

# SONY PLAYSTATION NETWORK ATTACK (2011)

Presented By

Kayleigh Buenaga

Michael Esparza

David Madsen

Thulasi Krishnan

Dan Scholnick

- ▶ Introduction
- ▶ About “Hacktivists” and “Attacks”
- ▶ The Hack - Part 1
- ▶ The Hack - Part 2
- ▶ The Aftermath
- ▶ Conclusion

# AGENDA

The Sony logo, consisting of the word 'SONY' in a bold, white, sans-serif font, centered within a black rectangular box.

**SONY**

Sony is a multinational conglomerate that was founded in 1946. Their headquarters are in, Tokyo, Japan and they currently employ 114,000 people globally. Sony has several aspects of their business: Sony Electronics, which provide audio and video electronics, as well as information technology products for both consumer and professional use.

The Sony logo, consisting of the word 'SONY' in a bold, white, sans-serif font, set against a black rectangular background.

Sony Interactive Entertainment is headquartered in San Mateo, CA and was founded in 1993, just prior to the launch of the first Playstation. There are currently four Playstations that have been created, the PS1-PS4. Sony Interactive Entertainment also develops games, and has subsidiary companies, like Naughty Dog, for example, that facilitate the creation of videogames. Sony Interactive Entertainment has also recently made a push into the mobile gaming world.

The Sony logo, consisting of the word 'SONY' in a bold, white, sans-serif font, set against a black rectangular background.

In the Sony Interactive Entertainment umbrella, there is a product called Playstation Network. Playstation Network was introduced in 2002 as a direct response to Microsoft's "Xbox Live" release. It was a lackluster release to say the least, and always lagged behind Xbox Live. The only competitive advantage that Playstation had was that it was free (at the time). It was a bare-minimum online gaming tool that allowed you to communicate in-game (at launch) and then across-game (years post launch). PSN has two different aspects: a store where you can purchase games and media content, and the online communication tool.

The Sony logo, consisting of the word 'SONY' in a bold, white, sans-serif font, set against a black rectangular background.

Playstation Network was continuously being improved... except for the security. On April 20<sup>th</sup>, 2011, a group of hackers brought down Playstation Network. They gained access to 77 million user's PII – including names, addresses, credit card numbers, birthdays, usernames, logins, and security questions, to name a few. Playstation Network is one of the largest holders of credit cards, just behind companies like Amazon, Apple, eBay, and PayPal, making this specific attack one of the largest ever into a repository of credit card information.

## How did the attack against PSN go down?

Between April 17 and 19, a so-far unnamed person illegally gained access to Sony's PSN servers in San Diego, Calif., by hacking into an application server behind a Web server and two firewalls. According to Sony Chief Information Officer Shinji Hajesima, the attack was disguised as a purchase, so it did not immediately raise any red flags. The vulnerability the attacker was able to exploit was known, according to Sony.

Sony flagged the attack on April 19 and on April 20 shut down PSN as well as Qriocity. The company hired security experts and contacted the FBI to investigate the exploit and find out what took place. Sony says it didn't actually learn for certain that personal information was exposed until April 25.

Sony described the attack as "very sophisticated" and still does not know the intruder's identity.



