Programme Name: **BCS HONS**

Course Code: **CSC 2734**

Course Name: **Information System Security**

Individual Project

Date of Submission: **4/30/2021**

Submitted By:

Student Name**: Dipesh Tha Shrestha**

IUKL ID: **041902900028**

Semester**: Third Semester**

Intake**: September 2019**

Submitted To:

Faculty Name**: Manoj Gautam**

Department**: LMS**

Pearl Innovation is a data warehousing and information processing having headquarter office in Kathmandu PI services are used by large organizations to conduct surveys and data analysis. In most instances, the data collected is highly confidential. Data collected is usually through an online website, but in some instances via paper. PI operates under a four-business day turn-around time meaning they cannot afford downtime, in order to maintain their current business reputation. PI currently employs twelve people, each using a company issued Windows 10 laptop. A year ago, an employee's laptop hard drive crashed, and the data was lost – this incident resulted in the company losing a valuable customer. In recent months, one employee's laptop was targeted with ransomware, and the company paid the ransom as they couldn't afford the downtime. In another breach of security, an office assistant was caught accessing and viewing a confidential data set on another employee's laptop. Last week, one employee left their laptop unattended in their vehicle. The vehicle was broken into, and the laptop was stolen

Report on Cyber Security Issue of Pearl Innovation

Introduction

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security. Cybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems. Without a cybersecurity program, your organization cannot defend itself against data breach campaigns, making it an irresistible target for cybercriminals.

Cybersecurity's importance is on the rise. Fundamentally, our society is more technologically reliant than ever before and there is no sign that this trend will slow. Data leaks that could result in identity theft are now publicly posted on social media accounts. Sensitive information like social security numbers, credit card information and bank account details are now stored in cloud storage services like Dropbox or Google Drive. The fact of the matter is whether you are an individual, small business or large multinational, you rely on computer systems every day. Pair this with the rise in cloud services, poor cloud service security, smartphones and the Internet of Things (IoT) and we have a myriad of cybersecurity threats that didn't exist a few decades ago. We need to understand the difference between cybersecurity and information security, even though the skillsets are becoming more similar.

Context

- **Cybersecurity issues**
- **Main reasons for addressing cyber security issue immediately**
- **Methods to address these issues**
- **Comparison of the chosen solution and alternative solutions**
- **Breakdown of the cost of addressing the security issue**

Cybersecurity issue

Cybersecurity issue is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information. Cyber threats can originate from various actors, including corporate spies, hacktivists, terrorist groups, hostile nation-states, criminal organizations, lone hackers and disgruntled employees. Some of cybersecurity issues and threats that PI organization and their employees may face are given below:

- **Unprecedented Attacks**

Many consumers store their sensitive data or information on a single computer and log into their accounts on multiple computers, compromising their security and privacy. Because the PI organization uses cloud-based services to store data provided by third-party sellers, their privacy is compromised. To improve the security of their computer networks, PI can use advanced communication systems and technologies such as the internet of things and cryptography. To avoid such cyber-attacks, the PI society must train security programmers to use only private cloud-based services rather than public CBS. All of these security issues and threats must be addressed immediately, or PI employees' personal information, such as login IDs, passwords, and bank account information, may be compromised. Data breaches are a very common problem for businesses, and they happen as a result of all of these security threats and risks.

- **Man in the Middle**

A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction. After interrupting the traffic, they can filter and steal data, according to Cisco. MITM attacks often occur when a visitor uses an unsecured public Wi-Fi network. Attackers insert themselves between the visitor and the network, and then use malware to install software and use data maliciously.

- **Malware**

Malware is one of the broadest terms when it comes to cyberattacks. It is any malicious form of software designed to harm a computer system. When malware enters a computer, it performs a malicious function such as stealing, deleting, or encrypting data, monitoring a computer users' activity or hijacks core computing functions. Common malware includes worms, viruses, Trojan horses, and spyware. Malware is designed to steal, encrypt, or delete data, alter or hijack core computer functions, or track a computer user's activity without their knowledge. Malware is commonly distributed through physical hard drives, USB external drives, or internet downloads.

- **Phishing**

Phishing is a common cybersecurity attack that tries to obtain personal information from a person, such as usernames, bank account numbers, credit card numbers, and debit card numbers. It's also known as a fraud attack because it employs a botnet to send spam emails to PI organization websites. When employees click on spam links or emails, hackers are able to identify users' account information and take control of all information using malware software. In the case of PI organizations, third-party applications and software are used to store data or information generated by malicious processes. As a result, computer network performance and efficiency suffer, and users risk losing their personal information.

- **DOS and DDOS attack**

A denial of service attack, also known as a DOS attack, is a serious problem in the field of computer networks. With the help of malware software, hackers generate a large number of traffic signals and unwanted data. Because their employees access unauthorized websites, the PI organization has experienced DOS and DDOS attacks. It has been discovered that the PI community uses wireless networks for communication, but they do not use any security systems, which has resulted in a DOS attack. Hackers use a flooding technique and a complex algorithm to block the servers of the PI organization in a DOS attack.

Main reasons for addressing cyber security issue immediately

- Preventing further loss of valuable information and data: The company's most valuable assets, such as PI id data and information. As a result, if they fail to protect these, they have failed to perform their primary function, which could result in a loss of reputation, financial loss, or other consequences. As a result, security concerns must be addressed.
- Prevent financial loss: One of the most important aspects of cyber security is the prevention of financial loss. Similarly, a financial loss can impede business operations, leading to a loss of customer confidence or even a business contract.
- Preventing a repeat of the same attack: If the vulnerabilities are not identified early on, the company may lose more data. As a result, cyber issues must be addressed as soon as possible to avoid ransomware, SQL attacks, and Dos attacks, among other things.
- Prevent reputational damage: The loss or theft of any type of data or information causes a lack of trust in the institution, resulting in the loss of potential customers and a slowdown in business.
- Avoid legal ramifications of cyber breaches: Failure to implement appropriate security measures may result in fines and regulatory sanctions. This legal process can take a year to complete, and it may be costly to the company in the long run, resulting in financial loss and reputational damage.

