whether security information, billing addresses, credit card information, and purchase history had been stolen but were not able to rule out the possibility [18].

Alan Paller, a research director of the SANS Institute, suggested that Sony overlooked security when constructing the Playstation 3 Network by deploying buggy code in units that were shipped to customers [3]. An example of the buggy code was exposed in a February 2011 Anonymous chatroom conversation, where hackers revealed that credit card information was transmitted (not stored) from client to server in plaintext. In addition, these hackers revealed that all communication between the Sony server and the console was through non-secure web protocols and was unencrypted, even to access and download games [10].

However, the most glaring buggy code left by Sony was profiled by ExtremeTech's Sebastian Anthony, who revealed that the likely source of the access to data was through a custom Playstation 3 firmware called Rebug. Rebug, developed by the home-brew community, effectively transforms a Playstation 3 into a developer unit, which is what internal Sony employees use to beta-test the functionality of the console. A major oversight by Sony was that the developer units had trusted access to the internal Sony developer network, and by association, access to the customer detail database [2].

Twenty nine days later, on May 15th, Sony began to restore access to its Playstation Network through a phased roll-out that moved from Europe to the United States, and finally to Japan [21]. Sony lightly detailed their enhancements to data security once they reopened in a May 15 2011 press release, citing: "considerable enhancements to the data security by adding advanced technologies, increasing software monitoring, conducting vulnerability testing, increasing encryption, implementing additional firewalls, and the addition of an early-warning system for unusual patterns to help detect breaches earlier" [21].

Comparing to the SQL injection to Sony websites, this hack-job was a true disaster. With user access to customer data and internal network information available, alongside the ability to enter a Sony-trusted network, virtually none of Sony's consumer information was safely stored on their databases. The entire structure of both the 'Playstation-3-to-Playstation-Network' communications and Playstation Network database storage would have be reexamined and revamped.

Sony made one giant blunder in the response to the disaster, in that the company did not divulge to its users or the media that there had been a breach until six days after Sony's discovery. For users, this meant six days of their usernames, billing information, purchase history, and possibly their credit card information was freely available to anyone with the processing power to break any low-level encryption who could access these documents. With this information, any user could potentially wreak havoc with high levels of identity theft and unauthorized purchases.

In addition, Sony continued to operate their services with this loophole for another six days after the four-hour theft. Sony used this time to contact a independent security auditing firm to determine the inner details of the hack [21]. As Won Kim et.al. presented in their 2011 paper "The dark side of the Internet: Attacks, costs, and responses", online thefts result in the companies having to take an average of 330 hours to clean up the after-effects [42]. This corresponds to approximately eight weeks of full-time eight hour days, which was about half of the time that Sony eventually kept its services down.

If hackers could consume this much information in a four-hour sweep (especially compared to the SQL injection attack, which was able to obtain a small percentage of this data over a four day period), the possibilities for a six-day free-for-all is unimaginable. Although it is likely that the four-hour theft was halted by Sony discovering unusual data transfers from the databases, keeping the backdoor methods open for that amount of time is a poor decision and a big gamble by the company.

As a result of this, Sony lost big with its customer loyalty in regards to private secure information such as credit card information. The company, as stated above, went to great lengths to rebuild their network to appropriate levels of security. Software monitoring systems were increased across the board on their systems, encryption methods and security audits were conducted, firewall rules were updated or implemented to further separate an internal intranet from the outward-facing Internet, and an alert system was implemented to warn of unusual activity. In addition, the company also spent the twenty-nine day downtime to develop a patch for the Sony Playstation 3 firmware that revamped the security on the video game console, including adding more root keys and obfuscating additional keys and detection methods to avoid detection by hackers. As a confirmation of Sony's level of commitment to security, Sony relocated their data center from San Diego to a third-party location that offered more stringent security measures [21].

So while Sony's response was thorough in that it looked at both areas of concern ('Playstation-3-to-Playstation-Network' communications and Playstation Network database storage), the biggest mistake came with alerting their customers. And while it may have been beneficial of the company to devote its resources to pinpointing and examining the data leaks in detail, the effort of the company to suppress rumors of a hack for a week was unethical to those who trusted Sony with the company data.

8.BUSINESS CONTINUITY

In order to keep its service secure and its customers happy following the hacking incidents and disaster, Sony returned to Playstation Network, its portal to online gaming, to the masses. Sony expanded and rebuilt its gaming cloud to increase security and detect abnormal conditions, which came in handy when 93,000 account names were being brute-forced attacked in October 2011 in an attempt to gain access to the accounts [40]. Because of the security measures in place, Sony was able to detect the attack attempts early and disable the accounts before the hackers were able to correctly guess the passwords to a majority of the accounts.

