**INITIAL POST**

Cyber security has a multitude of footprints in almost every aspect of modern technology as well as existential scientific, commercial and communal problems. The increasing number and dependence of people, businesses, companies and governments on computer systems mean a growing number of systems are at risk. Large companies have traditionally been a priority. In certain cases, cyberattacks aim to gain financial advantage through identity fraud and relies on data breaches.

Cyber security refers to the term which undertakes its responsibility to ensure safety in terms of software, systems as well as several technical bases. To protect from any unwanted threats namely data breaches, ransomware, or crypto-jacking malware, corporate sectors and commercial organizations should invest in Cyber defense to confirm buyer's safety, reliability, and trust. Otherwise, the corporate world will be facing large-scale malicious attacks and dissatisfaction from clients. Following its safety and security measures, all public, private and high-level properties should constantly implement their cyber security function, fundamental structure, and anti-malware process.

In today's world, the theft of payment card detail is no longer an unusual issue. Despite learning a lesson from the infringement of the Target data, the Russian/Ukrainian hacking ring referred to as "Rescator" broke into computers from Target company in the year of 2013 and 2014. Unlike other inconvenient sources of online transactions, Rescator was a quiet easily accessible sector in terms of virtual shopping which needs some general procedure to access any UK banks. As of April 2013, Michael Winter's (September 5, 2014) stated that approximately 56 million payment cards (debit and credit), including 53 million e-mail addresses were stolen from Home Depot computers.

Fortunately, one of them was detected among thousands of British customers. The conversation between the characters Geoff White and Joanne Smith reveals her endangered unawareness of the card. (Thousands at risk from credit card fraud website, 2014, 2.16-2.30). Channel4, 2014 reveals that buyers are provided individual's name, number as well as the expiry date; yet it is not required to provide the three-digit CVV of the transaction cards and so does Amazon. Further, Channel4, 2014 affirmed that instead of requesting the buyer's CVV number, Amazon conveys packages to one of its organizations of the warehouse. Furthermore, it results in the less necessity of cardholder's location while the card scammers are likely to attempt. Admittedly, the heists could have easily been stopped by the existing antivirus software if the company administrators would have responded immediately to the warnings of payment cards.

Reference list:

Thousands at risk from credit card fraud website. (2014) Channel4 6 Nov. [online] Available at: [Accessed 28 January 2021].

Michael, W. (September 5, 2014) Home Depot hackers used vendor log-on to steal data, e-mails. USA TODAY. [Accessed 29 January 2021].

**Peer Response 1-Charlotte**

Charlotte,

Samuel (2018) agrees that this is not the first time while Yahoo was attacked by Cyber theft. Admittedly, Yahoo also was victimized by a massive infringement of 1 billion accounts in 2013, yet it was discovered in 2016 after the 2014 hack’s announcement. Regardless, one of the most devastating data breaches which were occurred by a number of cyber criminals in Yahoo, and is no longer to be astonished about the prime reason of it was the negligence of investing in Cyber protection. No longer to say, they were terribly fined, in contrast, lost their reputation which is likely crucial to regain trust.

Global companies are under threat by the heist in terms of personal details, for instance, payment card number, name, address, contact numbers even transaction detail of the clients. As a result, the social portal named Yahoo was victimized due to their carelessness and delaying the process to maintain their security sector and ensure safeguard to every user of that online communicating tool.

Andrew (2016) states that ‘The company has announced that at least 500 million accounts have been stolen in what might be the biggest data breach ever.’ This clarifies that almost a massive number of Yahoo users had experienced the leakage of their personal information. Such an attack probably would never have happened if they would have prevented it earlier by investing and strengthening their cyber security consultants, expert technicians, and professional penetration testers.

