Functional Information Assurance Plan

Looking back on the Sony data breaches which occurred not once but two times over a less than 4-year period there are many questions which must be asked. How come Sony did not learn from the first hack which occurred in 2011 to be better prepared to protect themselves in 2014. Sony is one of the largest companies in the world, one which has its foot in multiple different industries from movies, games, hardware, and databases.

The goals that the organization should have as a priority is to protect its servers in any way possible. There should be strides made to constantly keep the security ahead of any potential hacks or breaches, through constant monitoring and the use of cryptographic algorithms. It is important to practice confidentiality, integrity, and an availability of information. Confidentiality is important for keeping any data, objects, or messages from unauthorized disclosure to parties. This is important because you can keep private information out of the wrong hands as well as protect trade secret. It is important to prepare your security to uphold integrity, which are different services used to counter any active treats taking place. There are many forms of integrity including the ability to detect unauthorized modification of data with the ability to effect retransmission of modified objects, without the ability to retransmit modified objects and more. It is important to not only be able to stop an attack on your systems or data but be able to first detect when you are being attacked. With integrity there should be data, and information integrity as well as separation of duty and well-formed transaction to protect from conspiring from inside to steal. Availability should be an important part of the information assurance plan because it is important that there is a continuity of the service and access if any outside threats try to take down the service or block access to the network in any way.

Based on the hacks that happened to Sony they were lacking in each of the categories. The company was not aware of the data that they had stored in many of the databases which were hacked so not only were they unsure of what could have been stolen it had taken them a while to stop the attack which is an indication of lack of Confidentiality and Integrity (Cyberscout, 2014). In the 2011 hack of the Sony PlayStation network, hackers were not only able to steal millions of user’s information and their own workers private HR information but knocked the service out for weeks on end before Sony was able to get the availability up again for paying users. Again in 2004 they were hacked using what is known as a Server Message Block (SMB) Worm tool, which used a brute force authentication method (Lennon, 2004).

Sony now uses a governed set of global policies and standards, based on internationally accepted best practices. They have a Chief Information Security Officer (CISO) which monitors the compliance of policies to protect from leakage, falsification, loss, destruction and many more security risks. They also state that they educate the workers on privacy and awareness in hopes to stop leaks through fraudulent emails. Another measure they are using is a 24-hour security operation center to detect and prevent any cyber security incidents before the ability to spread. (Sony, 2019)

The company now teaches staff members the importance of network security including identifying fraudulent emails and to spot attacks early through following procedures in place. There seems to be a lack of encryption methods to conceal data as a cypher from outside attacks based on what I see on their site. This could mean that if hackers are able to break into the system again then the data would still be up for grabs because there is no need to decode any information.

It is important for a company like Sony to gain as much profit as possible through multiple business avenues. E-Commerce has become a focus for many companies with Sony being no exception. There are many important leaders in a company as large as Sony Entertainment, which covers multiple types of business. The company has a chairman, Kazuo Hirai, who is mostly responsible for decisions about the direction the company should follow to find new ways to bring in money as well as be part of the board members. There are Chief Executive Officers (CEO) and Chief Information Security Officers (CISO) which have more influence over the every day security and business operations Sony will follow. The CEO should be responsible for setting goals and milestones for the company including holding other divisions accountable for doing their jobs. The CEO should be focused on making the company run as smoothly as possibly while also remaining profitable, which includes security of your clients and users. The CISO is responsible for overlooking and assigning security roles and tasks to security engineers to protect Sony from any data breaches and hackers looking to do the company or its users any harm.

In the recent hacks the company was hacked because they did not have proper training related to keeping the buildings secure and not allowing strangers into the location. This should be the responsible of all management in the company to ensure that everyone has training in security basics like phishing, password protection, and prevent access to unknown people.

It is important that a company follows ethical practices when securing their networks and its users’ information. Basing your Information Assurance on ethics is an important way to continue to hold the trust of your users and investors. It is important to know what is right and wrong to do when protecting data. This can include what information is stored and how it is stored or used, also who has access to that data. The ramifications for not following ethics when dealing with issues is that you not only lose the information during a hack, but you hurt your company’s name and trust as an organization.