# Everything you ever wanted to know about the those hacktivists

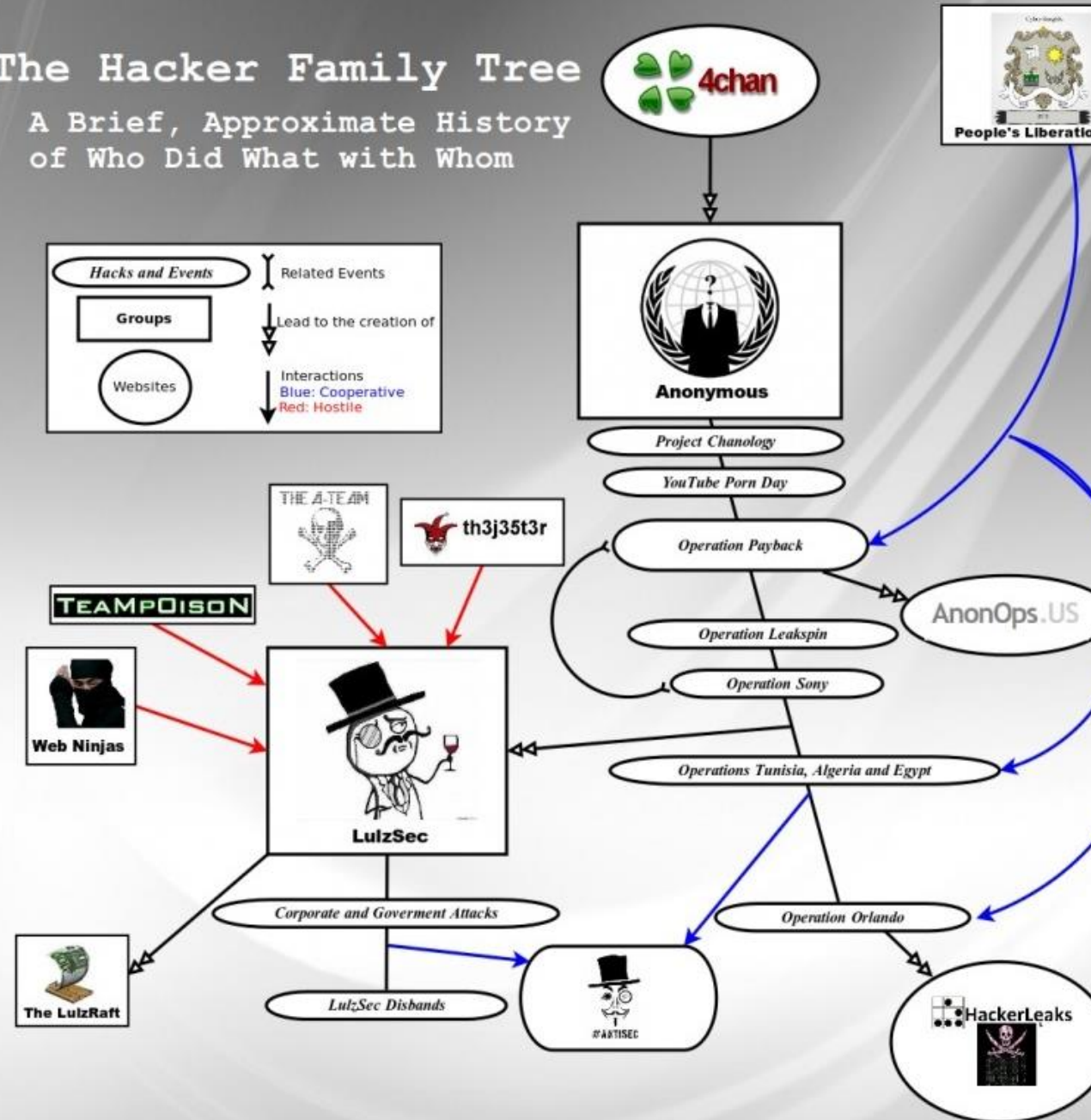
Have you been getting confused by all of the hacker groups and hacker group spinoff groups and side projects of hacker groups and their spinoffs? Are you a little tangled up in the web of connections between Anonymous, LulzSec, AntiSec and others? Don't feel bad. It's really confusing.

# HACKTIVISTS



## The Hacker Family Tree

A Brief, Approximate History of Who Did What with Whom





## TEAMPOISON

was a computer security research group consisting of 3 to 5 core members. The group gained notoriety in 2011/2012 for its blackhat hacking activities, which included attacks on the United Nations, NASA, NATO, Facebook, Minecraft Pocket Edition Forums, and several other large corporations and government entities.



