**Cyber Security Mitigation Strategy Plan**

For Sony Pictures Entertainment, Inc.

**Team 4**

Ayda Onat Orallar (041065990)

Gizem Akgul (041077358)

Zehra Nur Atay (041075404)

Pragya M. Parmar (041058460)

Ukuobong Mbaba (041063429)

**Content**

**Cyber Security and Information Management**

1. **Cyber Risks and Threats**

In cybersecurity, cyber threats are different from cyber risk and vulnerability. Vulnerability is the weakness in your system. A threat takes advantage of a weakness of the system and can hurt or destroy an asset. The possibility of assets being lost, damaged, or destroyed is a risk (Glover, 2022).

First, the types of cyber threats should be known to protect an organization from cyber threats. There are mainly three categories of cyber threats:

* Unintentional threats: These are mainly primarily human errors. Some examples of unintentional threats are forgetting to update the firewall or anti-virus program or having access to sensitive data by a former employee (Glover, 2022).
* Natural threats: While natural disasters (floods, hurricanes, tornadoes, earthquakes, and so on) are not linked with cybersecurity, they are unexpected and can harm the asset of an organization (Glover, 2022).
* Intentional threats are attacks malicious actors use to breach a security or software system. Examples of intentional threats are malware, phishing, DDOS, espionage, viruses, critical infrastructure attacks, and social engineering (Glover, 2022).

Conducting a cyber risk checkup and developing a cyber risk management plan is necessary to minimize the risk against cyber threats.

In Sony Pictures Entertainment cyber-attack case, this hacker group accessed all areas of the studio networks by taking advantage of a vulnerability in Sony's systems. It is said that they took advantage of "Zero-Day" vulnerability to destroy the studio's network (Hesseldahl, 2015). A software vulnerability the vendor has not yet patched is a zero-day vulnerability. Since there is no fix for zero-day vulnerabilities due to the suppliers, attacks are more likely to succeed (Kaspersky, 2022). An important technical fact that explains how the hackers could enter Sony's network as early as September and fully exploit it without being discovered until late November is the existence of a Zero-Day vulnerability in the investigation (Hesseldahl, 2015).

It was understood that Sony had not taken even the most basic precautions to protect user data. For instance, according to the organization's retention policy, outdated, encrypted communications could remain on corporate servers for seven years. In addition to using email for day-to-day communication, Sony also utilized emails as a permanent archive for contracts or other business data for archival purposes. They also kept their private data, such as I.T. administrator login credentials, in word documents with titles like "Computer Passwords" (Li, 2018). These weaknesses in the systems created cyber risk for Sony.

1. **Identification**

The common intentional cyber threats can be listed as follows:

* Malware-based attacks (ransomware, virus, etc.)
* Ransomware attacks
* Distributed denial of service (DDoS) attacks
* Cyber espionage
* Social Engineering Attacks (Phishing, spear phishing, etc.)

Malware: Malware is software installed on a computer without the user's suspicion and designed to conduct harmful operations. Malware may be installed in several methods, including through email attachments, drive-by downloads, and malicious website connections. Video, images, and any program file are all potential hiding places for malicious malware. Malware may infect your computer if you open one of these files (McAfee, 2022).

A virus attack is a kind of malware attack. When a user opens an infected file or software (such as a document), the virus attaches itself and, once executed, may multiply and spread to other computers. You may, for instance, download a virus after receiving an email with a dangerous attachment, opening the file without realizing its danger. Viruses are harmful because they may wipe data, drain resources, and record user input (Malwarebytes, 2022).

Ransomware: Ransomware is malicious software that locks you out of your computer (or the stored data). The computer itself could lock up, or its information could be stolen, lost, or changed. Some ransomwares can be used to spread to other computers through the network.

To protect an organization from malware and ransomware.

* Keep software updated.
* Do not click on a link in a pop-up.
* Use a minimum number of apps on your computer and uninstall the apps that are not in use.
* Use a security program
* Don't leave your computer unlocked if you are not standing at the computer (McAfee, 2022).
* Make filtration to allow downloading of only the file types that you know
* Block websites that are known to be harmful
* Use mail filtering and spam filtering
* Remote desktop protocols if not needed (National Cyber Security Centre, 2022).

Distributed denial of service (DDoS):

This threat actor utilizes several workstations to attack one target. DDoS not only strengthens attacks but also makes it more difficult to find out the attack's origin. It targets devices and protocols that link the network to the internet. (DDoS) episodes focus on servers and websites by interfering with network functions. Consequently, service can be slowed down or stopped for a long time (Canadian Centre for Cyber Security, 2022).

To protect an organization from DDoS:

* Develop a DOS defense strategy
* Follow up on your network and systems frequently. Install a monitoring tool which alerts when there is massive traffic on the network.
* Install firewalls
* Install and keep updated the anti-virus and anti-malware programs
* Use a layered mechanism by applying multiple control ways (Canadian Centre for Cyber Security, 2022).

Cyber espionage: Advanced persistent threats (APT), social engineering, virus assaults, and spear phishing are common forms of cyber espionage. Cyber espionage is a cyberattack carried out by a threat actor (or cyber spy) that maliciously accesses, steals, or discloses secret information or intellectual property (I.P.) to gain an economic, political, or competitive advantage in a business or government environment. It may also ruin a person's or corporation's reputation.

To protect your I.P. from cyber espionage, the organization should update the software programs, use multifactor authentication, segment the networks, observe unusual suspicious conduct, use a proactive detection strategy, review the organization's policy and use the concept of least privilege to limit access to sensitive data (Malwarebytes, 2022; What is Cyber Espionage).

Social engineering refers to an attack that relies heavily on human interaction and typically entails convincing people to violate standard security procedures and best practices to gain unauthorized access to systems, networks, or physical locations or to make a financial gain. Because it is often simpler to exploit individuals than it is to uncover a network or software vulnerability, social engineering is a common strategy used by attackers. Hackers often use social engineering techniques as part of a bigger plan to steal information or spread malware across a system or network. Phishing and spear phishing are two common types of social engineering attacks (Rosencrance & Bacon, 2021).

Phishing: Attackers who engage in phishing use websites that appear legitimate to steal their victims' sensitive information (such as passwords, bank account details, or credit card numbers) (Microsoft, 2022). Storytelling is common tactic scammers use in email and SMS communications to get you to visit a malicious website or download malicious software. Emails and texts purporting to come from well-known institutions, such as banks, credit card companies, or energy providers, may catch people off guard (Federal Trade Commission Consumer Advice, 2022).

Spear phishing is a type in which particular people or businesses are targeted through spam emails. Spear phishing uses much more attention-grabbing messages rather than standard messages.

To protect an organization from phishing and spear phishing:

* Use updated security software programs
* Recognize phishing messages (be suspicious of messages or emails that ask for urgent actions, first-time senders, lousy grammar, generic greetings, mismatched email domains, and suspicious links)
* Protect your accounts by using multifactor authentication
* When you recognize a phishing email, report it and delete it (Federal Trade Commission Consumer Advice, 2022).

The cyber-attack that Sony Pictures Entertainment faced in late November of 2014 by a group called "the Guardians of Peace" was a "malware-based attack. Using a "Destover" malware system, "100 terabytes of data were stolen, including unreleased movies, information about executive salaries, emails from the company's employee workplace complaints, movie scripts, and even the phone numbers of Hollywood celebrities. (Security, P., 2015). Destover, the malware program used in the Sony Entertainment hack, can wipe disc drives and MBR. A machine infected with the Destover malware will have its data deleted, leaving it worthless (Paganini, 2015).

It's not disclosed which software was affected. According to a recent article in The New York Times, malicious code was put into email attachments as part of "spear "phishing" operations in September. Once the attackers got into Sony's network, they moved around in a way that was called "low and slow." It took several weeks for them to carefully make a detailed map of the Company networks and the information needed to get into each one (Hesseldahl, 2015).

1. **Understanding Role and Governance**

In the past, information security programs and policies were designed to protect the Confidentiality, Integrity, and Availability of data within the confinement of an organization. But this became insufficient. Therefore cybersecurity, the process of protecting information by preventing, detecting, and responding to attacks, was formed (Santos, 2019, p.4). Organizations started to use cybersecurity programs and policies to protect themselves. Santos (2019) explains cybersecurity policy as a "directive that defines how the organization is going to protect its information assets and information systems, ensure compliance with legal and regulatory requirements, and maintain an environment that supports the guiding principles". Well-considered governance is at the core of any successful cybersecurity program, and many vital aspects require consideration - policy, best practices, ethics, legality, personnel, technical, compliance, auditing, and awareness (Dhillon, 2016). However, in Sony Pictures Entertainment, the company shows weak governance to protect its data and here is some supporting evidence of this:

* The lack of basic security measures in the company's headquarters, such as leaving guests without an escort, leaving administrative computers unattended etc. (DeSot, 2015).
* Their network lacked some of the basic protections, such as two-factor authentication or encrypted data (DeSot, 2015). That protection could reduce the amount of data which had been stolen.
* There was either no vulnerability management solution, or it was not correctly done because when hackers breached the system, the file transfer did not alert (DeSot, 2015).
* Lack of proper early warning intrusion detection system (IDS). The hackers spent many months inside Sony and other networks, learning what servers to hit, which employee accounts to mimic, etc. However, if there were proper IDS, it could be prevented (Strom, 2018).
* Segmenting the network is essential; however, Sony's network was not partitioned, which made it easier for hackers to move laterally across it (Strom, 2018). Keeping appropriate data in the proper places will be safer.
* Misconfigured servers that allowed unauthorized access (Sjouwerman, n.d.).
* Software vulnerabilities, either known or unknown zero-days (Sjouwerman, n.d.).

1. **Leadership**

The leaders should be willing to demonstrate visible leadership and to encourage and educate others to create a culture of compliance, where participants recognize and understand the policies and look for ways to promote them (Santos, 2019, p.27). However, in Sony's case, the management team failed to take responsibility and a proactive approach to cybersecurity threats and risks. Sony released a statement that they had prompted the company to strengthen security across all its products before this attack. However, they could not prevent this (Li, 2018).

Also, before that hack, Sony's executive director of information security said, "I will not invest $10 million to avoid a possible $1 million loss." (DeSot, 2015). However, today where everyone is a cybersecurity target, the net gain should be the way of thinking, especially for the leaders.

In the case examples, we can observe that the company does not have a positive corporate culture that focuses on protecting internal and customer information, proactive leaders and policies to follow.

1. **Response and Disaster Management**

After the attack, everything was basically "off the grid." Sony had to return to old methods, such as fax machines, paper checks, posted messages, etc. The main thing that Law Enforcement did was ask for an investigation by the FBI. Sony decided to shut down their network completely. Additionally, they delayed the release of the film "The Interview" to December 17 (Li, 2018).

After the attack, Sony implemented a new information security strategy and I.T. solution to prevent such incidents in the future. The plan's first step would be to distribute the idea of having no trust in anyone. With this new strategy, they want to stop hackers from entering company networks. As a security strategy, internet access would be tightly restricted; Sony would only maintain the minimum amount of data on its online network, with the remainder stored in an offline, encrypted, secure environment. Additionally, system administrators could only access the data needed to do their jobs. After a few weeks, emails would be stored in an archive. Most importantly, only authorized apps would be available for employee usage, multifactor authentication would be required, and firewalls would be set (Li, 2018).

**Methods of Cyber Attacks**

Today's range of cyber security attacks is increasing and becoming even more advanced. This growth is synonymous with the rate at which technological advancements are being recorded in our highly global economy (Singh & Singh, 2019). The attack on Sony Pictures Entertainment Inc by Guardians of Peace (North Korea) in 2014 was a large-scale cyber-attack caused by a blend of sophisticated and well-coordinated attacks (Tsukayama, 2011).

Attack methods to gain access to Sony's network included spear phishing, malware, Remote Access Trojans (RATs), and password spraying.

Social engineering (spear phishing) was a crucial tactic in the attack (Sjouwerman, 2014). The attackers sent carefully crafted emails to Sony's employees that appeared legitimate and necessary for day-to-day operations (SecureOps, 2021). Examples included emails that looked like they came from within the company, like H.R. emailing employees to verify personal information to comply with new requirements (The Cybersecurity Man, 2018). Phishing was used in which emails containing links that led to websites that looked like Sony's legitimate sites were used to steal employee credentials.

Social media was used to gather information about employees (SecureOps, 2021), which made the emails convincing. Phone calls impersonating the company’s I.T. help desk was also used to trick employees into revealing login credentials.

A variety of malware was used. FBI investigation found that the hackers used spear-phishing emails and links to distribute the malware (SecureOps, 2021). Among them were a Server Message Block (SMB) worm tool, a listening implant, a lightweight backdoor, a proxy tool, a destructive hard drive tool, and a destructive target cleaning tool.

One malware used was a customized version of a data-wiping (Wipall) trojan called a Destover. It was recorded to have significant improvements from similar known trojan malware (Paganini, 2015). Malware typically targets many systems performing their attack simultaneously across multiple systems in a network (Wowrack, 2022). A destover attack can be delivered without interaction (ISBuzz, 2015) and is often used for significant, long-lasting attacks. Based on the nature of the attack, the attackers are usually very well organized, patient and determined.

Several Remote Access Trojans (RATs) – lightweight backdoors - were used to gain access to the network to steal information (SecureOps, 2021). Another malware used was Brambul, designed to spread quickly across networks and steal data (SecureOps, 2021). They also used password spraying to guess common and weak passwords for many user accounts. The access found was then used to move laterally through Sony's network and gain access to other systems

The severity and importance of protecting against cyber-attacks are higher because attackers remain under the radar for months or longer (ISBuzz, 2015). From investigation, the attackers had been in Sony Picture's network for weeks and stole 100 terabytes worth of valuable data before deleting them from the network (Stengel, 2019). More so, unpreparedness leaves a company helpless in an attack.