References:

Andrew, G. (September 23, 2016) YAHOO HACK: HUNDREDS OF MILLIONS OF PEOPLE PROBABLY DON’T KNOW THEY ARE PART OF THE WORLD’S BIGGEST DATA BREACH. The Independent. Available from: https://www.independent.co.uk/life-style/gadgets-and-tech/news/yahoo-hack-flickr-account-how-know-what-do-have-i-been-hacked-data-breach-a7324701.html [Accessed 01 January 2021]

Samuel, G (June 12, 2018) Yahoo fined £250,000 for hack that impacted 515,000 UK accounts. The Guardian. Available from: https://www.theguardian.com/technology/2018/jun/12/yahoo-fined-hack-ico-uk-accounts-russia [Accessed 03 January 2021]

**Peer Response 2-Anum**

Dear Anum,

I certainly admire your points regarding Canva- one of the largest international graphics company and exploring two of the possible reasons behind it. An Australian organization named Canva which was secured enough to protect their client details, unfortunately, compromised a huge vulnerable cyber threat in 2019 owing to their password breakage.

There are millions of websites/ companies where the necessity of building up a brand-new password has become reduced or stopped, likewise, it was accessible to log into the client’s account in Canva based on Google login details with its mutual connection. Therefore, in May 2019 they experienced an enormous attack by the group hackers Gnosticplayers, which included 139 million users including their real name, personal contact, current/permanent address, email address, and many more (Guta, 2019).

Majority of those accident occurs without even providing an alarm to the companies. As a result, they should constantly be in check of their files, documents to keep them up to date or even securely maintaining passwords connected to third-party authentication. According to Guta (2019), it is better, as well as more secured to change the password by the password manager tool because the more complex and impenetrable the password, is, the more inflexible and harder to crack it by the thieves. Unfortunately, still, cyber hackers can take attempt to steal any company’s valuable data.

References:

Guta, M., 2019. Canva Hacked! Remember to Change Passwords Regularly. [online] Smallbiztrends.com. Available at: [Accessed 7 February 2021].

**Peer Response 3- Panagiotis**

In today's digital world, Cyber Security is a major key factor of the daily operation of organizations in terms of healthcare sectors. Unfortunately, hospitals and Medicare organizations are the second significant target of the black market and this leads to hacking various sources such as electronic prescription systems, assistance systems for functional administration, information of (radiology, pathology, gynecology) and so on. High- profile patient of a certain hospital can be exemplified here. Since hackers are primarily keen to attack financial documents, any celebrity might be in danger from money laundering which can be happened simply just punching the credit card to pay his hospital bill and the hacker can compromise his card detail later on.

Phishing is one of the most common ways of attacking any IoT devices or email, websites, research sector of any department of the hospital. Consequently, hundreds of user data have been hacked and 10 million people experienced an information breach by a ransomware attack at Blackbaud Inc. early last year that offers cloud services for hospitals, colleges, and other organizations (Rundle, 2021). It is also noticeable that a large number of data breaches are occurring due to covid-19 pandemic owing to the majority of the institutions are dependant online, yet the security protocol in the cyber world is not sufficient or neglected.

Several critical measures might be applicable to ensure safety such as employee awareness to shut down the devices every time they are using as well to log in either. Employees are not acquainted with the system maintenance, hence proper education and training might be effective. Another prime issue is developing backup files of all private documents which are necessary to recover if an unwanted attack happens. Moreover, changing passwords after a certain time, using two-factor authentication, highly inaccessible passwords, installing/uninstalling documents can be beneficial measures to control any sudden attack.

References:

Rundle, J., 2021. Hospitals Suffer New Wave of Hacking Attempts. THE WALL STREET JOURNAL, [online] Available at: [Accessed 10 February 2021].

**Peer Response-4 -Josef**

Dear Josef,

I undoubtedly agree with your points regarding the world-leading company “Sony” that you mentioned. It is quite surprising how they were victimized by the hackers in 2014 and after all landed on their feet. Admittedly, they lost terabytes of data along with thousands of private documents, confidential records, video clips which were original, but the reason behind was something irrational. North Korea was the source of this crime whereas they already threatened Sony to stop or remove those clips where their president Kim was shown being killed as the prime reason for their doubt was praising intentional terror activities. That devastating leakage of these data not only left Sony in a long-term awful experience but also proves the urgency of investment in the sector of cyber network as well as wider in order to protect any sort of accidental heist.