The LuizRaft

is the name of a computer

hacker group or individual that gained international attention in 2011 due to a series of high-profile attacks on Canadian websites. Their targets have included the Conservative Party of Canada and Husky Energy

# ATTACKS

## Who's Who in the Hacking World



### LulzSec

- Broke into **PBS** website to post story that Tupac is still alive (5/11)
- Broke into private network of game developer **Bethesda Software** (6/11)
- Took down **CIA** website (6/11)
- Hacked **Sony Pictures Entertainment** (6/11)
- Claimed to have hacked **U.S Senate** (6/11) and **Nintendo** (6/11)



### Anonymous

- Group originated out of the infamous **4chan** message board
- Hacked **Sony's PlayStation Network** (4/11)
- Took credit for hacks against **PayPal** (12/10) and **Visa** (12/10) because they refused to transmit donations to **WikiLeaks**



#ANTISEC

**Operation Anti-Security**, also referred to as **Operation AntiSec** or **#AntiSec**, is a series of hacking attacks performed by members of the hacking group LulzSec and the group Anonymous

Sony Play Station Network Attack was motivated by anger about Sony's lawsuit against an American hacker who attempted to reverse-engineer the PlayStation 3 to allow users to play third-party games not authorized by Sony.

The hacking group Lizard Squad is claiming responsibility for an attack on Sony's PlayStation network, which caused connection issues for gamers over the weekend.

**MOTIVATION**

Visitors to the PlayStation Store were met with the message “Page not found! It’s not you. It’s the internet’s fault”. Sony said: “We are aware of the issues some users are experiencing, and are working to address them,” but did not elaborate the cause.

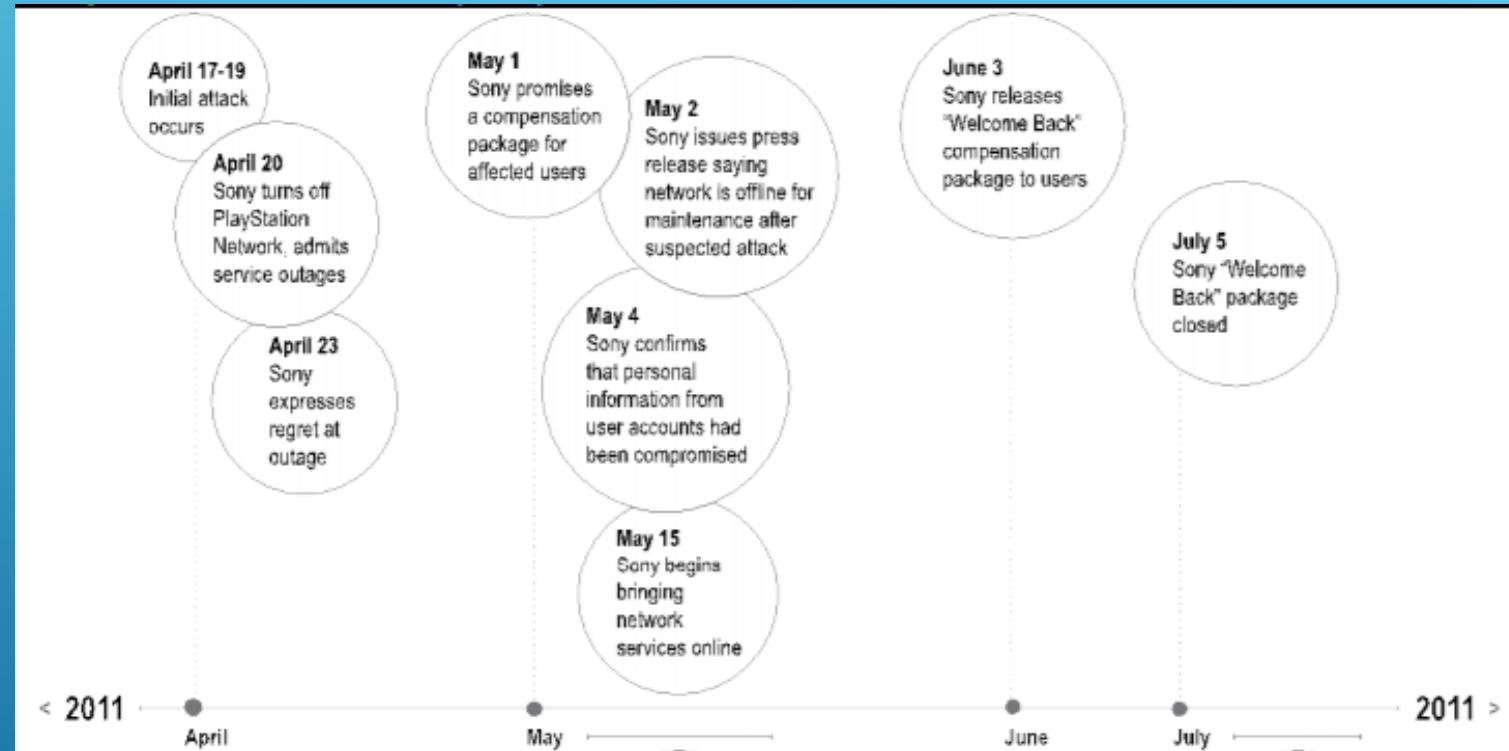
Lizard squad claimed credit for the outage via its Twitter account.