**Business Impact Analysis (BIA)**

The process of Business Impact Analysis (BIA) is an essential measure for effective cyber risk management. The BIA enables organizations to identify and prioritize the crucial networks, systems, and information that could be impacted by a cyber-attack (Weber, 2022). The BIA also assists in assessing the possible effects of such an attack. In the case of the Sony Entertainment cyber-attack, the BIA showed that it had significant repercussions, such as the loss of confidential information, harm to the company’s reputation, and financial losses.

1. **Identifying critical systems, networks and data (SND)**

The Sony Entertainment cyber-attack demonstrated the importance of identifying critical systems, networks, and data (SND). Organizations must understand SND's role in operations and prioritize these assets in their cyber security measures (Weber, 2022). In the case of Sony, the company's lack of attention to SND was a significant factor in the success of the attack by the North Korean attackers.

1. Description

It is essential for businesses to take measures to protect their critical systems and important data. Identifying SND is crucial in managing cyber risks because it allows organizations to prioritize their cyber security efforts and allocate resources appropriately.

The Sony Entertainment company system network comprised 1555 servers and 6797 personal computers (Stengel, 2019). The critical data includes confidential documents, unreleased movies, actors' personal information, employee information, formal and informal information exchange between employees, personal information of customers, detailed financial data, corporate and private bank account data, and crew and cast member passport copies (Sullivan, 2016).

1. Role it plays

Critical systems, networks, and data play a vital role in an organization's operations, and their loss or compromise can have severe consequences. The impact of a cyber-attack on these assets can include financial losses, legal liabilities, damage to the organization's reputation, and operational disruptions.

The fundamental attributes of information security are Confidentiality, Integrity and Availability (Santos, 2019). Together, this makes the CIA triad. Cyber-attacks can affect single or multiple aspects of the CIA triad, depending on a company’s mission, products and services, contracts and regulations governing its industry (Santos, 2019). A close look at Sony picture’s critical infrastructure emphasizes a high need for all three elements of the CIA triad.

*Table: Cyber Security Component Roles and Affected CIA Triads*

|  |  |  |
| --- | --- | --- |
| **Component** | **The Role It Plays** | **Affected CIA Triad** |
| Physical Security Procedures | Help protect critical systems and assets from physical threats such as theft or natural disasters. | Confidentiality  Availability |
| Roles and Access Methods | Access controls ensure the employee has access only to the data and systems they are assigned to. | Confidentiality  Integrity |
| Data Storage Devices | Stores data and is encrypted. | Confidentiality  Integrity  Availability |
| Network Security | Security of the network infrastructure, including firewalls and intrusion detection systems. | Confidentiality  Integrity  Availability |
| Backup and Recovery | Data can be restored in case of a cyber-attack or a system failure. | Integrity  Availability |
| Remote Access Procedures | Identifies and authorizes the use of virtual private networks (VPNs) and two-factor authentication. | Confidentiality  Integrity  Availability |
| Incident Response Plan | Mitigates the impact of a cyber-attack with critical planning and strategies to decrease the effects. | Integrity  Availability |
| Patch Management | Identifies software vulnerabilities and manages recovery. | Confidentiality  Integrity  Availability |
| Enterprise Resource Planning (ERP) Systems | Manages the business processes and data. | Confidentiality  Integrity  Availability |
| Data Classification | Classifies data based on sensitivity and criticality. | Confidentiality Integrity  Availability |

1. Impact

In the attack on Sony Entertainment, 3262 personal computers in the network system were shut down along with 837 servers, and the malware caused half of the digital to be shut down (Stengel, 2019). The hackers stole nearly 100 Terabytes of data from this attack and published in 8 sections, estimated to be 38 million files using file-sharing sites and e-mailing news publishers and journalists (Sullivan, 2016).

*Table: CIA Triad Impact of Hacking on Sony Pictures*

|  |  |
| --- | --- |
| **Aspect of CIA Triad** | **Impact on Sony Pictures** |
| Confidentiality | Stolen confidential data, leaked emails, sensitive organizations' essential unreleased movies, and employee data. |
| Integrity | Destruction and alteration of data, including wiping out hard drives and erasing entire networks. |
| Availability | Disruption of business operations, including shutting down networks, servers, and critical systems. |

Among other reasons, Sony works with high-profile clients whose security and rights to privacy are paramount and determinants of future working relationships. Not to mention the competitive advantage associated with keeping company data, such as new movie manuscripts, in-house until it has been produced and released; company data must also be readily available and accessible for smooth business operations (Santos, 2019). Through one attack, 100 terabytes of data were stolen and deleted from the company’s system (Panda Security, 2015). A couple more attacks may shake the company to its core. This increases the need for a major company like Sony Pictures to be well-prepared against the fast-growing trend of cyberterrorism. The resulting impact of losing availability, confidentiality and integrity would be reputational damage, the cost of responding to the breach, potential lost future revenue, and perhaps regulatory penalties (Santos 2019).

1. Importance and Vulnerabilities

Recognizing critical systems, networks, and data is vital to effective cyber risk management. It enables organizations to comprehend these resources' significance and attack susceptibility (Weber, 2022). Cybercriminals frequently target these critical assets, making it crucial for organizations to prioritize them in their cybersecurity measures.

Wiping out half of the network system caused Sony to shut down the virtual network completely and work manually for eight days to prevent further damage from the malware (Reuters, 2014). The data included massive personal information of employees, cast and crew members, along with detailed banking and finance data which was used to threaten the company to withdraw the release of the film the Interview (Li, 2018).

*Table: Risk Effect – Cause Result Relationship of the Hacking*

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Type** | **Affected Areas** | **Cause** | **Results** |
| Strategic Risk | Business decisions, competitiveness | Loss of sensitive data, such as unreleased films and employee information, compromised Sony's ability to make informed strategic decisions. | Hindered Sony's ability to compete in the market. |
| Financial Risk | Monetary loss | The attack resulted in substantial financial losses related to data recovery, legal fees, compensation to affected parties, and a decline in Sony's stock price. | Sony incurred significant financial losses. |
| Reputational Risk | Public opinion, trust | Attack severely damaged Sony's reputation by releasing confidential emails and other sensitive information, resulting in negative media coverage, public criticism, and a loss of trust among customers and partners. | Resulted in a decline in customer and partner trust in Sony. |
| Operational Risk | Processes, systems, productivity | The attack caused significant disruption to Sony's business operations, resulting in delays in film releases, the shutdown of some systems, and a loss of employee productivity. The incident also exposed weaknesses in the company's security systems and processes. | This disrupted Sony's business operations and exposed weaknesses in its security systems and processes. |
| Personnel Risk | Morale, productivity, retention | The attack compromised personal information, including Social Security numbers and medical records, decreasing employee morale and productivity. Some employees left the company due to concerns about their data security. | It resulted in decreased employee morale and productivity and loss of talent. |
| Regulatory/  Compliance Risk | Legal consequences, fines | The attack violated data privacy laws and regulations, potentially resulting in significant fines and legal consequences for Sony. | Sony faced potential fines and legal consequences for violating data privacy laws and regulations. |

*Note.* From Li, M. (2018, May 12). *The Sony Pictures Entertainment Hack Case Report - Muyuan Li*. Medium. Copyright 2018 by Medium.

1. Criticality

The hackers threatened the employees and their families via e-mails to push the employees to denounce Sony. They also threatened those that would go to the theatres to see the movie (Hess, 2015). The FBI got involved in the case after North Korea was named behind the attack, which resulted in the file being labelled as “one of the largest cyberattacks ever perpetrated in the U.S.” (Stengel, 2019).

**b)** **Cybersecurity technologies**

Half of Sony's global digital network was destroyed by malware before the entire system turned dark. It disposed of more than 3000 of the total 6,500+ personal computers of Sony and “837” of its “1,555” servers (Stengel, 2019). Almost immediately, the company was back in the 1980s, using fax machines, pens, and paper to communicate with no systems running. It was only possible to pay in cash at the studio shop (Stengel, 2019).

1. What Was Wrong with Sony?

Most breaches are caused by a breakdown in or lack of security controls in several areas. In the case of Sony, this is a crucial reason for their data loss and cyber theft. Due to inadequate malware defences, limited monitoring procedures and audit logs, insufficient encryption, and poor incident response, Sony experienced a massive breach (Sanchez, 2015). Aside from the theft of electronic data, the GOP group made a statement to Sony and the world by indicating that failing to safeguard an organization’s data could result in the same situation being experienced by Sony (Sanchez, 2015).

Sony could have mitigated or detected the breach sooner if some of the Critical Controls, including certain sub-controls, had been implemented. The tragic incident that unfolded due to Sony's missed opportunities resulted in leaking sensitive documents to a worldwide audience (Sanchez, 2015). Despite there is no single solution to the security problem, there are some fundamental concepts that every organization should employ. These concepts should help prevent cyber-attacks (Sanchez, 2015).

Furthermore, Sony was found to be using outdated web applications and did not use firewalls to protect its networks, making its websites an inviting target for cyber criminals (Sanchez, 2015). As a result of using weak passwords, Sony nearly failed a Sarbanes-Oxley (SOX) audit in 2005. However, they were granted an exemption to the rule because their "creative types" could not adhere to a strong password policy (SOX password compliance: Not taking it seriously can be costly, 2016).

There was an infamous reputation among the public for Sony Corp's lack of security. During a 2007 interview, its head of information security stated that he did not believe it was worth spending 10$ million on cyber-security to prevent a loss of $1 million. He publicly disputed the claims of an auditor who argued that employees used weak and obvious passwords, insinuating that there was no issue with this (SOX password compliance: Not taking it seriously can be costly, 2016).

Furthermore, Sony's security culture was unsatisfactory. As a result of the leak, a person's passwords for several expensive data services were made public. There were many passwords consisting of obvious nouns and numbers combined. Such a security infrastructure presents serious risks and embarrassment to Sony (Warzel & Zeitlin, 2014).

Changes Made After the Breach

Although Sony chose not to appear before the House Committee on Energy and Commerce's hearing on May 4, 2011, it sent a letter to the Subcommittee on Commerce, Manufacturing, and Trade describing what it was doing to take measures after the attack. In this detailed eight-page document, new tools are described to defend against future attacks and increase data security (Sanchez, 2015). Furthermore, internal detection mechanisms were implemented that alerted network administrators to abnormalities or unauthorized access. After the attacks, Mr Stinger, Chief Executive Officer of Sony, stated that the company had strengthened its security strategy across all its products in response to the attacks (Sanchez, 2015).

In response to this latest cyber-attack, Sony lost millions of dollars in cleanup efforts. Approximately 40% of large corporations now have plans in place to address aggressive cyber-attacks designed to disrupt their business.

1. What Else Should They Have Done?

Incorporating security controls without ensuring the organization has the right cybersecurity culture to adapt to the secure cyber system is like closing one's doors with a chain instead of a padlock. Possibly, this creates a false sense of security and increases the risk for an organization as incorrect assumptions are made (Sanchez, 2015).

Sony must implement a culture change and create employee awareness to use the internal control measures implemented. Employees must be trained and educated regarding the importance of security and adhering to all protocols and practices.

Additionally, to limit the spread of Zero-Day exploits, the organization must pay researchers and ethical hackers to report vulnerabilities in software to the companies that design it so that they can be fixed.

How To Avoid Such Attacks in Future?

There is no doubt that companies need to invest more in the security of their networks. A company such as Sony typically underinvests in the protection of its networks because it may seem to be an unnecessary expense until there is a catastrophe.

Several Critical Controls must be implemented in cyber security technologies to prevent such attacks from happening in future.

* Inventory record

Devices and software inventories must be kept by experts, who can monitor and utilize them if unauthorized access to the system is detected (Sanchez, 2015).

* Malware Defenses

Sony Pictures Entertainment's breach in 2014 was primarily the result of malware that was used to delete content from hundreds of computers. If malware defences and detections are implemented, wiper malware can likely be prevented from spreading (Sanchez, 2015).

* Data Recovery Capability

Backups should be restored as quickly as possible. One of the most critical components of restoring an organization's infrastructure is the ability to restore data (Sanchez, 2015). The backup data should be adequately protected via physical security or encryption when it is stored, as well as when it is transferred across the network. Among these services are remote backups and cloud services (Sanchez, 2015).

Likewise, in the case of Sony, the wiper malware deleted every file on the hard drive. Sony undoubtedly suffered financial losses and lost time as a result of each day that the system was down. Sony's systems could have been kept offline for a shorter period if they had been able to restore from malware-free backups quickly.

* Security Skills Assessment

It is imperative for organizations to conduct timely assessments of their employee’s security skills and to provide appropriate training to fill any gaps that may exist in the case of misinformation or ignorance of specific security procedures (Sanchez, 2015).

* Secure Configurations

Companies need to securely configure firewalls, routers and switches to have a better chance of preventing or at least minimizing the likelihood of cyber-attacks by hackers in the future (Sanchez, 2015).

* Controlled Use of Administrative Privileges

In most cases, attackers spread within a target organization through the misuse of administrative privileges. An attacker's compromise of even one account can lead to a breach that affects the entire organization. Hence, administrative privileges must be controlled and secured (Sanchez, 2015).