Sony appointed a Chief Information Security Officer (CISO) in September 2011 to monitor and evaluate the security of Sony services and information [1], having heavy experience at Microsoft and the U.S. Department of Homeland Security in information security [4]. By doing so, Sony can continue to provide the continuity of its online services and better protect and safeguard its systems from attacks.

Although the company has not been forthcoming about internal policies enacted in the wake of the Sony Playstation 3 hacking disaster, it is important to note that many of the changes and adjustments to their security and hardware implementations were all taken to maximize the security and safety of company data from hacks. In addition, by restoring its services completely to allow players to again access the Playstation Network and play competitively online, the company has resumed normal services for its console and for its players, with all of the additional measures taking place in internal Sony practices or in Sony Playstation 3 firmware updates that are periodically released to fix security loopholes as they arise. The important thing to note in this regard is that from a customer looking inwards, the gaming experience and interaction with Sony's Playstation Network did not change. The brunt of the changes and expectations for work fell solely on the company's hands by the company itself, which is something to be commended.

9.CONCLUSIONS

While Sony may have been the recipient of what is reported to be the largest hacks in Internet history [19], it allowed both Sony and the corporate industry in general to understand the necessity of proper network security. As Glenn Peoples of Billboard stated, the companies have incentive to keep security updated and high level to avoid government intervention and lawsuits, and to keep from being blacklisted by credit card companies [29]. There is also a monetary aspect to consider, as Sony spent $171 million in the wake of the hacking disaster to provide identity theft protection, provide additional customer support, enhance network security, pay for legal and consulting costs, and to fund the 'Welcome Back' program that thanked customers for their patience [7].

Sony learned the price on digital properties both for the company and its customers, but the information learned from the attack can better protect companies across all markets and industries from suffering the same costs and consequences, as any company is susceptible to an attack like this as long as their servers provide information to customers.

The key areas of concern for companies then must be a three pronged approach:

Firstly, the company should ensure that its private and confidential data, such as credit card numbers and account passwords, are encrypted using high-level encryption schemes. With computing processing power growing exponentially, adopting high-level encryption allows for the encryption to better stand the test of time and discourages brute-force attacks. This, while not evident to the company, will instill confidence in the company from its customers in the event that the company data is ever compromised and stolen.

Second, the company should ensure that it has hired the appropriate security employees to handle the maintenance, design, and scalability of their security schemas. Sony provides an excellent case for this, where a lack of security expertise resulted in consulting a third-party firm to determine the extent of their attack. By having a security team in-place full-time at the company, these employees can constantly monitor security on all database-driven aspects of the company and perform necessary maintenance and updates to keep the company safe. In addition, if the company is the target of a hacking attempt, these internal employees can use the zero-day response time of the hack fixing a plug, rather than having to learn the intricacies of the network and protocol make-up.

Finally, the company should be truthful to its customers regarding any potential loss of consumer or private information. This provides a two-fold benefit in that it shows a responsibility of the company to its customers and it allows the company to focus solely on incident response or disaster recovery, instead of public relations framing.

The case of Sony versus Anonymous/LulzSec, in addition to providing evidence towards the power of a 'David versus Goliath' match-up, should provide a calling-card for any company that deals in computer networking and online data storage but yet does not invest in security. Due to Sony's missteps, the company lost a sizable portion of its yearly earnings to a response and lost much of its reputation on the action of a few hackers. To survive in an ever-evolving and ever-growing online environment, companies must realize that their data is their largest asset both to themselves and their customers. More importantly, the security and management of this priceless data should be paramount, due to the fact that this data cannot simply be bought - the company data is custom-tailored to the company itself due to its customers' unique actions. Hopefully, Sony's wake-up call should serve as an additional wake-up call to companies to ramp up security costs and implementations to save themselves the embarrassment, costs, and liabilities.

10.REFERENCES

[1] Adams, E. 2011. Sony appoints CISO in response to Playstation attacks.. but reports to the CIO?. SecurityInnovation. Retrieved October 21, 2011, from http://web.securityinnovation.com/blog/bid/70713/Sony-appoints-CISO-in-response-to-PlayStation-attacks-but-reports-to-the-CIO

[2] Anthony, S. 2011. How the Playstation Network was Hacked. ExtremeTech. Retrieved October 21, 2011, on http://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked

[3] Arthur, C. 2011. Playstation Network hack: why it took Sony seven days to tell the world. The Guardian. Retrieved October 21, 2011, from http://www.guardian.co.uk/technology/gamesblog/2011/apr/27/playstation-network-hack-sony