# COMMUNICATION





The 2011 PlayStation Network outage was the result of an "external intrusion" on Sony's PlayStation Network and Qriocity services, in which personal details from approximately 77 million accounts were compromised and prevented users of PlayStation 3 consoles from accessing the service. The attack occurred between April 17 and April 19, 2011, forcing Sony to turn off the PlayStation Network on April 20. On May 4 Sony confirmed that personally identifiable information from each of the 77 million accounts had been exposed.<sup>[5]</sup> The outage lasted 23 days. At the time of the outage, with a count of 77 million registered PlayStation Network accounts, it was one of the largest data security breaches in history.



# TIMELINE



- ▶ SQL Injection Attack – or breach point with the PS3 REBUG Firmware?
- ▶ Impacts of the PS3 REBUG Firmware prior to the hack
  - ▶ Transforms the PS3 Console into a Developer Unit
  - ▶ Activated a slew of developer features that regular consumers could not access
  - ▶ Most significantly: REBUG firmware gave console trusted access to Sony's internal developer network.
  - ▶ Once the internal developer network was breached, trusted access was wide open
    - ▶ Once in the internal trusted network, a whole range of new hacks became available, including the use of faked credit card details on the PlayStation Network.



HACK!



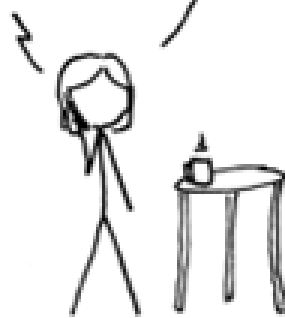
## PSN HACK – REBUG FIRMWARE

**With the REBUG custom firmware installed the customer details database — the one that was breached — became easily accessible. It's possible that Sony's security mechanisms simply didn't account for an internal attack from a trusted network !**

HI, THIS IS  
YOUR SON'S SCHOOL.  
WE'RE HAVING SOME  
COMPUTER TROUBLE.



OH, DEAR - DID HE  
BREAK SOMETHING?  
IN A WAY - )



DID YOU REALLY  
NAME YOUR SON  
Robert'); DROP  
TABLE Students;-- ?



OH. YES. LITTLE  
BOBBY TABLES,  
WE CALL HIM.

WELL, WE'VE LOST THIS  
YEAR'S STUDENT RECORDS.  
I HOPE YOU'RE HAPPY.



AND I HOPE  
YOU'VE LEARNED  
TO SANITIZE YOUR  
DATABASE INPUTS.