* Maintenance, Monitoring, and Analysis of Audit Logs

Inadequacies in security logging and analysis enable attackers to conceal their location, malicious software, and activities on the victim's computer system (Sanchez, 2015). System administrators and security personnel can develop profiles of everyday events utilizing a SIEM tool in such cases, enabling them to tailor detection to focus on unusual activity, thereby avoiding false positives, identifying anomalies more quickly, and preventing overloading analysts with unnecessary alerts (Sanchez, 2015).

* Controlled Access Based on the Need to Know

Various software or data must not be accessible to all employees; access should be restricted based on an individual's need to know that information. Security experts or top management should be the only ones with access to secure data (Sanchez, 2015).

* Data Protection

In the case of data exfiltration, it is preferable to detect it at the earliest possible stage of the attack; however, if the information is stolen, having it encrypted makes the attackers' task more difficult.

An automated tool can be deployed at network perimeters to detect unauthorized attempts to exfiltrate data across network boundaries. This tool monitors certain sensitive information, keywords, and other biometric information. In addition, information security personnel should be alerted of such transfers while blocking them (Sanchez, 2015).

With an alleged 100 terabytes of data stolen by the GOP, an enormous amount of traffic would have been generated. Only a fraction of that would have been required by Sony to detect an attack on their network (Sanchez, 2015).

* Secure Network Engineering

The network should be segmented to provide the necessary layers of protection for critical systems. To provide granular control over system access and to augment intranet boundary defences, segmenting the enterprise network into multiple, separate trust zones will help (Sanchez, 2015).

* Continuous Vulnerability Assessment and Penetration Tests

Organizations should be aware of the different attack vectors and the methods by which attackers can compromise their telecommunications systems. Identify vulnerabilities that can be exploited successfully by conducting regular external and internal penetration tests (Sanchez, 2015). Ethical hackers can be employed to identify such vulnerabilities.

To simulate both outsider and insider attacks, penetration testing should be conducted both from outside and within the network perimeter.

**c)** **Legal Implications and Regulations**

In terms of legal implications, the attack raised a few notable issues. Due to illegal access to Sony's computer system and the theft of confidential information, the attack constitutes **a violation of U.S. law**. Since the U.S. Department of Justice indicted several North Koreans for their involvement in the attack, they have not been extradited to the US for trial (Schmitt, 2014).

According to Article 51 of the UN Charter and customary international law, the United States would have been entitled to respond forcefully, whether by kinetic or cyber means, if the malicious cyber operation against Sony had met the criteria of an “armed attack” (Schmitt, 2014). Among the experts in the International Group of Experts (IGE), it was unanimously agreed that cyber operations alone might be sufficient for physical damage or injury to cross the threshold of armed attacks, emphasizing the severity of the attack's impact rather than its nature. The authors contend that an attack that is sufficiently severe and non-injurious, such as one that results in a state's economic collapse, can qualify as an armed attack. However, it did not qualify (Schmitt, 2014).

As per Federal Cybersecurity and Data Privacy Laws Directory, the attack raised concerns about **cyber-security and data protection laws**. Sony faced criticism for its allegedly weak cyber-security practices, which resulted in sensitive data being stolen. Several states have their own cyber-security and data breach notification laws.

Organizations are required to demonstrate their cyber-security credentials under **Sarbanes-Oxley (SOX)**. Only public companies are subject to SOX. Regulatory and legislative measures were put in place under this rule to ensure that public companies produce accurate financial statements (Federal Cybersecurity and Data Privacy Laws Directory, 2022). Additionally, **Section 5 of the FTC Act** is both a privacy law and a regulation relating to information security (requiring appropriate cyber-security measures). Besides banks and common carriers, almost every company in the United States is subject to the law (Federal Cybersecurity and Data Privacy Laws Directory, 2022).

It is intended to ensure the privacy and security of sensitive personal information under the proposed **Consumer Privacy Protection Act of 2017**. Providing notice of security breaches involving sensitive personal information is in the interest of preventing and mitigating identity theft (Federal Cybersecurity and Data Privacy Laws Directory, 2022). Several other objectives are also intended to enhance law enforcement assistance and protect personal information against security breaches, fraudulent access, and misuse. This law applies to organizations collecting, using, accessing, transferring, storing, or disposing of confidential personally identifiable information of 10,000 or more US citizens in any 12-month period (Federal Cybersecurity and Data Privacy Laws Directory, 2022).

In the wake of the breach, former employees filed a lawsuit claiming their personal information was stolen. The company settled this lawsuit for $8 million. Additionally, multiple **class-action lawsuits** have been filed against Sony due to the cyber-attack. Other than former employees, the plaintiffs included shareholders who alleged that the company failed to disclose the cyber-security risks it faced. The number of settlements Sony reached for several lawsuits was not disclosed (U.S. Department of Justice, 2018).

Art, music, and literature are all protected under **copyright law**. Confidential information used in business operations is protected under the **law of trade secrets**. As evidence of **intellectual property theft**, the attackers stole several unreleased films, scripts, and other materials. North Korea was subsequently identified as the perpetrator of the attack by the FBI. Subsequently, the US government-imposed sanctions on North Korea for stealing intellectual property and engaging in other cyber activities (U.S. Department of Justice, 2018).

A threat was made to expose sensitive information concerning SPE if the movie "The Interview" was released. This raised concerns regarding the **right to free speech and censorship**. In order to uphold free speech, some argue that SPE should have released the movie as planned, while others believe that the company should have taken the threats seriously to ensure the safety of its employees (American Library Association, 2008).

By virtue of the Fourteenth Amendment, the First Amendment's constitutional right to free speech and intellectual freedom also applies to state and local governments. Criticism of the government, political dissatisfaction, and advocacy of unpopular ideas that people may find distasteful or against public policy are nearly always protected by the First Amendment (American Library Association, 2008).

Considering this attack, a more robust set of international norms and regulations regarding cyber-attacks is required. The UN General Assembly has established an open-ended working group to study and develop guidelines for the responsible behaviour of states in cyberspace. Despite this, progress has been slow due to disagreements between states regarding acceptable cyber behaviour (Sony cyber-attack: North Korea faces new US sanctions, 2015).

However, the attack led to several regulatory changes that impacted the company and the broader industry through the implementation of the following:

· A new law passed by Congress, the Cyber-security Information Sharing Act (CISA), allows businesses to share cyber threat information securely with the government without fear of legal repercussions (Cyber Security and Infrastructure Security Agency, 2021).

· In order to strengthen Sony's data security policies, the Federal Trade Commission (FTC) initiated an investigation to analyze Sony's data security practices (FTC, 2022).

·To help businesses better protect customer payment card information, the PCI Data Security Standards Council (PCI DSS) released updated guidelines (PCI Security Standards Council, 2018).

· President Obama released executive order 13636, encouraging voluntary development of cyber-security frameworks for critical business infrastructure (Department of Homeland Security, 2016).

·The executive order prompted the National Institute of Standards and Technology (NIST) Cybersecurity Framework to develop guidelines for managing and reducing cybersecurity risks (Cybersecurity Framework).

**d)** **Incident Response Plan (IRP)**

An incidence response plan includes a roadmap of responding, reporting and recovery actions (Santos, 2019). An incident response plan ensures the company is well prepared and protected against cyber-attacks. Thus, systems are put in place to ensure no data is lost, attackers are stopped on time, and business goes on as usual. An incident response plan will include policies, strategies, plans, and procedures to prevent and/or reduce the impact of cyber-attacks (Santos, 2019).

In a nutshell, the incident response plan is a document that outlines the organization's incident response procedures, steps, and responsibilities in the event of an attack (CrowdStrike, 2021). The steps include Preparation, Detection and Reporting, Triage and Analysis, Containment and Neutralization, and Recovery/Post-incident analysis (Bandos, 2016; Cichonski et al., 2012).

In addition to the zero-day opportunity (Hesseldahl, 2015) and information gained from social media, a lack of preparedness enabled the successful attack in 2014. It is reported that Sony had inadequate malware defences, limited monitoring procedures and audit logs, insufficient encryption, poor incident response, outdated web applications and used no firewalls to protect its networks (Sanchez, 2015). And Sony failed to detect the breach beforehand (Li, 2018).

In a single attack, Sony Pictures was deprived of 100 terabytes of data, 3,262 out of 6,797 personal computers were hacked, 837 of 1,555 servers were tampered with, and thousands of confidential information were released to the public (Panda Security, 2015). A well-outlined and practical IRP stops this from happening again.

To ensure business continuity and minimal losses in an attack, an organization needs to be proactive, paranoid and critical in preparation against an attack (Sassi, 2023). The technological world is fast growing, and so is the rate of cyber-attack advancements (Singh & Singh, 2019). Equally increasing is the vulnerability of Sony Pictures without an adequately implemented cyber security program and incidence response plan.

Cyber incidents drain resources. They are usually expensive, financially and otherwise, diverting attention from profitable business operations. The Destover attackers were in Sony’s system for weeks. With an efficient incidence response plan, an attack like this could have been detected quickly and mitigated or prevented.

**Governance and training/Awareness**

1. **Leadership buy-in**

Leadership buy-in is essential for the success of any cybersecurity program, from policy-making to implantation (Santos, 2019). A company’s leadership must actively champion cybersecurity programs and encourage and educate employees in a cybersecurity compliance culture (Santos, 2019, p.27).

However, Sony's management team was laissez-faire in its cybersecurity management. They did not take a proactive approach to cybersecurity threats and risks and failed to take responsibility (Li, 2018). Desot (2015) reports that before that hack, Sony's executive director of information security had said he would not invest $10 million to avoid a possible $1 million loss.

Despite an impeding ton of ego associated with leadership (Pfeffer, 2014), organizational management needs to learn that privacy is a thing of the past and that cybersecurity is the responsibility of every in the organization, starting from the management team (Santos, 2019).

1. **Who Is in Charge**

The Board of Directors, the CEO and every member of management are responsible for instituting and ensuring cyber security management programs (Santos, 2019). The Chief Information Security Officer (CISO) is responsible for ensuring the right security and governance practices, including – oversight, communication and enforcement of cybersecurity policy and program (Raza, 2020). System administrators/Information custodians are responsible for implementing, maintaining, and monitoring safeguards and systems (Santos, 2019). A designated Information owner is responsible for ensuring the confidentiality, Integrity and Availability of company data (Santos, 2019).

Cybersecurity is a collaborative effort of individuals with critical and multifaceted roles, from the board of directors to the CEO, management, data/Information owner, Information Security officer, system administrators and employees (Santos, 2019). However, the CISO/ISO has the highest role and is therefore in charge of ensuring the cyber security program of an organization (Raza, 2020).

1. **Organizational Culture**

An organization’s culture plays a significant role in creating and implementing cybersecurity programs (Santos, 2019). Employees in the organization pose a cybersecurity threat based on ignorance and their organizational functions (Ogden, 2021). Because cybersecurity is everybody’s business, there is a need for efficient communication, education, collaboration, training, and feedback to ensure a successful cybersecurity program (Huang & Pearlson, 2019).

The magnitude of the cyber-attack attack Sony Pictures experienced was more than any company should handle (LIFARS, 2015). However, the company had a culture of lousy cybersecurity practices (Mitnick, 2014; Westby, 2014). Employees were unaware of basic cybersecurity responses (The Cybersecurity Man, 2018). Two, there was no functional channel for reporting cybersecurity suspicions based on the time it took for the hacker’s attempts at employees to be discovered (SecureOps, 2021).

1. **Policies and Procedures**

In addition to collaborating with employees, cybersecurity policies, protocols, and procedures must be continuously accounted for, reviewed, and updated (Santos, 2019). The cybersecurity policies and protocols were inadequate. As reported, the company used weak passwords and failed to change them regularly or to conduct frequent reviews of its security network (Sanchez, 2015). More so, evidence showed the hackers gained access to Sony’s private cryptographic keys and encrypted information for a long time (Page Society, 2014).

The CISO/ISO, in collaboration with the CIO, CEO and other management, is responsible for identifying the organization’s assets, assessing potential threats and vulnerabilities, and creating comprehensive cybersecurity strategies to protect against them (Santos, 2019). However, Sony’s CISO and executives erred in this duty in that, even when the CISO was informed about a possible threat, he was more concerned about a 10-million-dollar expense than the security of the organization’s assets (DeSot, 2015).

**E) Response Plan**

The CISO is responsible for a cybersecurity response plan and will be a standing member of the Incident Response Team and the Continuity of Operations Team (Santos, 2019). In smaller companies, this will be the ISO. The response plan is governed by the details of the incidence response policy agreed upon and signed off on by the board and senior management and the incidence response procedures.

The response plan is a significant aspect of a company’s cyber security response. Based on NIST Framework, a company’s cyber security response includes the response plan, communications, analysis, mitigation and improvements (Santos, 2019). The company’s CISO, in collaboration with management, plays a critical role in all aspects of cybersecurity response. Efficient and continuously upgraded levels of governance, the response plan and all other cybersecurity response elements are necessary to make the company’s cybersecurity program successful.

In addition to the CISO, the incident management personnel include Incident Response Coordinators (IRCs), Designated Incident Handlers (DIHs), and Incident Response Team (IRT) members (Santos, 2019).

Employees play a role in reporting suspicious incidents (Ogden, 2021). The incident is accessed and classified based on levels 1, 2, or 3 (Santos, 2019). Depending on the severity, the Incidence Response Coordinator (IRC) is informed and works closely with Designated Incidence Handlers (DIHs) and the Incident Response Team (IRT) to neutralize the situation. Overall, in accordance with the NIST framework, the response plan requires preparation, detection and analysis, containment, eradication and recovery, and post-incident activities and reporting (Santos, 2019).

It is also important to identify and review planning shortfalls after every incident response (Dhillon, 2016).