Sony hid the fact that they had been hacked from their users until it was necessary to announce they had been hacked because they had their services disconnected and shut down by the hackers. Allowing customers to know what was going on would have potentially reduced anger related to the service outage. After the attack the company was in panic mode trying to gain information but were slow to fix any of the security holes, leading to an additional set of attacks over the next couple weeks.

The company says they are using policies which are compliant with law, including increased training to raise awareness of key security components of information security, which lead to the hack originally. The key components that should be important to key leaders is making sure that access is only granted to people who are meant to have it. They should make sure that everything they store or send is encrypted to make stealing it more complicated to nearly impossible. It is important that they do a better job of authorizing users, the original hack happened do to people allowing a stranger into the building, who later gained access to an IT professionals password which gave the hacker free reign over the databases. After the data was stolen the company failed to uphold its availability portion when the hacker shut down and blocked their service for weeks on end, making customers and workers unable to access any of the services. They appeared to have no strategies set up for disaster recovery in the event of a worst-case scenario such as the hack that happened. The new changes which have been made to the company should hopefully help with future hacks, and at the very least will set them up to stop the hack as soon as it happens instead of allowing it to continue for weeks.

Sony Operates in a wide range of environments offering services ranging from a movie studio, hardware development, game distribution, tv and game streaming and more. The fact that they cover so many different roles and environments in the business world there is a large amount of data being transferred and stored in the company. The company is most likely running a Wireless Environment possibly using a Wide Area Network (WAN) or Wireless Lan (LAN) ensuring that they are quickly able to access and store data in a shared database and server. The company currently maintains a robust Information Assurance and privacy program led by a Chief Information Security Officer (CISO) (Sony.net, 2018). Sony used security and privacy practices which follow global standards and are internationally accepted practices. The CISO monitors the global implementation of compliance with the policies they use while coordinating with a group of Information security Officers (ISO) and Privacy Officers (PO). Protocols and policies start with strong executive support, with the executives taking responsibility for employee awareness and setting policies. This included new policies put into place to enhance security of protection of personal data including 24/4 global security equipped with the equipment to monitor, analyze, and detect any unwanted activity while bolstering security. The company probably uses a guideline to prepare and plan for an attack similar to ISO 27002, which would give them standards to follow.

Sony is a major corporation which has information gathered from millions of people worldwide including its employees and users. In the new threat environment faced by the company shows that hackers are not just interested in the amount of money they can hack. During the attacks on Sony in the past hackers set out not to steal money but to instead humiliate them to ruin their reputation and for political reasons. (Roy, 2015). This threat environment shows that information other than just financial information is at risk to being stolen and used by unwanted users. To prepare for attacks in this nature a company must make strides to not only bolster their firewalls but also fix any vulnerabilities within their security. This includes the threat of data breaches from inside the company, either from weak passwords being stolen or employees not understanding their security roles and responsibilities.

Based on analysis of past attacks that occurred on Sony it is important that they work to understand their potential weaknesses in their overall security. The hack occurred due to a very weak password policy in place which saw Sony storing unencrypted passwords on their corporate network in a document labeled Passwords.doc. (Peden, 2014) The first improvement to their security would be to implement a strong password policy which requires different cases, numbers, symbols, and longer password lengths.

The company needs to identify all the data they are storing in their network and get rid of any information which may not be needed while classifying the other data and properly encrypting it into a safe storage space within the internal network and segregated and controlled by a firewall. Stored data should have an access log that tracks any attempts to access put into place. The next step is to train all employees of the responsibilities they must protect personal data and network security. Anyone given access to privileged information or storage should be trained properly as well as sign some form of a non-disclosure agreement.

There should be an outline which gives the security team procedures to follow to protect the organizations assets, determines if anything has been compromised, assigns roles and security to employees, and create procedures to follow in the instance of an attack. It is important to set your policies to be inline with practices that are considered globally accepted while keeping up with the found vulnerabilities to make hacking harder. This includes using something like the FISMA risk management framework or NIST checklist.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Low | Low To medium | Medium | Medium to High | High |  |
| Low | Username loss |  | Employees without security training |  |  |  |
| Low to Medium | User passwords |  |  |  |  |  |
| Medium |  |  | Storing data in network servers |  |  |  |
| Medium to High |  |  |  |  | Unclassified Stored information |  |
| High | Usernames and passwords stored together |  |  |  | Passwords unencrypted stored on word document |  |
|  |  |  |  |  |  |  |

Vulnerabilities that have been found is the stored passwords without encryption allowing any hacker to gain access to the file all the usernames and passwords of employees in the company. This could be solved by hashing and encrypting the passwords then storing them in a secure part of the network. Another threat is the attempts to gather employee information away to ransom the company for political and reputation gains. To avoid losing worker information only information that is vital should be stored and if it is stored it should be encrypted and tracked with a log.