# SQL INJECTION

# SQL INJECTION

## The Expected Input

 http://mysite.net/MyRestApi/ValidateLogin?username=JohnDoe&password=12345

-- what the programmer expected SQL to run


```
SELECT userId
FROM users
WHERE username = 'JohnDoe' and password = N'12345';
```

```
public class MyRestApi
{
    // it starts out simple and innocent enough!
    string sqlString = "select userId FROM users where username = '[username]' and password = '[password]'";

    // then thing gets interesting
    // A public web API which takes two strings, username and password as parameters
    [HttpGet()]
    public int? ValidateLogin(
        string username,
        string password)
    {
        // unvalidated input is manipulated and inserted into the query string!
        var queryString = sqlString.Replace("[username]", username).Replace("[password]", password);

        // then a connection to a database is open and the SQL is executed
        using (var conn = new SqlConnection(Constants.ConnectionString))
        {
            SqlCommand command = new SqlCommand(conn, queryString);
            conn.Open();
            return (int?)command.ExecuteScalar();
        }
    }
}
```

## The Attacker's Input

 http://mysite.net/MyRestApi/ValidateLogin?username='';DROP TABLE users;--&password=It's been fun!'

-- what SQL actually executes

```
SELECT userId FROM users WHERE username = '';DROP TABLE users;--' and password = 'It's been fun!'
```

Unless saved by security or constraints, the users table is gone!

## Something a little more elaborate!

```
-- depending on the actual query, more may be possible,
-- consider "username=' or (1=1)---' and password=Thanks for that!" and a query that returns sensitive information!
-- the expectation is this will only return data on a valid username/password combination, but here all rows are returned!
SELECT username, address, city, state, ccnum, ccexpr FROM users WHERE username = '' or (1=1)---' and password = 'Thanks for that!'

-- one might EXECUTE a stored procedure
-- here is a popular one!
EXECUTE xp_cmdshell(/* my script here to run in the SQL Server user context */);

-- other popular commands
EXECUTE xp_availablemedia      -- display local drives
EXECUTE xp_loginconfig         -- display the server security mode
EXECUTE xp_ntsec_enumdomains   -- enumerate domains the system can access
EXECUTE xp_terminate_process   -- kill a process

-- attempt to escalate privilege!
-- this will attempt to access the database as the built in SQL
-- administrator account using the password test.
select * from OPENROWSET('SQLOLEDB', '', 'sa','test','select @@VERSION')
```





### **VALIDATE INPUT**

Do not allow special characters, single quotes, etc...

Use parameters instead of string replacement



### **Use Stored Procedures**

These are parameterized



### **Use Least Privilege on SQL Connection**

Don't let the web service have permissions to drop your users table!



### **Use Least Privilege on SQL Server**

Limit the SQL process' access to the OS



### **Harden against attack**

Where possible, lock down stored procedures such as xp\_cmdshell!

# DEFENSE AGAINST SQL INJECTION



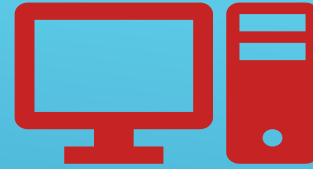
## Keys to the Kingdom

Knowledge of network topology and systems

Access to system account passwords

Knowledge of potential vulnerabilities

- Open firewall ports
- Unprotected systems



## Ability to manipulate the system

Install malicious software

Install backdoors

# INSIDER AND FORMER EMPLOYEE THREATS



## Comprehensive Monitoring

- Flag and remove unknown accounts
- Virus and malicious software scans
- Detection of anomalous activity
- Strong security policies



## Mitigations for Dismissed Employees

- Rotate Certificates
- Change service account and other non-user passwords

# DEFENSE IN THE INSIDER AND FORMER EMPLOYEE

Critics have argued that Sony has taken a lax approach to online security. They pointed out, for example, that the company **laid off two security workers** just weeks before the 2011 attacks.

And security expert Chester Wisniewski **told Gizmodo** that the hackers' efforts in 2011 were made easier by Sony's flat-footed response. They'd exploit a vulnerability in one Sony office, then use the same attack days later in another part of the world. "The crooks were able to attack the same thing because Sony Pictures wasn't going out and fixing it," Wisniewski said.

In Sony's case, that may have led to disaster. An experienced security analyst examining the PSN's logs on a regular basis should have been able to detect the earliest warning signs of the upcoming breach. We don't know exactly what measures Sony had in place before the breach, but it has clearly tried to bolster security measures since then. In September, Sony hired the former director of the National Cyber Security Center at the US Department of Homeland Security Philip Reitinger to be **its new chief information security officer (CISO)**.