**Response Plan**

Sony's business units included electronics, music, pictures, and gaming, and the company had various subsidiaries worldwide (Sony Corporation). Among the organization's top leaders was CEO Kazuo Hirai. Michael Lynton, the CEO of Sony Pictures Entertainment, was below him, responsible for different business units. The studio's cyber-security policies and practices were ultimately under his management. His involvement in day-to-day cyber-security efforts is unclear, however (Nusca, 2017)

The actions of Sony's management team reveal such a lack of understanding of cyber incident response that they take the baton to the finish line ahead of others (Westby, 2014).

In addition to its global team, Sony's cyber-security operations are divided into regional and local teams, which are supervised by the company's Chief Information Security Officer (CISO) (Irwin, 2014). John Scimone was promoted to the position of CISO by Sony in September. Previously, he served as director of security engineering for the company. He was responsible for monitoring threats and vulnerabilities and responding to incidents (Keise, 2014).

An organized and sophisticated cyber-attack requires a coordinated response, and preventing and responding to such an attack falls to all employees. In this case, a critical error in the studio's cyber-security practices led to a significant breach of its network several months before it was discovered (Warzel, Zeitlin, 2014). The company eventually strengthened its security controls and incident response procedures in the wake of the incident.

A response plan for Sony to have in an incident of a cyber-security breach should contain the following components,

|  |
| --- |
| 1. Identify the breach’s scope and nature |
| 1. Containment of breach |
| 1. Notifying appropriate authorities, customers & stakeholders |
| 1. Investigation of breach |
| 1. Mitigation of Damages |
| 1. Communication & public relations management |
| 1. Improvement of cyber security posture & control |

*Note.* Adapted FromSantos, O. (2019). Developing Cybersecurity Programs and Policies, Copyright 2019 by Pearson Education, Inc., From Embroker Team. (2022, December 7). *How to Design a Cyber Incident Response Plan for Your Business*. Copyright 2022 by Embroker

**Cyber Security and the Law**

*Table: Cyber Security Legal Frameworks and Sony*

|  |  |  |
| --- | --- | --- |
| **Legal Framework** | **Description** | **Sony** |
| Data Protection Laws | Laws that mandate the protection of personal data, such as the GDPR and CCPA. | Sony was targeted for their intellectual property rather than personal data, but it still had a duty to protect the personal information that it held. The attack exposed the personal information of Sony employees, including social security numbers, medical records, and salaries, which triggered obligations under breach notification laws. |
| Cybersecurity Standards | Standards that provide guidelines on how to manage cybersecurity risks, such as the NIST Cybersecurity Framework and ISO 27001. | Sony was criticized for having inadequate cybersecurity practices, which contributed to the success of the attack. The attackers were able to exploit vulnerabilities in Sony's network and gain access to sensitive information. If Sony had followed established cybersecurity standards, they might have been able to prevent or mitigate the attack. |
| Breach Notification Laws | Laws that require organizations to notify affected individuals in the event of a data breach. | As mentioned above, the attack exposed the personal information of Sony employees, which triggered obligations under breach notification laws. Sony was required to notify affected individuals and provide them with identity theft protection services. Failure to comply with breach notification laws can result in significant fines and damage to the organization's reputation. |
| Liability and Negligence | Organizations can be held liable for damages resulting from a data breach if they were negligent in their cybersecurity practices. | Sony faced several lawsuits from employees and other individuals whose personal information was exposed in the attack. These lawsuits alleged that Sony was negligent in their cybersecurity practices and failed to take reasonable steps to protect personal information. |
| Industry-Specific Regulations | Certain industries have specific regulations that relate to cybersecurity. | Sony operates in the entertainment industry, which is not subject to any specific cybersecurity regulations. However, they may be subject to regulations related to intellectual property protection. |
| Specific to Sony's Case | US Computer Fraud and Abuse Act and the US Economic Espionage Act. | The US Department of Justice charged several individuals linked to the North Korean government under the Computer Fraud and Abuse Act and the Economic Espionage Act for their involvement in the Sony hack. These regulations were used to prosecute the attackers and hold them accountable for their actions. |

*Note.* From Federal Cybersecurity and Data Privacy Laws Directory. (2022). Copyright 2022 by FCDPLD.

**Cyber Security Risk Mitigation**

Risk management is the process of deciding what level of risk is acceptable (risk appetite and tolerance), assessing the present level of risk (risk assessment), accepting the amount of risk (risk acceptance), or making efforts to decrease risk to an acceptable level (risk mitigation).

Risk mitigation strategies include below actions:

Risk Reduction: Taking one or more "countermeasures" to lower the risk

Risk reduction is the priority of the company in risk mitigation. Risk can be reduced by offensive controls, such as security patches or training and defensive controls, such as alarms, alerts. Risk reduction should be assessed for efficacy, resource needs, complexity, productivity and performance impact, unexpected effects, and cost before adoption (Santos O., 2019).

Risk Sharing: Sharing the risk with someone else

Risk transfer is done when an organization wants to share liability and responsibility for a risk with another organization which has the resources to do so. Purchasing insurance is the best example of risk sharing as it helps reduce the security incident's financial impact on the organization (Santos O., 2019).

Risk Transfer: Shifting the risk to another person or organization who can handle it best

This method gives the risk to someone else, such as a third-party vendor or contractor. Risk transfer may happen via agreements in which a third party takes on the risk. In this way, the organization transfers the responsibility and liability to another organization with the know-how and experience to manage the related risk (Santos O., 2019).

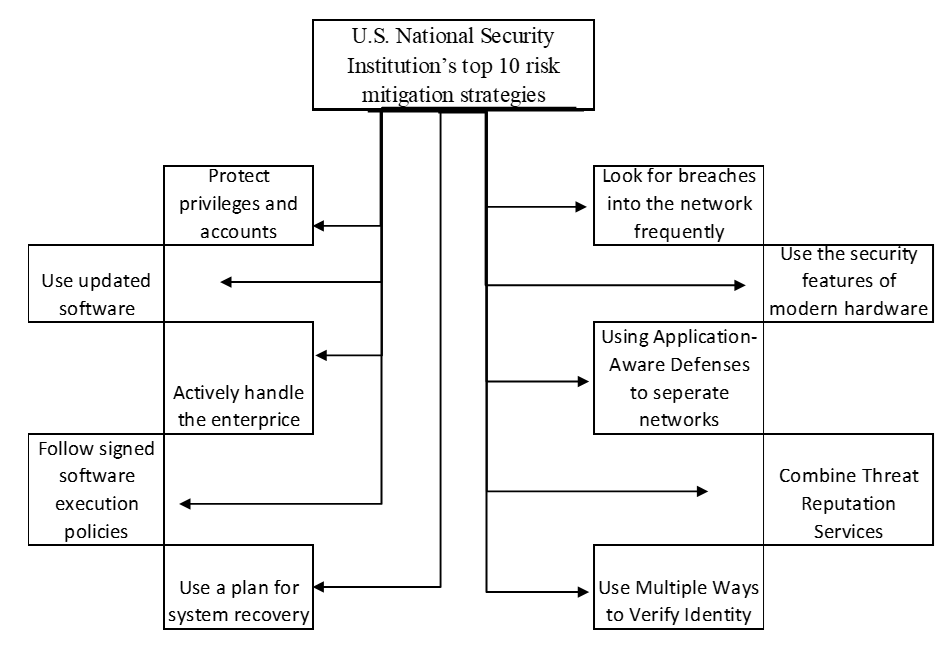
Risk Avoidance: Changing or stopping the activity that causes the danger, or a combination of the two

Risk avoidance may be acceptable when the assessed risk exceeds the organizational risk appetite and tolerance. Risk avoidance involves removing or drastically altering the risky process or activity. New processes, goods, services, activities, and partnerships may benefit from this approach. When assessing new procedures, goods, services, activities, and relationships, this method could be quite useful (Santos O., 2019).

The NIST Cybersecurity Framework (CSF) has a list of 108 suggested security activities for the five most important security functions: 1) identify, 2) protect, 3) detect, 4) respond, and 5) recover. It is made to help organizations better manage and decrease all kinds of cyber risks, such as malware, password theft, phishing attacks, DDoS, traffic interception, social engineering, and more (Knowles M., 2023).

In risk mitigation, identifying the potential risks on IT infrastructure such as hardware, software, and networks through risk assessment is the first step.

U.S. National Security Institution’s top 10 risk mitigation strategies:



*Flowchart: U.S. National Security Institution’s top 10 risk mitigation strategies*

* 1. **Use updated software**

Organizations should apply all software updates, automate the process, and use a vendor-provided update service. Threat actors may bypass defenders' patch cycles if patches aren't applied quickly (U.S. National Security Agency, 2018).

* 1. **Protect privileges and accounts**

Using a Privileged Access Management (PAM) system will enable to automatically manage the passwords and make arrangements on how to safely reset passwords are necessary to control privileged accounts as threat actors first look for privileged accounts to get high-value assets and move laterally around the network (U.S. National Security Agency, 2018).

* 1. **Signed Software Execution Policies must be followed**

Organizations should use a system that only lets the company run software that has been signed. By catching the injection of prohibited software, threat actors won't be able to use implanted malicious code to get a foothold and stay there (U.S. National Security Agency, 2018).

* 1. **Use a plan for system recovery**

Restoring lost data is quite important, so a security plan has to be implemented in the organization to mitigate the risk of data loss. Additionally, backups should be encrypted and kept offsite and offline. This is necessary if the organization is exposed to malware or ransomware (U.S. National Security Agency, 2018).

* 1. **Actively handle the enterprise**

Based on the inventory list of the organization, the unneeded hardware and software should be removed from the network system. This enables systems to detect threat environments while streamlining management operations (U.S. National Security Agency, 2018).

* 1. **Look for breaches in the network frequently**

It is suggested that malware can be detected earlier if companies authorize a dedicated team to search the system for any possible suspicious malware frequently. In this way, malware can be found, stopped and removed earlier than a worse consequence (U.S. National Security Agency, 2018).

* 1. **Use the security features of modern hardware**

Modern hardware security technologies have capabilities that improve the integrity of the boot process, verify the system, and help confine high-risk applications (U.S. National Security Agency, 2018).

* 1. **Using Application-Aware Defenses to separate networks**

Keeping important networks and services separate is necessary. Threat actors mask their bad acts and delete data by using common protocols. So, a sophisticated application software network defences to prevent traffic that is not properly structured (U.S. National Security Agency, 2018).

* 1. **Combining Threat Reputation Services**

The company should use services that provide information about potential threats to their systems, such as malicious files, websites, and email addresses. These services can help to quickly detect and prevent attacks and provide access to a more extensive network of threat analysis resources (U.S. National Security Agency, 2018).

* 1. **Use Multiple Ways to Verify Identity**

The company should use multiple ways to confirm a user's identity when accessing important systems or data. This might include using physical tokens in addition to passwords or PINs. This helps to protect against hackers who might guess or steal passwords (U.S. National Security Agency, 2018).

**Risk Mitigation Plan for Sony Pictures Entertainment Inc.**

The most important lesson learned from the attack is that the company should invest more in network security and ensure they're well-prepared to respond to attacks and mitigate the risks. Implementing the measurements below could have significantly assisted Sony with mitigating or at least detecting the breach sooner.

*Table: Risk Mitigation Suggestions with Description and Application to Sony Case*