Methods to address these issues

One of the primary weapons in their arsenal is malware, or malicious software, what we used to call a computer virus. While email has been the main method for the spread of these recent computer viruses, it is not the only method. Malware can enter a network by USB device, internet download, visiting an infected website, instant messaging or messaging in social media platforms, file transfer and file sharing programs, or by remote users connecting directly to the corporate network with an infected PC.

There are simple steps you can take you increase security and reduce risk of cybersecurity issue:

- **Predictive Analytics**

In order to effectively counter cyberattacks, IT personnel of PI office need to know what an attack looks like, when it's likely to occur, and where it's coming from. Predictive analytics software driven by machine learning can gather huge amounts of data on known cyberattacks and apply the results to existing security protocols. This is especially useful for active DDoS mitigation because it allows cybersecurity systems to identify threats and take proactive measures to redirect traffic before the system is overwhelmed. Rapid response times are critical for avoiding the worst effects of cyberattacks. The longer a breach goes undetected, for instance, the more data will be compromised, which can be costly to companies of all sizes. Predictive analytics can give remote hands teams the advance notice they need to actively combat hacking attempts.

- **Back Up Critical Data**

In the case of DDoS and ransomware attacks, it's essential for companies to have a data back-up plan in place. Having access to mission critical data can mean the difference between getting systems and services back online quickly with minimal downtime and suffering a catastrophic server outage. With a thorough back-up strategy in place that frequently stores vital data and assets in a separate, and preferably off-site system, companies can avoid the "all or nothing" risk of a cyberattack causing prolonged downtime. Data centers can provide extensive back-up solutions reinforced by multiple layers of cybersecurity and physical security. PI should make back up of all important data and information

- **Training and Awareness**

Many data breaches result from phishing scams that introduce malware into network systems. Educating employees regarding the latest tactics used by scammers can help reduce the likelihood that they will click links that expose them to malicious software. Implementing basic data security policies that explain how to properly handle company data is also key to reducing the threat of internal misuse. Organizations should also be stricter about who has access to sensitive data in the first place. These strategies can greatly reduce the impact of human error on cybersecurity measures.

- **Anti-Virus Software**

As one of the oldest methods for combating cyber security issues, anti-virus software should be a no-brainer. PI organization don't install antivirus or neglect to update the software they do have. Start by installing reputable, effective anti-virus software on each laptop and desktop computer of PI organization. When the antivirus program prompts you to download an update, don't just ignore it. Viruses, spyware, and malware evolve very quickly, so antivirus software requires constant updates to stay ahead. Download each update immediately to ensure that you're protected from the latest cyber security threats.

- **Firewalls**

Set up a firewall in PI office in order to protect network and computers from outside attackers. These devices can come in either hardware or software formats, and both can be quite effective in filtering out unnecessary traffic. Firewalls in hardware form can be placed between your computer and your modem in order to prevent malicious code or viruses from getting through. Firewalls in software format can be installed on nearly any operating system and can also effectively block cyber security risks from attacking your computer or network. It protects PI data from being hacked.

- **Installation of security cameras**

Security cameras should be installed throughout the office, along with a sensor-enabled verification and scanning system at each entry and exit point. This allows you to track every employee's movements and see if they've done anything illegal or used any non-company-owned electronic devices.

Comparison of the chosen solution and alternative solutions

A firewall is a hardware and/or software which functions in a networked environment to block unauthorized access while permitting authorized communications. Firewall is a device and/or a software that stands between a local network and the Internet, and filters traffic that might be harmful. An Intrusion Detection System (IDS) is a software or hardware device installed on the network (NIDS) or host (HIDS) to detect and report intrusion attempts to the network. We can think a firewall as security personnel at the gate and an IDS device is a security camera after the gate. A firewall can block connection, while an Intrusion Detection System (IDS) cannot block connection. Though they both relate to network security, an intrusion detection system (IDS) differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An Intrusion Detection System (IDS) alert any intrusion attempts to the security administrator. However, an Intrusion Detection and Prevention System (IDPS) can block connections if it finds the connections is an intrusion attempt.
A firewall is a hardware and software-based security system designed to protect and monitor both a private internet network and a computer system. While antivirus is a software program that detects and eliminates any threats that will destroy a computer system. Firewalls help control network traffic in the system by acting as barriers for incoming traffic, whereas antiviruses protect systems against internal attacks by perceiving or spotting malicious files and viruses. Antivirus and firewall are part of the Cyber Security which safeguard systems.

- **Breakdown of the cost of addressing the security issue**

To reduce the issues and threats of cyber security the PI organization can adopt security programmed and steps. The cost of using the network security systems the PI community requires around 10 lakhs in and its Cost breakdown in addressing the selected issues is given below:

S.N	Terms	Costs(proposed cost per year)
1.	E-Mail protections service	12000(<500 employer)
2.	Anti-virus software	8000+8000(20 device)
3.	Two- factor authentication service	24000(20 Person)
4.	Training program	100000
5.	Private enterprise WIFI service charge	100000
6.	Google Suite	14000
7.	MS-Office Suite	15000
8.	CCTV	300000(10000 per piece)
9.	Finger print door	32000
10.	External Firewalls	200000(3 years)
11.	Others	190000-230000

Thank You