"Organizational complexity and a lack of good security support at board level is probably the biggest mistake Sony made that led to the PSN hacks," says Stuart Thomas, a UK security expert who has worked as head of security at the London Stock Exchange and wrote the national cryptographic standards for the UK National Health Service.

Thomas has special insight into the matter: he built the original PlayStation 2 network for Sony back in 2001. "If you don't have a solid expert at board level championing good security management of people, technology and processes, everything else fails," says Thomas.

## Where the hack information came from:

- Government Investigations
- Lawsuits with supporting evidence from former and continuing employees provided insights into Sony practices with regards to security.

- ✓ Sony
- ✓ Profits
- ✓ Shareholders
- ✓ Executives

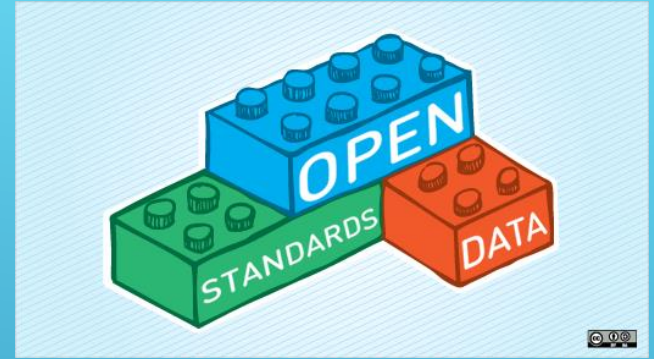
## Profits over Protection



- Customers
- Employees
- Partners
- Industry

# THE AFTERMATH

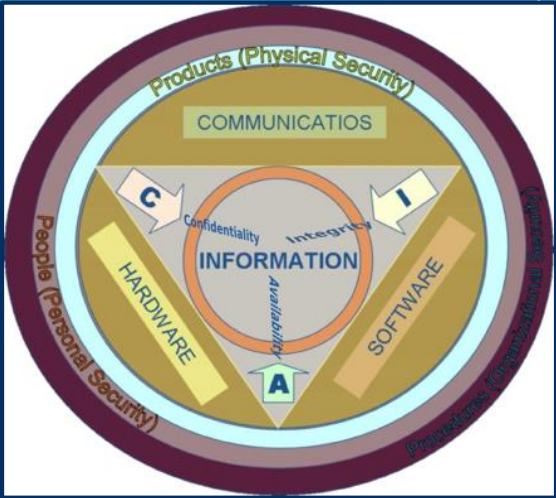
- General lack of use of industry accepted security standards.
- Need more security workers.
- The personal information was compromised during the attack.
- Either can spend on more security or more likely will have to spend considerably more to resolve damages after.
- Could have been much more expensive if hackers had wanted to use the client data they collected.
- Customer confidence needed to be rebuilt.
- Need to purchase separate cyber liability insurance.



## INSIGHTS/LESSONS LEARNED



## New security measures instituted by Sony



## SONY RESPONSE



- \$171 Million dollar loss (estimated)
- \$15M class action lawsuit
- Declining customer faith

*However...*

- Sony bounced back!



# THE IMPACT



The current trends as defined by a survey of 683 CIOs released in 2019:

- Increased spending on information security.
- In addition, 2/3 of these companies planned to have their security budgets grow in the near future.
- Security spending is being driven by compliance to regulations, response to incidents and general best practices.
- The end goal is to be at a point where the organizations can prove due diligence and regulations are reached.