|  |  |  |
| --- | --- | --- |
| **Suggestion** | **Description** | **Application to Case** |
| Secure Configurations for Hardware and Software on all devices | Execute an assessment of data to identify sensitive information that requires the application of encryption and integrity controls. | Identifying sensitive data, such as Social Security numbers, passwords, and emails, provides an additional layer of protection in the case of a breach. The difficulty of uploading these sensitive documents in clear text to the Internet grows with the use of secure setups on this material. |
| Implement Malware Defenses | In order to identify illegal efforts to exfiltrate data over network boundaries and stop such transfers while alerting information security employees, deploy an automated tool on network perimeters to monitor for certain sensitive information and other document characteristics. | Sony needed to detect a fraction of that in order to be tipped off that their network was under attack. Automating a tool to chase for unauthorized sensitive information leaving the network could have helped the company and could diminish the amount of stolen data. |
| Application Software Security | Perform routine server scans with automated tools to check for the presence of sensitive data in clear text. These instruments can be used to determine whether a business or technical process is falling behind or otherwise leaking sensitive data. | If Sony had proactively encrypted sensitive information instead of storing it in clear text, it could have significantly impeded attackers' ability to access and read the data, although no organization wishes their data would be stolen. |
| Controlled Use of Administrative Privileges | Monitor all traffic leaving the organization and detect any unauthorized use of encryption. It is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system because attackers often use an encrypted channel to bypass network security devices. | Sony could have established controlled use to further investigate large amounts of data leaving their network. If Sony was able to differentiate between legitimate encryption channels vs an unauthorized, covert communication channel that allows an attacker to transfer sensitive data, it would have alerted Sony in advance that they were being attacked. |
| Applying malware defences and detection | To improve security, it is recommended to restrict the use of external devices to only those that are necessary for business purposes and keep track of any attempted use or usage of such devices. | These defences would have alerted Sony's security team if any abnormal activities happened through external devices. By utilizing this defence, Sony could have potentially stopped the spread of the wiper malware. |
| Implement advanced backup procedures | To minimize data loss and facilitate fast system restoration in case of a malware attack, it's recommended to have an automatic backup schedule of at least once a week for all systems, with more frequent backups for those storing sensitive information. It's also crucial to ensure that the backup procedure includes the operating system, application software, and data on each machine, even if they are backed up separately or using different software. Multiple backups should be kept over time, allowing for the restoration of a version that predates the malware infection. It's also essential to ensure that backup policies comply with regulatory or official requirements to avoid legal or compliance issues. | The longer Sony Pictures Entertainment's systems were offline, the more time and money they would have lost. Still, if they could quickly recover malware-free backups for critical systems, they could have shortened their system downtime. |
| Proper backups protection | Protecting backups against theft or unauthorized access is crucial by implementing physical security measures or encryption during storage and transfer, whether using remote backups or cloud services. | Protected backups could have helped Sony minimize the impact of the breach caused by the GOP attack. |
| Implementation of Multi-Factor Authentication | The use of multi-factor authentications such as smart cards with certificates, One-Time Password (OTP) tokens, and biometrics for all administrative access is recommended. | The hackers used legitimate usernames and passwords in their malware to spread it more effectively. If Sony had implemented additional security measures for administrative accounts, the hackers might not have been able to access sensitive information. |
| Deploy a SIEM (Security Incident and Event Management) or log analytic tools | System administrators and security personnel should use a tool called SIEM to create profiles of normal events, so they can set the tool to detect only unusual activity. This will prevent false alarms, quickly spot any unusual activity, and avoid overwhelming analysts with unnecessary alerts. | Having a clear understanding of their infrastructure's usual activities would have allowed Sony to identify any unusual or malicious activity by comparing it to their baseline, which could have helped detect the breach sooner. |
| Establish network segmentation for a secure network | To improve control over system access and provide more intranet boundary defences, the enterprise network should be divided into multiple separate trust zones. | Sony could have potentially reduced the impact of a breach or become aware of it sooner if they had implemented this measure. |
| Penetration Tests and Red Team Exercises | Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (e.g., the Internet or wireless frequencies around an organization) as well as from within its boundaries (e.g., on the internal network) to simulate both outsider and insider attacks. | Having penetration tests on one’s infrastructure can point out many ways attackers can breach an organization. More importantly, had Sony established action items to mitigate the highest risks, they could have potentially prevented the attack vector utilized by the GOP group |
| Deploy an Incident Response and Management | Conduct periodic incident scenario sessions to provide an understanding of current threats and risks and remind the team of its responsibilities in supporting the incident handling team. | It could have aided Sony’s technicians and experts with being able to recover and bring the organization online quicker |
| Set the right security culture for the company | Simply implementing security measures without a strong security culture can create a deceptive sense of safety and potentially increase an organization's risk by making inaccurate assumptions. | Sony presented a security document to the Subcommittee on Commerce in 2011, suggesting encryption and anomaly detection mechanisms, but the improvements were not implemented. To establish a proper security culture, upper management must lead the way and work with knowledgeable personnel while also educating employees on the importance of the shift. |

*Note.* From Sanchez, G. (2015). Case Study: Critical Controls that Sony Should Have Implemented. *Global Information Assurance Certification Paper. SANS Institute*. Copyright 2015 by SANS Institute.

**Incident Response Plan**

An incident response plan is central to an organization's cyber risk mitigation strategy (Santos, 2019). It includes instruction, procedures and guidance to ensure the efficient execution of the following ten steps to handle cyber security incidents timely, effectively and efficiently. After carefully considering Sony Picture’s size, business objectives, assets, and critical infrastructure, this is the recommended IRP for the company going forward. This IRP is adapted based on NIST SP 800-61.

|  |  |
| --- | --- |
| **Incident Response Plan** | |
| **Prevention** | **Incident** – an incident refers to any adverse event that threatens Sony Picture’s business security and/or disrupts business operations (Santos, 2019). An example of this is the cyber-attack on Sony Pictures that was discovered on November 24, 2014 (Colatin, 2021). Incident severity levels could range from levels 1 to 3. Where level 1 refers to incidents that can course significant damage to the business, its customers, and the public or are in violation of corporate laws, regulations or contractual obligations (Santos, 2019). Level 2 constitutes “compromises or unauthorized access to noncritical systems or information; detection of a precursor to a focused attack; a believed threat of an imminent attack; or any act that is a potential violation of law, regulation, or contractual obligation” (Santos, 2019). Finally, level 3 includes “situations that can be contained and resolved by the information system custodian, data/process owner, or HR personnel, where there is no evidence or suspicion of harm to customer or proprietary information, processes, or services” (Santos, 2019).  **Need** – The security of Sony Picture’s information management system is vital to its mission, operations and business continuity (StateRAMP, 2021). To prevent cyber-attacks, protect information confidentiality, integrity and availability and address cybersecurity threats timely and effectively, it is much safer to be proactive and resilient.  **Purpose** – The document describes Sony Picture’s overall plan for preparing and responding to cybersecurity incidents.  **Scope** - This plan provides instructions, policies, procedures and guidelines for the effective and timely handling of cyber security incidents. It provides information on the actions that will be taken once the Incident Response Team (IRT) is notified of a cyber security incident, such as unauthorized access, malicious software, a compromise, DoS attacks, or inappropriate usage (Santos, 2019). It defines the roles, responsibilities and interactions of the parties involved and reporting requirements (Criminal Justice Information Centre, n.d.). |
| **Planning** | **Team** – Based on Sony’s Picture’s Incident Response Policy, this Incident response plan will be overseen by the Chief Information Security Officer (CISO) in collaboration with the Computer Security Incident Response Team (CSIRT), the Chief Information Officer (CIO), system and network administrators, security staff, technical support staff, computer security program managers, and any other personnel who are responsible for preparing for or responding to, security incidents (Cichonski et al., 2012).  **Approval** – The incident response plan (IRP) and any updates must be signed off on and fully supported by Senior Management (Santos, 2019). More so, it must be annually authorized by the Board of Directors.  **Team Structure** – Because Sony Pictures Entertainment is a large organization with multiple divisions, we recommend a Distributed Incident Response Team model, where different IRTs are responsible for each division. However, each divisional IRT will form the company’s single coordinated incident response entity to share information, and Sony Picture’s incident response process is well coordinated and consistent across the organization (Cichonski et al., 2012).  **Personnel** – The incident management personnel will include an Incident Response Coordinator (IRC), Designated Incident Handlers (DIH), and the Incident Response Team. The IRC is the central point of contact and is responsible for verifying and logging all incidents (Santos, 2019). DIHs are senior-level personnel with relevant crisis management, communication skills, experience and knowledge to handle incidents (Santos, 2019). The divisional Incident response teams may comprise the team leader, a communications lead, Legal support, a Technical lead, an interface to the security committee, a security officer, a note-taker, a network, desktop and server personnel (Innovation, Science and Economic Development Canada, 2021; Speed & Ellis, 2003).  **Incident Response Roles and Responsibilities**:  The responsibility of the IRT includes – investigation and analysis, response and improvement, communications, and reporting (Moore, 2023).  **Sharing information with outside sources** – Communication with law enforcement, the media, Customers, Internet Service Providers (ISP), Software and Support Vendors, Owners of attacking IP addresses, and other IRTs will be enforced based on applicable laws and overseen by the DIH lead in collaboration with upper management, as well as the company’s legal and PR departments (Cichonski et al., 2012; Santos, 2019).  **Testing** – To ensure the effectiveness of the IRP, the plan needs to be thoroughly tested through tabletop exercises and simulation incidents to ensure it would be effective in real-world incidents (Cichonski et al., 2012). |
| **Preparation** | * The cyber security team creates controls based on Sony Picture’s cyber risk assessment (Cichonski et al., 2012). * This stage ensures the organization possess the staffing and training necessary to enhance risk assessment capabilities (Criminal Justice Information Centre, n.d.). * The CISO is responsible for ensuring Sony pictures has appropriately deployed network security, host security and malware prevention solutions (Santos, 2019). * The CISO and the Incident Response coordinators will work together to ensure communications and facilities necessary for the IRT to function are in place (Santos, 2019). * They will also ensure the organization has appropriate incident analysis and mitigation software and hardware (Innovation, Science and Economic Development Canada, 2021).   **Staffing** –Sony Picture’s employees will comprise the incident response team, with limited technical or administrative support from outside contractors. Employees will be available full-time, with 24/7 availability to handle any cyber-security incident (Cichonski et al., 2012).  **Training** – All employees, contractors, consultants, and vendors will receive incident response training appropriate to their role.  **Tools and Resources** – tools and resources needed to successfully investigate and resolve cybersecurity incidents, as recommended by the Incident Response Team (IRT), will be treated and provided as a priority (Santos, 2019). |
| **Detection** | **Prerequisites** – To ensure incidence response is efficient at Sony Pictures, it is necessary to establish a profile of the company’s networks and systems, understand normal behaviours, and institute a log retention policy (Santos, 2019). So as to monitor and identify events as they occur (Carnegie Mellon University, 2016).  **People** – Detection is often the responsibility of the help desk and network operations centers; however, an employee in any unit of the organization may also help escalate any suspicious activities (Carnegie Mellon University, 2016).  **Detection Tools** – Relying on employees and the company’s cyber security accounting is reliable, only to an extent. It is necessary to have further safeguards that will help immediate detection of cyber security incidents (Santos, 2019), as the cyber security team recommends. Examples include a firewall, Intrusion Detection and Prevention systems (IDS), Security Information and Event Management (SIEM) products, file integrity checking software, Antivirus and antispam software, third-party monitoring services, as well as frequent vulnerability checks (Cichonski et al., 2012).  **Incident Reporting** – Once a suspicion is detected, the Incident Response Coordinator (IRC) is notified, who assigns it to the Designated Incident Handler (DIH). The DIH evaluates the incident report to determine whether it is an incident. If not, the DIH reports back to the IRC for follow-up. If it is an incident, the Designated Handler will declare it as such. And depending on the category (Level 1, 2, or 3), he would initiate the path for the appropriate response, which may involve the Incident Response Team, an information system custodian, the data/process owner, or HR personnel.  Diagram  Description automatically generated  *Figure 1: Incident Response Roles and Responsibilities. Source; Santos (2019).* |
| **Analysis** | The incident response team must promptly confirm an incident -including the attack approach and what assets were impacted – and analyze the extent of the effect (Duran, 2022).  Information is gathered from detection tools such as log files, error messages, firewalls and IDPS to find evidence that would help determine if an incident has occurred and what category/level (Innovation, Science and Economic Development Canada, 2021).  The analysis includes event categorization, prioritization, data correlation and analysis, incident declaration, incident analysis and response determination (Carnegie Mellon University, 2016).  The DIH evaluates and categorizes the incident reported and initiates follow-up action (Cichonski et al., 2012). Incidents are prioritized and responded to based on the impact of the incident on functionality, information confidentiality, integrity, and recoverability (Cichonski et al., 2012). Level 1 incidents are the highest priority because they cause significant harm and are responded to immediately upon report (Santos, 2019). Thus, the IRT is assembled to take further action. The CEO, COO, legal counsel and CISO must be informed of Level 1 incidents (Santos, 2019).  A level 2 incident must be handled within four (4) hours, and the COO, legal counsel and CISO must be kept informed (Santos, 2019).  A level 3 incident must be handled within 24 business hours, and the CISO must be kept in the loop (Santos, 2019).  The IRT must record all facts concerning the incident immediately (Juno Risk Solutions, n.d.). |
| **Containment** | This is a more technical part of the Incident Response Plan. It includes actions taken to limit damage and prevent further damage from the incident (Innovation, Science and Economic Development Canada, 2021).  Based on the discretion of the Incident Response Team, activities include (Criminal Justice Information Centre, n.d.; Juno Risk Solutions, n.d.):   * Identify affected host * Identification of attacker(s), * Shutting down affected systems or disconnecting them from the network, * Identification of malware and its capabilities, * Identifying and monitoring attacker(s)’ communication channels   In most cases, these activities must occur simultaneously to prevent further damage (Criminal Justice Information Centre, n.d.). It is worthy of note that the containment strategy to be used depends on the type of cyber-attack incident (Cichonski et al., 2012). The company’s set SOP for handling different attacks will be deployed here. |
| **Communication** | The communication lead is responsible for working in collaboration with the CISO, upper management, legal department, and PR department to make internal and external communications with stakeholders based on applicable laws and Sony Pictures set communication policy (Santos, 2019) |
| **Eradication** | Eradication is equally a technical phase. It involves removing system infections and restoring affected systems (Innovation, Science and Economic Development Canada, 2021). Activities include - deleting a malware, disabling a breached user account, and update to system controls (Juno Risk Solutions, n.d.). It also consists of identifying and mitigating potential vulnerabilities and misconfigurations that led to or can lead to future exploitation. (Criminal Justice Information Centre, n.d.). |
| **Recovery** | Affected systems are restored to normal operational status, and vulnerabilities are fixed to prevent similar incidents (Juno Risk Solutions, n.d.).  The recovery stage is often technical, involving OS and application changes (Cichonski et al., 2012). However, collaborative efforts from management and other units of the organization are necessary to ensure success (Santos, 2019).  Activities include – “restoring systems from backups, rebuilding systems from approved baselines, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security” (Criminal Justice Information Centre, n.d.).  For large-scale incidents like the 2014 attack on Sony Pictures, recovery may take months (Sanchez, 2015). The early phase would be focused on increasing the company’s overall security, operationality and changes to prevent future incidents (Cichonski et al., 2012). Long-term changes are infrastructural and include further efforts to increase enterprise security (Santos, 2019).  Testing, monitoring and system validation is necessary to ensure that the network systems are no longer infected by malware and are not compromised in any other way (Innovation, Science and Economic Development Canada, 2021). |
| **Post-Event Analysis** | Involves reflection, compilation, and analysis of activities that led to the security incident, actions that were taken by all involved in the security incident, including the IRT, lessons learned are documented, decisions are made on how to use collected data, and evidence is retained (Criminal Justice Information Centre, n.d.; Santos, 2019).  The goal is to review how effectively the Incident Response Plan was executed during an incident and to improve SPE’s security architecture (Juno Risk Solutions, n.d.).  Incident Response Report (IRR) is required within 14 days of the completion of an incident investigation. A post-incident report must include – business/ customer impact, incident severity, root cause description, repair items, timeline, and external public statement where necessary (StateRAMP, 2021). |

**EXECUTIVE SUMMARY**

**Overview of Risk Mitigation Strategy**

The North Korean hacking incident has caused a major security breach in Sony Entertainment. To prevent any similar attacks in the future, it is crucial to take steps to protect the company. One important measure is to develop a risk mitigation strategy that can reduce the likelihood of future breaches and ensure the confidentiality, integrity, and availability of the company's information assets (Sanchez, 2015). With a comprehensive risk mitigation strategy in place, the impact of any potential security incidents can be minimized, and the organisation's reputation, customer trust, and financial stability can be safeguarded (Sanchez, 2015).