Preparation for a data breach is as important as the security that you use to protect the network. There are many responsibilities a company has when dealing with security of their network which includes disclosing hacks to the public. The first step Sony should take in an incident response protocol is to identify all the data which the company is holding and collecting. They should identify the risk associate with each piece of data including the impact of that data being stolen. This will allow the company to better protect the data which is most important through separate storage and encryption. The incident response team should be given proper training, equipment, software, access, and more things to allow them to better prepare their network defenses and spot any intrusions. Because the hack is thought to have come from inside the company through an outsider gaining access into the company it is important to train all employees on basic security and password security. This training should include software training, permitted online use, and policies on security and data privacy.

The company was very slow to announce any information about the hack to the public and their employees after it occurred. They were also slow to stop the attack and recover the network to a working state. The company should form a plan which allows them to search for and identify abnormal activities using security monitoring and reviewing. This will allow them to identify and attempt to stop the hack before it has gotten to far along and before to much data has been stolen. Developing a communication plan is important as well which will allow Sony to know how to approach informing workers, customers, and partners of the hack including what Sony is doing to remedy the issue and protect the network in the future. It is important that the company constantly updates their network security and seeks out any vulnerabilities which may lead to a breach before the breach is able to happen.

Having a trained staff which has all the preparation and tools to spot and respond to an attack allows the Information assurance team to better protect the network. Being better prepared will ensure that the company can keep up to date with best practices that will help to not only protect their network but also the workers, customers, and partners. Having a tool which tracks network usage for abnormal use and vulnerabilities will help to prevent a hack due to being able to spot and stop a potential threat before ever giving it a chance to do real damage. The hack on Sony in 2014 was do to Malware which was inserted into the network which removed code and allowed the hackers to siphon and steal both user and worker information, and un-released movies. The Attack in 2011 caused the network to completely shut down, ending all availability to customers for weeks on end. Having a plan in place to restore the network and secure it will ensure that the network always remains available and secure for users, or at least as quick as possible in the event of a breach. Much of the issue with the hack was the lack of communication seen from Sony, letting the public know of the magnitude of their attack. Preparing a outline to follow for making the public aware, including what to say and include will make the process go more smoothly and effectively.

The first thing that should be included in a disaster response protocol is the priorities and recovery time objectives the company wishes to follow in case of a hack. This should target which data, services, and systems are most important, as well as which ones should be the priority to get back up quickest. This should include plans to restore hardware, applications, and any data in a timely manner. Priority should be set to getting business functions and security back to functioning properly and finding out the cause for the breach and what data was at risk.

The company should be prepared for outages to the network from disasters including weather, power outages or any other external force which may cause the network to go down. The company has many locations so there should be a secure transfer of data between them for backing up data in case of a outage at one of the facilities to be sure there is as little loss to the network availability as possible. All critical data should always be backed up in a secure and safe location to prepare for any potential threats which may cause lose of data or important network functions. It is also important that you have critical software and applications backed up.

Having a secured and updated backup of the network, all important data and applications will provide a quick way to restore your network in the event of an emergency. Having the data backed up or shared between multiple locations will provide a safety net in the event one or multiple locations is hit with a disaster which may cause the network to go down. Backing up data will protect the loss of important data and information which you would lose otherwise if you were unprepared. Working to get the network up and running as fast as possible will help to prevent monetary and network losses which may hurt both the pockets and reputation of the company.

The company should place access control tiers using role based Mandatory Access Control (MAC). This is important in business to protect data and software privileges for those which are meant to have them. New or untrained employees will be sure to only be given access to specific items required to perform their job role, with more access given to people based on their job title. This creates a layer of confidentiality by protecting sensitive data from access by anyone it is not meant for both in the workplace and out.