## CURRENT TRENDS

# There Is No Other Way To Start Talking About Defense Strategies Than By Starting With Security Policies!

- ▶ The Comprehensive Need for MAC Policy
  - ▶ A strong MAC prevents an authenticated user or process at a specific classification or trust-level from accessing information, processes, or devices in a different level. This provides a containment mechanism of users and processes, both known and unknown (an unknown program (for example) might comprise an untrusted application where the system should monitor and/or control accesses to devices and files).
- ▶ Understand the Cybersecurity Kill Chain
- ▶ Fortifying Security Policy – emphasize Information Security as a foundational element of the IT Discipline!
  - ▶ Review Current Security Policy
  - ▶ Educate the End User on Security Policies in Place
  - ▶ Establish Social Media Guidelines to supplement Security Policy
  - ▶ Security Awareness Training
    - ▶ Real World Examples: This Case Study
    - ▶ Practice: Well Written text and Rich visual elements in training materials
  - ▶ Policy Enforcement
  - ▶ Continuous Monitoring for Information Security Compliance
  - ▶ Establish a Disaster Recovery Plan

## CONCLUSIONS

- <https://www.cnet.com/news/the-playstation-network-breach-faq/>
- <https://www.theatlantic.com/technology/archive/2011/07/hacker-family-tree-anonymous-lulzsec-history/352641/>
- <https://pdfs.semanticscholar.org/9065/23b48b3949cae921d912b2f8fc3ecb08725a.pdf>
- <https://www.theguardian.com/technology/2014/dec/08/hackers-claim-responsibility-sony-playstation-network-outage-lizard-squad>
- <https://www-sciencedirect-com.libezproxy2.syr.edu/science/article/pii/S1353485806703531?via%3Dihub>
- <https://www.vox.com/2014/12/14/7387945/sony-hack-explained>
- <https://venturebeat.com/2011/09/22/security-lessons-from-the-playstation-network-breach/>
- <https://www.csoonline.com/article/3432138/how-much-should-you-spend-on-security.html>
- [https://www.gamasutra.com/view/news/125594/Suit\\_Alleges\\_Sony\\_Laid\\_Off\\_Network\\_Security\\_Employees\\_Just\\_Before\\_PSN\\_Breach.php](https://www.gamasutra.com/view/news/125594/Suit_Alleges_Sony_Laid_Off_Network_Security_Employees_Just_Before_PSN_Breach.php)
- <https://www.forbes.com/sites/insertcoin/2011/05/23/sony-pegs-psn-attack-costs-at-170-million/#5651701d44ca>
- <https://www.eurogamer.net/articles/2011-05-01-psn-sony-outlines-welcome-back-gifts>

## REFERENCES

- <https://www.lexology.com/library/detail.aspx?g=0cd8a3d7-9dba-467c-9d66-b301d3a1c87a>
- <https://esmemes.com/t/lulzsec>
- <https://en.wikipedia.org/wiki/LulzSec>
- <https://en.wikipedia.org/wiki/TeaMp0isoN>
- [https://en.wikipedia.org/wiki/Operation\\_AntiSec](https://en.wikipedia.org/wiki/Operation_AntiSec)
- <https://www.bbc.com/news/world-us-canada-13952864>

Diogenes, Yuri and Ozkaya, Erdal. “Cybersecurity – Attack and Defense Strategies: Infrastructure Security with Red Team and Blue Team Tactics.” 2018, Packt Publishing, Ltd,

- <https://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked>
- [https://en.wikipedia.org/wiki/Mandatory\\_access\\_control](https://en.wikipedia.org/wiki/Mandatory_access_control)
- [https://www.sony.com/en\\_us/SCA/who-we-are/overview.html](https://www.sony.com/en_us/SCA/who-we-are/overview.html)
- <https://www.playstation.com/en-us/corporate/about/>
- <https://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today>
- <https://www.wired.com/2011/05/sony-psn-hack-losses/>
- <https://www.zdnet.com/article/sony-settles-psn-hack-lawsuit-for-15-million/>

## REFERENCES CONTD..

- <https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/what-s-new-for-managed-service-accounts>
- <http://web.a.ebscohost.com.libezproxy2.syr.edu/ehost/detail/detail?vid=0&sid=ded45250-0bb6-4e8b-9dfb-54f0c5bd145e%40sessionmgr4006&bdata=JnNpdGU9ZWwhvc3QtbGl2ZQ%3d%3d#AN=149588&db=e000xna>

## REFERENCES CONTD...