**Vision of Risk Mitigation Strategy**

Sony's risk-mitigation plan will ideally:

* Improve the company's cybersecurity posture by putting in place different steps to better avoid, identify, and react to cyber threats.
* Contribute to the confidentiality, integrity and availability inside the company.
* Ensure compliance with industry regulations and standards related to cyber security. This includes the General Data Protection Regulation (GDPR), ISO 27701 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
* Support business continuity: This will allow the company to continue key business processes even if there was a cyber-attack.

**Strategic Goals and Objectives**

*Table: Strategic Goals and Objectives*

|  |  |
| --- | --- |
| **Strategic Goal** | **Objectives** |
| Enhancing Security Controls: The goal of enhancing security controls is to improve the overall security posture of the organization by implementing additional security measures and controls. This involves identifying and addressing vulnerabilities in our systems, networks, and applications. This process includes measures such as multifactor authentication, regular software and hardware updates, and network segmentation to reduce the attack surface and mitigate the cyber-attack risk. | *Objective 1:*Implement multifactor authentication (MFA) for all employees to reduce the risk of unauthorized access to systems and data. This objective involves implementing a secure login process that requires users to provide two or more forms of authentication to access critical systems and applications. This could include a password, a smart card, or biometric authentication. By implementing MFA, Sony Entertainment can reduce the risk of unauthorized access, even if an attacker gains access to a user's credentials. |
| *Objective 2:* Regularly update and patch software and hardware to address vulnerabilities and minimize the attack surface. This objective involves implementing a proactive approach to system and software updates, patching, and maintenance. Sony Entertainment should regularly review system logs and security alerts to identify vulnerabilities and apply necessary security patches and updates to minimize the attack surface. Regular patching ensures that known vulnerabilities are addressed, reducing the risk of successful cyber-attacks. |
| Strengthening Incident Response: The goal is to ensure the organization is prepared to respond quickly and effectively to security incidents. This includes establishing an incident response plan, defining roles and responsibilities, conducting regular training and simulations, and implementing incident escalation procedures. | *Objective 1:* Establish an incident response plan defining roles, responsibilities, communication protocols, and incident escalation procedures. This objective involves developing and implementing a formal incident response plan that describes how the organization will respond to a security incident. The plan should include defined roles and responsibilities, communication protocols, and incident escalation procedures to ensure a rapid and effective response to security incidents. |
| *Objective 2:* Conduct regular tabletop exercises and simulations to test the incident response plan and identify areas for improvement. This objective involves conducting simulated security incidents to test the incident response plan and identify areas for improvement. Regular testing and simulations help to identify gaps in the plan and ensure that the organization is prepared to respond to a security incident effectively. |
| Improving Security Awareness: The goal of improving security awareness is to educate employees, contractors, and partners on the importance of cybersecurity and promote security best practices. We recognize that human error is a significant contributor to security incidents. Therefore, we will invest in training and awareness programs to educate our employees about security risks and best practices. This includes providing comprehensive security training, implementing security awareness campaigns, and reinforcing security behaviours to reduce the risk of security incidents caused by human error. | *Objective 1:* Develop and deliver comprehensive security training programs for employees, contractors, and partners to promote security awareness and best practices. This objective involves providing comprehensive security training programs for employees, contractors, and partners to ensure they are aware of the latest security threats, best practices, and policies. The training should include topics such as password security, social engineering attacks, phishing, and other security awareness topics. |
| *Objective 2:* Implement a security awareness campaign that includes regular reminders, newsletters, posters, and other awareness materials to reinforce security behaviours. This objective involves implementing a security awareness campaign that uses periodic reminders, newsletters, posters, and other awareness materials to reinforce security behaviours. The campaign should promote the importance of security awareness and best practices to reduce the risk of security incidents caused by human error. |
| Ensuring Regulatory Compliance: The goal of ensuring regulatory compliance is to ensure that the organization is complying with all applicable regulations, standards, and laws. This includes establishing a compliance program, conducting regular risk assessments, monitoring regulatory requirements, and auditing security controls to ensure ongoing compliance. By meeting regulatory requirements, the organization can mitigate the risk of fines, legal action, and reputational damage. | *Objective 1:* Establish a compliance program that includes regular risk assessments, policy development, and monitoring of regulatory requirements. This objective involves establishing a compliance program that ensures that the organization is meeting all relevant regulatory requirements, including data privacy laws, financial regulations, and industry standards. The program should include regular risk assessments, policy development, and monitoring to ensure ongoing compliance. |
| *Objective 2:* This objective involves regularly auditing and assessing security controls to ensure that the organization is complying with all applicable regulations, standards, and laws. The audit and assessment process should include identifying gaps in security controls and taking corrective action to ensure ongoing compliance. |

*Note.* Strategic Goals and Objectives. From Canadian Centre for Cyber Security. (2021, June). *Top Measures to Enhance Cyber Security for Small and Medium Organizations (ITSAP.10.035).* Copyright 2021 by Government of Canada. From *What are Security Controls? | IBM*. (n.d.). Copyright by IBM.

**The Assessment Metrics for the Objectives**

*Table: Assessment Metrics for Objectives*

|  |  |  |
| --- | --- | --- |
| **Strategic Goal** | **Objectives** | **Metrics** |
| Enhancing Security Controls | Multi-Factor Authentication | 1. Percentage of systems with multifactor authentication enabled  2. Number of successful login attempts blocked by multifactor authentication  3. Time to implement multifactor authentication on all systems |
| Enhancing Security Controls | Regular Updates | 1. Percentage of systems with up-to-date patches and software versions  2. Number of vulnerabilities identified and patched during regular updates  3. Time to deploy updates to all systems |
| Strengthening the Incident Response Process | Incident Response Plan | 1. Percentage of employees who have read and understand the incident response plan  2. Number of successful incidents resolved using the incident response plan  3. Number of unsuccessful attempts to resolve incidents using the incident response plan |
| Strengthening the Incident Response Process | Regular Tabletop Exercises | 1. Percentage of employees who participate in regular tabletop exercises  2. Time to complete tabletop exercises and identify gaps in the incident response plan  3. Number of identified gaps that were addressed and resolved before a security incident occurred |
| Improving Security Awareness | Security Training Programs | 1. Percentage of employees who have completed comprehensive security training  2. Time to complete training for all employees  3. Number of identified security incidents caused by employee error before and after training was implemented |
| Improving Security Awareness | Security Awareness Campaign | 1. Number of security awareness campaigns conducted annually  2. Percentage of employees who participate in security awareness campaigns  3. Number of identified security incidents caused by employee error before and after security awareness campaigns were implemented |
| Ensuring Regulatory Compliance | Compliance Program | 1. Percentage of employees who have received compliance training  2. Number of identified compliance issues  3. The time used for solving identified compliance issues |
| Ensuring Regulatory Compliance | Regular Audits and Assessments | 1. Number of compliance audits and assessments conducted annually  2. Percentage of audit findings that were addressed and resolved  3. Time to resolve audit findings and implement corrective actions |

**Threat Actors and Methods of Attack**

*Table: Threat Actors and Methods of Attack*

|  |  |  |
| --- | --- | --- |
| **Threat Actor** | **Method of Attack** | **Protection** |
| Malware: Malicious software installed without the user's knowledge | E-mail attachments, drive-by downloads, malicious website connections | * Keep software updated * Use a security program * Use mail filtering and spam filtering * Don't click on links in pop-ups * Minimize the number of apps on your computer * Block harmful websites * Allow only known file types to be downloaded * Use remote desktop protocols only when needed |
| Ransomware:  Encrypts files or locks a user out of their computer, demanding payment to restore access | Malicious software, e-mail attachments, drive-by downloads, malicious website connections | * Keep software updated * Use a security program * Use mail filtering and spam filtering * Don't click on links in pop-ups * Minimize the number of apps on your computer * Block harmful websites * Allow only known file types to be downloaded * Use remote desktop protocols only when needed |
| Distributed Denial of Service (DDoS): An attack that floods a network or website with traffic, overwhelming it and causing it to crash | Utilized multiple workstations (Botnets) | * Develop a DoS defense strategy * Install a monitoring tool to detect traffic surges * Install firewalls * Use anti-virus and anti-malware programs * Use layered security mechanisms |
| Cyber Espionage: Cyberattack that maliciously accesses, steals, or discloses secret information | E-mail attachments, drive-by downloads, malicious website connections | * Update software programs * Use multi-factor authentication * Segment networks * Observe unusual behaviour * Use a proactive detection strategy * Review Policies * Limit access to sensitive data |
| Social Engineering: Attack that relies on human interaction to gain unauthorized access | E-mail attachments, drive-by downloads, malicious website connections | * Use updated security software programs * Recognize phishing messages * Protect accounts with multifactor authentication * Report and delete phishing emails |
| Phishing: Attack that steals sensitive information through fake websites | E-mail attachments, drive-by downloads, malicious website connections | * Recognize phishing messages * Protect accounts with multifactor authentication * Report and delete phishing emails |
| Spear Phishing: Targeted phishing attack with attention-grabbing messages | E-mail attachments, drive-by downloads, malicious website connections | * Recognize phishing messages * Protect accounts with multifactor authentication * Report and delete phishing emails |

*Note.* From Canadian Centre for Cyber Security. (2022). DDoS protection for your business. Copyright 2022 by CCCS; Federal Trade Commission Consumer Advice. (2022). How to recognize and avoid phishing scams. Copyright 2022 by FTCCA.; Malwarebytes. (2022). Cyber espionage: How to protect your intellectual property from cyber spies. Copyright 2022 by Malwarebytes.; McAfee. (2022). Malware: What is malware, and how to prevent it? Copyright 2022 by McAfee; Microsoft. (2022). How to recognize and avoid phishing scams. Copyright 2022 by Microsoft.; National Cyber Security Centre. (2022). Protecting against malware. Copyright 2022 by NCSC.

**Business Critical Assets and Vulnerabilities**

*Table: Critical Business Assets of Sony Entertainment with Possible Vulnerabilities*

|  |  |  |
| --- | --- | --- |
| **Critical Asset** | **Importance** | **Vulnerabilities** |
| Intellectual Property | Sony Entertainment has a vast library of original content, including movies, TV shows, music, and video games. These assets are crucial to the company's success as they generate revenue and help maintain its market position. | Cyber espionage, hacking, insider threats, physical theft, use of malicious code to steal or destroy intellectual property |
| Talent Pool | The company's talent pool is also a critical asset, including actors, directors, producers, and musicians. The success of Sony's projects heavily depends on the quality and popularity of the talent involved. | Lack of security controls to protect sensitive employee information, phishing attacks, social engineering |
| Distribution Channels | Sony's ability to distribute its content through various platforms, including theatres, streaming services, and retail outlets, is also a critical asset. The company needs to maintain strong relationships with these channels to ensure its content reaches the right audiences | Cyber-attacks on partners or vendors, supply chain attacks, inadequate vetting of suppliers |
| Brand Reputation | Sony Entertainment's brand reputation is another important asset, as it influences customer loyalty and the perception of the company's quality and trustworthiness. | Negative publicity on social media, fake social media accounts, brand impersonation |
| Technology and Infrastructure | The company may rely on specific technology and infrastructure, such as servers, software, and network systems, to produce, store, and distribute its content. Ensuring the availability and security of these systems is critical to the company's operations. | The exploitation of vulnerabilities, inadequate security controls, insider threats, third-party risks |
| Financial Resources | Access to financial resources, such as investment capital, loans, and credit lines, is essential for the company to fund its operations and growth. Sony Entertainment may need to maintain strong relationships with financial institutions and investors to ensure it has the necessary resources to meet its goals. | Fraud, embezzlement, cyber-attacks on financial systems, insider threats |
| Human Resources | Sony Entertainment may consider its employees as a critical asset as well, as they are responsible for creating, producing, and distributing the company's content. The company may need to attract and retain talented individuals in various fields, including creative, technical, and administrative roles, to maintain its operations and competitive edge. | Insider threats, social engineering, phishing attacks, lack of security awareness training |
| Customer Data | The customer data that Sony Entertainment holds, including personal information, purchase history, and preferences, is a critical asset that the company must protect. It is essential to maintaining customer trust and complying with relevant data protection regulations. | Data breaches, phishing attacks, social engineering, insider threats, inadequate encryption of sensitive data |

*Note.* From Sanchez, G. (2015). Case Study: Critical Controls that Sony Should Have Implemented. *Global Information Assurance Certification Paper. SANS Institute*. Copyright 2015 by SANS Institute.

**Cybersecurity Governance**

The Cyber Security Governance Plan ensures that the organization has a robust cybersecurity program and that cyber security risks are identified, assessed, and mitigated promptly and effectively (CISA, n.d.).