[4] Ashford, W. 2011. Sony appoints Philip Reitinger as CISO after data breach hits 100m customers. Computer Weekly. Retrieved October 21, 2011, from http://www.computerweekly.com/Articles/2011/09/06/247806/Sony-appoints-Philip-Reitinger-as-CISO-after-data-breach-hits-100m.htm

[5] Braiker, B. 2008. The Passion of 'Anonymous'. Newsweek. Retrieved October 21, 2011, from http://www.thedailybeast.com/newsweek/2008/02/07/the-passion-of-anonymous.html

[6] Colter, A. 2011. 'V for Vendetta' Inspires Anonymous, Creator David Lloyd Responds. Comics Alliance. Retrieved October 21, 2011, from http://www.comicsalliance.com/2011/08/04/v-for-vendetta-anonymous-david-lloyd/

[7] Dignan, L. 2011. Sony's data breach costs likely to scream higher. ZDnet. Retrieved October 21, 2011, from http://www.zdnet.com/blog/btl/sonys-data-breach-costs-likely-to-scream-higher/49161

[8] EFF. 2011. Digital Millenium Copyright Act. Electronic Frontier Foundation. Retrieved October 21, 2011, from https://www.eff.org/issues/dmca

[9] Fang-Yie, L., & I.-Long, L. 2010. A DoS/DDoS Attack Detection System Using Chi-Square Statistic Approach. Journal of Systemics, Cybernetics & Informatics, 8(2), 41-51. Retrieved October 21, 2011.

[10] Garratt, P. 2011. Supposed hacker chat-logs reveal PSN security lapses. VG24/7. Retrieved October 21, 2011, from http://www.vg247.com/2011/04/27/supposed-hacker-chat-logs-reveal-stunning-psn-security-lapses/

[11] Gaweda, S. 2011. PS3 Firmware 3.56 Brings Bans to 'Black Ops' Hackers. Game Rant. Retrieved October 21, 2011, from http://gamerant.com/ps3-firmware-356-bans-black-ops-hackers-seb-63719/

[12] Hachman, M. 2011. Playstation 3's Root Key Reportedly Found. PC Magazine. Retrieved October 21, 2011, from http://www.pcmag.com/article2/0,2817,2375056,00.asp#fbid=nb1w-AL5m8J

[13] Hachman, M. 2011. Sony sues PS3 hackers. PC Magazine. Retrieved October 21, 2011, from http://www.pcmag.com/article2/0,2817,2375660,00.asp#fbid=nb1w-AL5m8J

[14] Helgeson, M. 2011. The Saga of the Hacked PS3 Root Key Continues. GameInformer. Retrieved October 21, 2011, from http://www.gameinformer.com/b/news/archive/2011/01/27/the-saga-of-the-hacked-ps3-root-key-continues.aspx

[15] Hess, K. 2011. What is a hacker?. ZDnet. Retrieved October 21, 2011, from http://www.zdnet.com/blog/security/what-is-a-hacker/9468

[16] Higgins, K.J. 2011. Anonymous hacks security company, researcher. Dark Reading. Retrieved October 21, 2011, from http://www.darkreading.com/authentication/167901072/security/attacks-breaches/229202863/anonymous-hacks-security-company-researcher.html

[17] Kuchera, B. 2011. Playstation Network hacked, data stolen: how badly is Sony hurt?. Ars Technica. Retrieved October 21, 2011, from http://arstechnica.com/gaming/news/2011/04/sonys-black-eye-is-a-pr-problem-not-a-legal-one.ars

[18] Kuchera, B. 2011. Sony Admits utter PSN Failure: your personal data has been stolen. Ars Technica. Retrieved October 21, 2011, from http://arstechnica.com/gaming/news/2011/04/sony-admits-utter-psn-failure-your-personal-data-has-been-stolen.ars

[19] Kulicke, H. 2011. Hacked. Editor & Publisher, 144(10), 32-32-35. Retrieved October 21, 2011, from http://search.proquest.com/docview/898422997?accountid=11824

[20] Latif, L. 2011. Anonymous calls out Sony over its treatment of hacker geohot. The Inquirer. Retrieved October 21, 2011, from http://www.theinquirer.net/inquirer/news/2040139/anonymous-calls-sony-treatment-hacker-geohot

[21] Lee, A. 2011. Sony Playstation Network gets restored, but uncertainty lingers over the extent of the breach. Huffington Post. Retrieved October 21, 2011, from http://www.huffingtonpost.com/2011/05/15/sony-playstation-network_n_862121.html

[22] Martin, A. 2011. LulzSec's Sony Hack Really Was as Simple as it Claimed. The Atlantic. Retrieved October 21, 2011, from http://www.theatlanticwire.com/technology/2011/09/lulzsecs-sony-hack-really-was-simple-it-claimed/42851/