There are many cases when data is leaked from an internal source both purposefully or accidentally. By restricting access to functions and data on the network you can safeguard the sensitive material from any un-authorized users. It is important to not only restrict the access to material but also to log and track all access to the restricted information. This will give you a list of anyone who has accessed, read, or changed the data to protect it from unauthorized changes. This ensures both confidentiality and integrity of the network and data.

There should be proper training given to all employees in the company. This will prepare them for the responsibilities and tasks they will need to achieve to protect the network in the event of any breaches, as well as preparing for the breaches before they happen. There should be involvement from board members and management holding the team and security team accountable for their job and data security. Having a grasp on the importance of the data you are storing will better prepare you to know the risks associated with the data and potential threats to the data and your network. It is important to keep the policies updated and constantly training the employees of any changes which may have occurred in updates.

Doing these things will help to protect the network from accidental leaks from inside the company as well as keep the network security up to date. This will keep the network free of vulnerabilities which will make the data a lot harder to access. If all data is encrypted, securely stored, and given access to only those essential to the task you reduce the risk of losing confidentiality.

Bibliography

Kincaid, P. and Kincaid, P. (2018). *Building an incident response program: creating the framework - Malwarebytes Labs*. [online] Malwarebytes Labs. Available at: https://blog.malwarebytes.com/101/business/2018/03/building-an-incident-response-program-creating-the-framework/ [Accessed 16 Feb. 2019].

Winder, D. (n.d.). *Top incident response steps: Incident response team responsibilities*. [online] ComputerWeekly.com. Available at: https://www.computerweekly.com/tip/Top-incident-response-steps-Incident-response-team-responsibilities [Accessed 16 Feb. 2019].

SearchSecurity. (2011). *Incident response best practices after Sony breach*. [online] Available at: https://searchsecurity.techtarget.com/answer/Incident-response-best-practices-after-Sony-breach [Accessed 16 Feb. 2019].

Ready.gov. (n.d.). *IT Disaster Recovery Plan | Ready.gov*. [online] Available at: https://www.ready.gov/business/implementation/IT [Accessed 16 Feb. 2019].

Sony.net. (2018). *Sony Global - Information Security and Privacy*. [online] Available at: https://www.sony.net/SonyInfo/csr\_report/compliance/index6.html [Accessed 1 Feb. 2019].

Roy, R. (2015). *Why the Sony hack marks a new age of cybersecurity*. [online] Federal News Network. Available at: https://federalnewsnetwork.com/technology-main/2015/01/why-the-sony-hack-marks-a-new-age-of-cybersecurity/ [Accessed 1 Feb. 2019].

Peden, S. (2014). *The Sony Hack – Security Failures and Solutions*. [online] risk3sixty LLC. Available at: https://www.risk3sixty.com/2014/12/19/the-sony-hack-security-failures-and-solutions/ [Accessed 1 Feb. 2019].

Rouse, M. (2014). *What is confidentiality, integrity, and availability (CIA triad)? - Definition from WhatIs.com*. [online] WhatIs.com. Available at: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA [Accessed 25 Jan. 2019].

Sony.net. (2019). *Sony Global - Information Security and Privacy*. [online] Available at: https://www.sony.net/SonyInfo/csr\_report/compliance/index6.html [Accessed 25 Jan. 2019].

Riskbasedsecurity.com. (2014). *A Breakdown and Analysis of the December, 2014 Sony Hack*. [online] Available at: https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/ [Accessed 25 Jan. 2019].

Bort, J. (2014). *How The Hackers Broke Into Sony And Why It Could Happen To Any Company*. [online] Business Insider. Available at: https://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12 [Accessed 25 Jan. 2019].

Lennon, Mike. “Indicators of Compromise for Malware Used by Sony Hackers.” *Information Security News, IT Security News and Cybersecurity Insights:*

*SecurityWeek*, 2004 [www.securityweek.com/indicators-compromise-malware-used-sony-hackers](http://www.securityweek.com/indicators-compromise-malware-used-sony-hackers).

“Information Security and Privacy.” *Sony Global - Sony Global Headquarters*, 2019 [www.sony.net/SonyInfo/csr\_report/compliance/index6.html](http://www.sony.net/SonyInfo/csr_report/compliance/index6.html).

“3 Major Security Lessons from the Sony Pictures Data Breach.” *CyberScout*, cyberscout.com/education/blog/3-major-security-lessons-from-the-sony-pictures-data-breach.