1. ***Cyber Security Leadership Plan***
2. Cyber Security Steering Committee: Create a steering committee for cybersecurity that includes executives from various departments to supervise governance, risk management, and compliance in cybersecurity. The committee will offer advice and leadership to the Chief Information Security Officer and the cybersecurity team, ensuring that cybersecurity efforts are consistent with the organization's overall strategic goals.
3. Define the scope and objectives of the cyber security steering committee, including its roles and responsibilities, decision-making authority, and reporting structure (SANS Institute, 2023).
4. Identify and appoint executives from different departments to join the cyber security steering committee (MIT, n.d.).
5. Develop a charter outlining the committee's purpose, composition, and operating procedures.
6. Conduct regular meetings to review and approve cybersecurity policies and procedures, assess cybersecurity risks, and ensure that cybersecurity is aligned with the organization's strategic objectives (SANS Institute, 2023).
7. Chief Information Security Officer (CISO): Appoint a Chief Information Security Officer (CISO) to lead the cybersecurity team and report to the Chief Information Officer (CIO) or Chief Executive Officer (CEO). The CISO will be responsible for managing the organization's cybersecurity program, developing cybersecurity policies and procedures, and implementing security controls.
8. Define the role and responsibilities of the CISO, including their reporting structure, authority, and accountability (SANS Institute, 2023).
9. Develop a job description for the CISO that outlines their qualifications, skills, and experience (MIT, n.d.).
10. Identify and recruit a qualified candidate for the CISO position based on the job description and selection criteria (SANS Institute, 2023).
11. Provide the CISO with the necessary resources and support to carry out their responsibilities, including a dedicated cybersecurity team, budget, and access to senior executives.
12. Cyber Security Program:
13. Develop a cybersecurity program that includes policies, procedures, and standards for information security, network security, and application security.
14. Conduct regular risk assessments to identify cybersecurity risks and develop mitigation strategies (SANS Institute, 2023).
15. Establish a security governance framework that includes roles, responsibilities, and accountability for cybersecurity across the organization (MIT, n.d.).
16. Implement a continuous monitoring program that includes threat intelligence, vulnerability assessments, and incident response capabilities (SANS Institute, 2023).
17. Communication and Collaboration:
18. Foster a cybersecurity awareness and communication culture throughout the organization, including regular training and awareness programs (MIT, n.d.).
19. ***Management Process Improvement Plan***

As a result of this incident, Sony can create a management process improvement plan that includes the following measures to prevent and mitigate the impact of future cyber-attacks:

1. Evaluate the security policies and protocols in place by conducting risk assessments and develop a plan to address potential vulnerabilities. Cyber-attacks can negatively impact an organization's reputation and financial health. It is essential to implement a crisis management plan to address such incidents (Swanagan, 2022).
2. Assist employees and managers with developing a communication protocol and notification procedure for responding to cyber-attacks (Santos, 2019). This can serve as a blueprint or guide during an attack (Swanagan, 2022).
3. Improve security awareness and create a culture of cyber-safety among employees by educating and training them and gathering their feedback. Practice response management practices by conducting drills. The use of advanced technologies should be regularly assessed and audited to ensure that security measures are being taken (Gelnaw, 2019).
4. An organization's management must appoint a succession of individuals with the chain of command and responsibility to oversee different incidents (Santos, 2019). Coordinate response to cyber-attacks by implementing a centralized authorization practice. Improve collaboration and communication between departments to combat cyber-attacks (Jollans, 2018).
5. Threat intelligence can be shared more effectively by collaborating and exchanging information with other companies and government agencies (Cyber Fusion, 2022).
6. ***Cybersecurity Awareness-Training Program***

Implementing a Cybersecurity and Awareness Training program on specific topics is required to train and remind users of imminent dangers and to make them an effective first line of defence against attack, intrusion, and error (Santos, 2019). Steps to implement a training program:

*Table: Suggested Steps to Implement Awareness- Training Program*

|  |  |  |
| --- | --- | --- |
| Step 1 | Involve Company Leadership | By taking this step as a priority, you can avoid any possible hindrances in the future, as the company's resources will be directed towards this goal. |
| Step 2 | Performing a risk assessment of your current systems | Identifying the areas that pose the most significant risk to business security helps prioritize and tailor the training program to effectively |
| Step 3 | Define the content | The subsequent stage involves creating the training content, which should include subjects like data protection, password management, malware, phishing attacks, and social engineering. |
| Step 4 | Select training method | Choosing the appropriate method of delivering cybersecurity training, such as classroom sessions, online courses, workshops, or simulations, is based on various factors, including the audience, availability of resources, and budget. |
| Step 5 | Develop the training schedule | The timetable should be structured to guarantee all personnel receive training, including the new employees. |
| Step 6 | Deliver the training | The training should be engaging, interactive, and informative. |
| Step 7 | Simulate attacks | Assessing employees to determine their comprehension and adherence to cybersecurity best practices. |
| Step 8 | Compile test results and improve | A successful training program should consist of advanced reporting tools that provide information about effectiveness. |
| Step 9 | Implement and Enforce New Policies | This step is crucial and should be carried out appropriately. |
| Step 10 | Retrain Employees Regularly | Organizing cybersecurity training sessions every three or six months can emphasize to employees the significance of this effort and help them retain the information they have acquired. |
| Step 11 | Be Consistent and Stay Informed | To keep up with the ever-changing cyber threats and methods of compromise, the company needs to motivate its employees to revisit their training resources regularly. |

# *Note.* Adapted From Jennings, M. (2022). 8 Steps to Implement a Cyber Security Awareness Training Program, SymQuest, Copyright 2022 by SymQuest.

Designing and implementing a training program requires addressing the elements mentioned below.

*Table: Elements That Need to Be Addressed in The Awareness-Training Program*

|  |  |  |
| --- | --- | --- |
| **Item** | **Description** | **Number of step/s that item had been implemented.** |
| Compliance | Immediate Compliance Requirements to the Organization | Step 9 |
| New Users | Training Programs for New Employees and Contractors as They Begin Employment | Step 5 |
| Periodic | Periodic Training (Specialized or General) | Step 10 |
| Ongoing | Ongoing Cybersecurity Awareness Programs | Step 11 |

*Note.* Adapted FromSantos, O. (2019). Developing Cybersecurity Programs and Policies, Copyright 2019 by Pearson Education, Inc.

**Cyber Security, Internal Physical Security, And External Physical Security**

A good cybersecurity plan has multiple layers of defence against cyber threats. Each of the domains below, which are open to cyber threats, should be protected by related technologies by Sony Pictures Entertainment (SPE) (IBM, n.d.).

|  |  |
| --- | --- |
| **Domain** | **Protective Technology** |
| Critical Infrastructure Security | The National Institute of Standards and Technology (NIST) has made a protection system to help organizations protect computer systems, networks and other assets in this area. |
| Network Security | Systems that assist with safeguarding both on-premises and cloud-based apps. Applications should be designed with security in mind, taking into account how data is treated, how users log in, etc. |
| Application Security | Encrypting cloud data in storage, in motion and in use to protect client privacy, business needs, and legal compliance. |
| Cloud Security | Data protection policies, like the General Data Protection Regulation (GDPR), keep your most private data from being accessed, shared, or stolen by people who shouldn't be able to. |
| Information Security | To improve security, the whole organization needs to learn more about security. Users can be taught to remove strange email files, not use USB devices they don't know about, and so on. |
| End-User Education  Business continuity planning | Methods and procedures for dealing with unplanned events like natural disasters, power blackouts, or cyberattacks in a way that causes the least amount of trouble to key processes. |
| Disaster Recovery/ | Implementing sustainable storage infrastructure such as IBM FlashSystem® |
| Storage Security | Using validated unified endpoint management (UEM) program such as “IBM Security® MaaS360 with Watson.” |

*Note.* From IBM. (n.d.). What are Security Controls? Copyright by IBM.

**Cyber Security Questions:**

1. What are our critical assets, and are they secure? (Pearlson, 2023)
2. What kind of data breach, whether caused by malware, a computer attack, or a mistake made by a person, would significantly affect our business? (Tunggal, 2023)
3. What is the amount of effect each identified threat could have? (Tunggal, 2023)
4. What are the vulnerabilities of my system? What will happen if these vulnerabilities are exploited? (Tunggal, 2023)
5. What are our response plans in case of a cyber-attack? (Pearlson, 2023)

*Table: Technologies That Can Be Implemented for Cybersecurity*

|  |  |
| --- | --- |
| **Technology** | **Description** |
| Identity and Access Management (IAM) | It keeps track of users' digital names and entry rights when they use a company's systems, networks, and data. IAM methods like single sign-on, multifactor authentication, special user accounts, and user lifetime management are used to make sure that users only have access to the tools they need to do their jobs and to keep private data from being accessed by people who shouldn't be able to see it. |
| Comprehensive data security platform | Its main goal is to secure digital data and block data leaks. This technology gives organizations automated, real-time data flaws and ongoing tracking that warns them of data vulnerabilities. Backups and encryption can also be provided by this tool. |
| Security Information and Event Management (SIEM) technology | Security Information and Event Management (SIEM) is a protection system that collects and analyses data from security events to find suspicious user actions and cause a preventative or corrective reaction. |

*Note.* From IBM. (n.d.). What are Security Controls? Copyright by IBM.

**Internal Physical Security Questions:**

1. Do we have security policies and procedures in place, and are they satisfactory? (Sassi, 2023)
2. Do we have access controls to sensitive areas and critical systems? (Sassi, 2023)
3. Are security cameras in high-risk places like entrances, exits, and data centers? If so, how often are they checked? (Sassi, 2023)
4. Are employees taught regularly for physical security, such as how to handle passwords, recognize phishing, and avoid social engineering? (Sassi, 2023)
5. Are the visitors and contractors coming to the office by signing in and being escorted? (Sassi, 2023)

*Table: Technologies That Can Be Implemented for Internal Physical Security*

|  |  |
| --- | --- |
| **Technology** | **Description** |
| Surveillance | Guards, danger alarms, CCTV, sound and movement sensors, and logs of who went where are all part of surveillance. |
| Alarm systems | Alarm devices alert security of unauthorized entry to crucial areas. |
| Access control systems | It restricts the entrance of unauthorized employees to crucial areas. |

*Note.* From Devoteam. (2023, March 21). Cybersecurity | The importance of Physical Security Copyright 2023 by DevoTeam

**External Physical Security Questions:**

1. How are perimeter controls, such as walls, fencing and gates, maintained and monitored? (ISO, 2022)
2. How are surveillance and detection technologies used to monitor the external environment? (ISO, 2022)
3. What is the process for managing and controlling access to the organization’s physical facilities? (ISO, 2022)
4. How are physical security incidents responded to, and what is the process for reporting them to law enforcement? (ISO, 2022)
5. What are the procedures for testing and updating the organization’s physical security controls? (ISO, 2022)

*Table: Technologies That Can Be Implemented for External Physical Security*

|  |  |
| --- | --- |
| **Technology** | **Description** |
| Video Surveillance | To monitor the movement of the external area of the company | |
| Perimeter Security | Includes walls and gates to make it harder for people to get into crucial areas. | |

*Note.* From Devoteam. (2023, March 21). Cybersecurity | The importance of Physical Security Copyright 2023 by DevoTeam

**References**

Aon (2022). Use These 8 Successful Strategies to Mitigate Growing Ransomware Risk; <https://www.aon.com/insights/articles/2022/ransomware-epidemic-8-strategies-to-mitigate-risk>

Bandos, T. (2016, September 20). *The Five Steps of Incident Response*. Digital Guardian. <https://digitalguardian.com/blog/five-steps-incident-response>

Canadian Centre for Cyber Security. (2021, June). Top Measures to Enhance Cyber Security for Small and Medium Organizations (ITSAP.10.035) - Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035>

Canadian Centre for Cyber Security. (2022). Guidance <https://cyber.gc.ca/en/guidance/protecting-your-organization-against-denial-service-attacks-itsap80100>

Carnegie Mellon University. (2016). *CRR Supplemental Resource Guide Incident Management*. https://www.cisa.gov/sites/default/files/c3vp/crr\_resources\_guides/CRR\_Resource\_Guide-IM.pdf

‌ Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. *Computer Security Incident Handling Guide*, *2*(2). <https://doi.org/10.6028/nist.sp.800-61r2>

‌CISA. (n.d.). *Cybersecurity Governance*. Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance>

Colatin, S. D. T. (2021, June 9). *Sony Pictures Entertainment attack (2014) - International cyber law: interactive toolkit*. Cyberlaw.ccdcoe.org. <https://cyberlaw.ccdcoe.org/wiki/Sony_Pictures_Entertainment_attack_(2014)>

Criminal Justice Information Centre. (n.d.). Example Incident Response Plan. In *Michigan State Police*. https://www.michigan.gov/-/media/Project/Websites/msp/cjic/pdfs6/Example\_Incident\_Response\_Policy.pdf?rev=4bf335b6d1344226a92a0947bc8688ec

‌CrowdStrike. (2021, May 6). *Incident Response [Beginner’s Guide] | CrowdStrike*. Crowdstrike.com. <https://www.crowdstrike.com/cybersecurity-101/incident-response/>

Cyber Fusion. (2022, July 25). *What is Security Collaboration in Cybersecurity?* Retrieved from <https://cyware.com/security-guides/cyber-fusion-and-threat-response/what-is-security-collaboration-in-cybersecurity-1907>

DeSot, T. (2015, September 15). *8 Lessons to Learn from the Sony Breach*. Security Magazine. <https://www.securitymagazine.com/articles/86649-lessons-to-learn-from-the-sony-breach>