[23] Menn, J. 2011. They're watching, and they can bring you down. FinancialTimes. Retrieved October 21, 2011, from http://www.ft.com/intl/cms/s/2/3645ac3c-e32b-11e0-bb55-00144feabdc0.html#axzz1bBP0O8rH

[24] Mostyn, S. 2011. Sony enforcing lifetime PSN bans against Playstation 3 users. The Tech Herald. Retrieved October 21, 2011, from http://www.thetechherald.com/article.php/201107/6835/Sony-enforcing-lifetime-PSN-bans-against-PlayStation-3-users

[25] Murphy, S. 2011. Agents provocateurs. New Scientist, 46-49. Retrieved October 21, 2011.

[26] Newman, J. 2011. Sony and George Hotz Settle PS3 Hacking Lawsuit. Technologizer. Retrieved October 21, 2011, from http://technologizer.com/2011/04/11/sony-george-hotz-settle-ps3-hacking-lawsuit/

[27] Newman, J. 2011. Sony Issues Ultimatum to PS3 Hackers. Technologizer. Retrieved October 21, 2011, from http://technologizer.com/2011/02/16/sony-issues-ultimatum-to-ps3-hackers/

[28] Paul, I. 2011. LulzSec, Anonymous Hacks were Avoidable, Report Says. PCWorld Magazine. Retrieved October 21, 2011, from http://www.pcworld.com/article/231303/lulzsec_anonymous_hacks_were_avoidable_report_says.html

[29] Peoples, G. 2011. Attack Of The Hackers. Billboard, 123(21), 8. Retrieved October 21, 2011, from EBSCOhost.

[30] Pink, D.H. 2005. Why the world is flat. Wired. Retrieved October 21, 2011, from http://www.wired.com/wired/archive/13.05/friedman.html

[31] Philipp, J. 2011. A timeline of cyberattacks against Sony. TechZwn. Retrieved October 21, 2011, from http://techzwn.com/2011/06/a-timeline-of-cyberattacks-against-sony/

[32] Plunkett, L. 2011. Hacker Claims to have the PS3's Front Door Keys. Kotaku. Retrieved October 21, 2011, from http://kotaku.com/5723105/hacker-claims-to-have-the-ps3s-front-door-keys

[33] Rachwald, R. 2011. SQL Injection: by the numbers. Imperva. Retrieved October 21, 2011, from http://blog.imperva.com/2011/09/sql-injection-by-the-numbers.html

[34] Ragan, S. 2011. LulzSec: Sony was asking for it - millions of records compromised. The Tech Herald. Retrieved October 21, 2011, from http://www.thetechherald.com/article.php/201122/7230/LulzSec-Sony-was-asking-for-it-millions-of-records-compromised-Update-2

[35] Schwartz, M. 2008. The trolls among us. The New York Times. Retrieved October 21, 2011, from http://www.nytimes.com/2008/08/03/magazine/03trolls-t.html?_r=1

[36] Sony under attack. 2011. Computer Fraud & Security, 2011(5), 3. Retrieved October 21, 2011.

[37] Stone, M. 2011. Anonymous #OpSony: DDoS attacks against PlayStation succeed. Examiner. Retrieved October 21, 2011, from http://www.examiner.com/anonymous-in-national/anonymous-opsony-ddos-attacks-against-playstation-succeed

[38] Stuart, K. 2011. Playstation 3 jack - how it happened and what it means. The Guardian. Retrieved October 21, 2011, from http://www.guardian.co.uk/technology/gamesblog/2011/jan/07/playstation-3-hack-ps3

[39] Tiku, N. 2010. Who are those 'anonymous' wikileak hactivists? New York Magazine. Retrieved October 21, 2011, from http://nymag.com/daily/intel/2010/12/who_are_those_anonymous_wikile.html

[40] Weinberger, M. 2011. Sony Playstation Network Gaming Cloud Attacked Once Again. TalkinCloud. Retrieved October 21, 2011, from http://www.talkincloud.com/sony-playstation-network-gaming-cloud-attacked-once-again/

[41] Williams, M. 2011. Sony yet to determine scope of Playstation Network attack. PCWorld. Retrieved October 21, 2011, from http://www.pcworld.com/article/226162/sony_yet_to_determine_scope_of_playstation_network_attack.html#tk.rss_news

[42] Won Kim, Ok-Ran Jeong, Chulyun Kim, Jungmin So. The dark side of the Internet: Attacks, costs and responses. Information Systems, Volume 36, Issue 3, May 2011, Pages 675-705, ISSN 0306-4379, 10.1016/j.is.2010.11.003. Retrieved October 21, 2011.