Devoteam. (2023, March 21). Cybersecurity | The Importance of Physical Security. Devoteam. <https://www.devoteam.com/expert-view/cybersecurity-the-importance-of-physical-security/>

Dhillon, G. (2016). *The Changing Faces of Cybersecurity Governance: What To Do Before And After A Cybersecurity Breach?* <https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf>

Duran, D. (2022, July 7). *NIST Incident Response Plan*. Rhyno Cybersecurity. https://rhyno.io/nist-incident-response-plan-steps-and-template/

‌Embroker Team. (2022, December 7). *How to Design a Cyber Incident Response Plan for Your Business*. Retrieved from [https://www.embroker.com/blog/cyber-incident-response-plan](https://www.embroker.com/blog/cyber-incident-response-plan/#:~:text=Create%20a%20Detailed%20Response%20Plan%20Checklist,-According%20to%20the&text=Identification%3A%20Identify%20the%20breach.,to%20their%20pre%2Dincident%20state)

Federal Cybersecurity and Data Privacy Laws Directory. (2022). Retrieved from <https://www.itgovernanceusa.com/federal-cybersecurity-and-privacy-laws>

‌Federal Trade Commission Consumer Advice, (2022, October 25); How to Recognize and Avoid Phishing Scams. <https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

Gelnaw, A. (2019, March 22). *The Importance of Continuous Improvement in Security Performance Management*. Retrieved from <https://www.bitsight.com/blog/importance-continuous-improvement-security-performance-management>

Glover, C. (2022). The Difference Between Threat, Vulnerability, and Risk, and Why You Need to Know <https://www.travasecurity.com/blog/the-difference-between-threat-vulnerability-and-risk-and-why-you-need-to-know>

Hess, A. (2015, November 22). *Inside the Sony Hack: What it was like to be a rank-and-file Sony employee as the unprecedented cyberattack tore the company apart.* Slate Magazine. <http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html>

Hesseldahl, A. (2015, January 20). Here's What Helped Sony's Hackers Break In: Zero-Day Vulnerability. Vox. <https://www.vox.com/2015/1/20/11557888/heres-what-helped-sonys-hackers-break-in-zero-day-vulnerability>

Huang, K., & Pearlson, K. (2019). *MIT CAMS -Organizational Cybersecurity Culture Building a Model of Organizational Cybersecurity Culture Identifying Factors Contributing to a Cyber-secure Workplace 2019 Survey Results MIT CAMS -Organizational Cybersecurity Culture 2*. <https://cams.mit.edu/wp-content/uploads/Culture_Survey_Report_Findings_Dec2019.pdf>

IBM. (n.d.) What is Cybersecurity? <https://www.ibm.com/topics/cybersecurity>

IBM. (n.d.). What are Security Controls? <https://www.ibm.com/topics/security-controls>

Innovation, Science and Economic Development Canada. (2021, December 8). *Develop an Incident Response Plan: Fillable template and example*. Government of Canada. <https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-tools/develop-incident-response-plan-fillable-template-and-example>

‌Irwin, L. (2014, December 17). *Despite appointing military-grade CISOs, archaic systems result in Sony breach*. Retrieved from <https://www.vigilantsoftware.co.uk/blog/despite-appointing-military-grade-cisos-archaic-systems-result-in-sony-breach>

‌ISBuzz. (2015, December 7). How Destover Evades Detection. Information Security Buzz. <https://informationsecuritybuzz.com/new-toolset-linked-to-destover-attackers-arsenal-helps-them-to-broaden-attack-surface/>

ISO. (2022, June 13). ISO 27002:2022 - Control 7.1 - Physical Security Perimeters. ISMS.online.[https://www.isms.online/iso-27002/control-7-1-physical-security-perimeters](https://www.isms.online/iso-27002/control-7-1-physical-security-perimeters/#:~:text=Physical%20security%20perimeters%20may%20include,monitor%20activity%20outside%20the%20facility)

Jennings, M. (2022, November 9). *8 Steps to Implement a Cyber Security Awareness Training Program*. <https://blog.symquest.com/steps-to-implement-a-cyber-security-awareness-training-program-at-your-company>

Juno Risk Solutions. (n.d.). *Cyber Incident Management Planning Guide For IIROC Dealer Members*. <https://www.iiroc.ca/media/12571/download?inline>

Jollans, A. (2018, August 13). *Three ways to collaborate to improve cybersecurity*. Retrieved from <https://www.ibm.com/blogs/systems/three-ways-collaborate-improve-cybersecurity/>

‌Kaspersky. (2022, February 9). What is a Zero-day Attack? - Definition and Explanation. www.kaspersky.com. <https://www.kaspersky.com/resource-center/definitions/zero-day-exploit>

Keise, E. (2014, December 3). *Chief information security officers hard to find — and harder to keep*. Retrieved from <https://www.usatoday.com/story/tech/2014/12/02/sony-hack-attack-chief-information-security-officer-philip-reitinger/19776929/>

Knowles, M. (2023, March 1). Cybersecurity Risk Management: Frameworks, Plans, & Best Practices. Hyperproof. https://hyperproof.io/resource/cybersecurity-risk-management-process/

Li, M. (2018, May 12). *The Sony Pictures Entertainment Hack Case Report - Muyuan Li*. Medium. <https://medium.com/@muyuanlii/the-sony-pictures-entertainment-hack-case-report-195c4681bf72>

LIFARS. (2015, December 15). *Sony Entertainment CEO Shares Simple Cybersecurity Habits following Breach*. LIFARS, a SecurityScorecard Company. https://www.lifars.com/2015/12/sony-entertainment-ceo-shares-simple-cybersecurity-habits-following-breach/

‌Malwarebytes, (2022); What is Cyber Espionage? <https://www.malwarebytes.com/cybersecurity/business/what-is-cyber-espionage>

McAfee, (2022); What is malware and how cybercriminals use it. <https://www.mcafee.com/en-us/antivirus/malware.html>

Microsoft, (2022); What is phishing? <https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44>

MIT. (n.d.). Cybersecurity Leadership for Non-Technical Executives. <https://executive.mit.edu/course/cybersecurity-leadership-for-non-technical-executives/a056g00000URaaBAAT.html>

Mitnick, D. (2014, December 23). *Sony Pictures Hack Shows Weak Security but No Reason to Violate Privacy, Start A War*. Access Now. https://www.accessnow.org/sony-pictures-hack-shows-weak-security-but-no-reason-to-violate-privacy-sta/

‌National Cyber Security Centre, (2022); Mitigating Malware and Ransomware Attacks <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>

Nusca, A. (2017, January 13). *Michael Lynton, Sony Entertainment Chief, to Step Down*. Retrieved from <https://fortune.com/2017/01/13/michael-lynton-sony-entertainment-chief-to-step-down/>

Ogden, S. (2021). Cybersecurity: Creating A Cybersecurity Culture. In *CSUSB ScholarWorks*. Office of Graduate Studies California State University, San Bernardino. https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=2425&context=etd

‌Panda Security. (2015, January 8). *Who are the Guardians of Peace? A new hacker group is on the loose*. Panda Security Mediacenter. https://www.pandasecurity.com/en/mediacenter/news/guardians-peace-new-hacker-group-loose/

Paganini, P. (2015, November 23). *Damballa revealed the secrets behind the Destover malware that infected the Sony Pictures*. Security Affairs. <https://securityaffairs.co/42194/malware/destover-malware-analysis.html>

Page Society. (2014). *Sony Pictures Entertainment, Inc.: A Cybersecurity Attack from North Korea (A) Cyberattack*. <https://page.org/attachments/fa4bc642c80c9c1f39e1f5a6a7e2413906b131fa/store/eadb7324c8431d8d90d4e19b408cffe387e0afc9df0479f1e4994e67bd1a/Sony+Cybersecurity+Attack+(A).pdf>

Pearlson, K. (2023, March 28). *7 Pressing Cybersecurity Questions Boards Need to Ask*. Harvard Business Review. https://hbr.org/2022/03/7-pressing-cybersecurity-questions-boards-need-to-ask

‌Pfeffer, J. (2014, December 12). *3 critical lessons from Sony’s email hack*. Fortune. https://fortune.com/2014/12/12/sony-hack-lessons-leadership-power/

Raza, M. (2020, July 7). *The Chief Information Security Officer (CISO) Role Explained*. BMC Blogs. https://www.bmc.com/blogs/ciso-chief-information-security-officer/

‌Reuters. (2014, December 3). Sony Pictures struggles to recover eight days after cyberattack. *CNBC*. [https://www.cnbc.com/2014/12/03/sony-pictures-struggles-to-recover-eight-daKorea'sKorea's-attack.html](https://www.cnbc.com/2014/12/03/sony-pictures-struggles-to-recover-eight-days-after-cyber-attack.html)

‌Rosencrance, L., & Bacon, M. (2021, June 3). Social Engineering. Security. <https://www.techtarget.com/searchsecurity/definition/social-engineering>

Sanchez, G. (2015). Case Study: Critical Controls that Sony Should Have Implemented. *Global Information Assurance Certification Paper. SANS Institute*. https://www.giac.org/paper/gsec/36744/case-study-critical-controls-sony-implemented/116887

‌SANS Institute. (2023, March 17). SANS Cybersecurity Leadership Curriculum. <https://www.sans.org/blog/sans-cybersecurity-leadership-curriculum/>

Santos, O. (2019). Developing Cybersecurity Programs and Policies, Copyright © 2019 by Pearson Education, Inc.,

Sassi, F. (2023, March 20). *Cybersecurity Incident Response*. Cyber Security & Information Management MGT2151. Algonquin College. Class Lecture.

SecureOps. (2021). *The Hack on Sony Group Pictures Entertainment The Anatomy of One of the Most Devastating Attacks in History*. <https://www.secureops.com/wp-content/uploads/2021/06/Sony-Breach-Analysis-v4.pdf>

Singh, A., & Singh, S. K. (2019, May 19). *Technology Revolution Gives Cybercrime A Boost: Cyber-Attacks And Cyber Security 1*. Proceedings of ARSSS International Conference, Cochin, India.

‌Sjouwerman, S. (2014, December 8). *How Was Sony Pictures Hacked?* Blog.knowbe4.com. https://blog.knowbe4.com/how-was-sony-pictures-hacked

‌Sjouwerman, S. (n.d.). *Lessons Learned From The Sony Pictures Hack*. <https://blog.knowbe4.com/lessons-learned-from-the-sony-pictures-hack>

Sony Corporation. (n.d.). Retrieved March 2023, from <https://www.sony.net/>

Speed, T., & Ellis, J. (2003). *Internet Security: Chapter 10 - Disaster Recovery*. Elsevier.

‌StateRAMP. (2021). *Template: Incident Response Plan*. StateRAMP. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwixqpj-oYT-AhVKjIkEHfJyAYwQFnoECCsQAQ&url=https%3A%2F%2Fstateramp.org%2Fwp-content%2Fuploads%2F2021%2F05%2FSSP\_A\_IRP\_TEM\_202104.docx&usg=AOvVaw2fVxQkLTxnSQPWCbxgTm9x

‌Stengel, R. (2019, October 6). The Untold Story of the Sony Hack: How North Korea’s Battle with Seth Rogen and George Clooney Foreshadowed Russian Election Meddling in 2016. *Vanity Fair*. <https://www.vanityfair.com/news/2019/10/the-untold-story-of-the-sony-hack>

Strom, D. (2018, September 25). *The Sony hacker indictment: 5 lessons for I.T. security*. CSO Online. <https://www.csoonline.com/article/3305144/the-sony-hacker-indictment-5-lessons-for-it-security.html>

Sullivan, C. (2016). The 2014 Sony Hack and the Role of International Law. *Journal of National Security Law & Policy*, *8*(437). <https://jnslp.com/wp-content/uploads/2017/10/The-2014-Sony-Hack-and-the-Role-of-International-Law_2.pdf>

Swanagan, M. (2022, September 22). *How To Plan & Develop An Effective Cyber Security Strategy*. Retrieved from <https://purplesec.us/learn/cyber-security-strategy/>

The Cybersecurity Man. (2018, September 9). *The Sony Pictures Entertainment Hack: A Look at the Evidence We Have*. The Cybersecurity Man. <https://thecybersecurityman.com/2018/09/09/the-sony-pictures-entertainment-hack-a-look-at-the-evidence-we-have/>

Tsukayama, H. (2011, May 4). *Cyber attack was large-scale, Sony says*. Washington Post. <https://www.washingtonpost.com/blogs/faster-forward/post/cyber-attack-was-large-scale-sony-says/2011/05/04/AF78yDpF_blog.html>

Tunggal, A. T. (2023, February 22). How to Perform a Cybersecurity Risk Assessment | UpGuard. <https://www.upguard.com/blog/cyber-security-risk-assessment>

‌U.S. National Security Agency (2018, March). Cybersecurity Information, NSA’S Top Ten Cybersecurity Mitigation Strategies: <https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf>

Weber, J. L. (2022, June 24). *What Is Business Impact Analysis & Why Is It Important?* ProjectManager. <https://www.projectmanager.com/blog/business-impact-analysis>

Westby, J. (2014, December 17). *Instead Of A Real Response, Perennially Hacked Sony Is Acting Like A Spoiled Teenager*. Forbes. https://www.forbes.com/sites/jodywestby/2014/12/17/sony-earns-cyber-troglodyte-award/?sh=3cd2a2293f36

Wowrack. (2022, October 26). *How to Handle Destructive Malware and Protect Your Company | Wowrack*. Wowrack Blog. <https://www.wowrack.com/blog/how-to-handle-destructive-malware/>

‌