(VanDerWerff and B.Lee, 2015) states that it was November 2014 when the employees of Sony initially went through the experience of their hacked corporate network and the terrifying notes of warning signs by the hacker to reverse the situation. One of the big reasons for these cyber attempts is the interconnected world and the easy access, low- priced way to hack whereas it is much more inconvenient to attack through military weapons or other terms of destruction, hence, it is easier for the cyber criminals to destroy a company by breaking down of their network, than of its cyber technicians (VanDerWerff and B.Lee, 2015).

References:

VanDerWerff, E. and B.Lee, T., (2015). The 2014 Sony hacks, explained. [online] Vox. Available at: [Accessed 7 February 2021].

**Peer Response-5-Till**

Whether it is piracy, extortion or even cyber assault, nations are constantly in danger and facing nonstop threats to their networking sites. Consequently, policymakers tend to adopt cybersecurity necessary and emergency measures in order to tackle ever-growing cybercrime. Unfortunately, cybercrime is taking place in almost all sectors of a nation from the corporate level to federal institutions and confront large-scale infringements of security, privacy and cyber assault. Therefore, Governments are taking urgent steps to prevent these attacks and responding with regulatory intervention to provide security and safety especially to the companies, banking sources, governmental institutions, and sensitive origins of national documents.

Till, I certainly admire the points that you have mentioned in terms of the cybersecurity strategies of European and U.K commissions which has given a proper dimension to protect all levels of data confidentiality, but there is another prime clue which had been arisen, where (Hallenback, 2020) argues that Cybersecurities regulation must provide ways to enhance IT hygiene and visibility. Which means, providing the fundamental hygiene of data and making sure there are no gaps to clear up. It is also assumed that security not only depends on the expansion of unnecessary extra security tools but also to target exactly the doubtful movements and preparing cautions to protect it prior it happens (Hallenback, 2020). Therefore, strong protection relies on these activities along with others such as two-factor authentication, employee seriousness, and investing in safeguard protections.

References:

Hallenback, C., 2020. What New Cybersecurity Legislation Doesn't Include. [Blog] Security Boulevard, Available at: https://securityboulevard.com/2020/06/what-new-cybersecurity-legislation-doesnt-include/ [Accessed 14 February 2021].

**Peer Response-6—Michael**

Unlike other general attackers, Cybercrime is not an ordinary term where it is mostly observed in the small sector, the majority of the victim organisations are likely to seem like the most leading global companies such as Yahoo, Netflix, Facebook, Target, eBay and many more. The reason is simply because of their huge data with massive profit either financially, socially, or personally. The ways of data breaches are increasing gradually, especially in the period of Covid-19 due to staying/working or purchasing from home, thus it reflects the double security demands simultaneously.

I surely agree with all the principal issues which have been discussed by Michael and Czeska, and adding up an option namely fundamental risk management where (The fundamentals of risk, 2021) states that risk management can opt for supporting responsible, ethically building up plans for the near future and to understand what precisely right or wrong in a company whereas NCSC explores risk assessment works on assessing, explaining, potential implications in a comprehensible manner to enhance decision-making. Additionally, any unexpected concern should technically and professionally be handled and prepared for a brand-new breach, hence, there is no possibility to notice the same attack repeatedly and technicians are required to concern almost round the year.

References:

Ncsc.gov.uk. 2021. The fundamentals of risk. [online] Available at: https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/fundamentals [Accessed 15 February 2021].

**Peer Response7- Lulia**

To precise, Cyber data breach can be reduced even stopped with the workforce of the organisation or a company. It is currently observed that the majority of the data breaches are occurring in the larger companies and the employees rarely had taken any initiative decisions on the spot. Therefore, the less knowledgeability and underrated training overweigh their negligence in this case. Employees are required to perform as per their prior oriented infrastructure, develop their fundamental and technical capabilities for any emergency condition, and establish all the backup storages to replace them in case of any urgency.

Importantly, it stands in need of establishing the practice of security, for instance, securely browsing of email, website, social media, bank transaction detail and remind the employees in the period when they are using other business devices to be vigilant and questionable connections and certainly changing all the official passwords weekly/monthly basis. Subsequently, Red flag for the warning is effective, yet, it is emphasized to not deter workers for even though it is a bogus warning, contrarily, strengthen the planning strategy if false alerts arise frequently (Esposito, 2017). It is also suggested to practice a culture of Cryptoransomware owing to in the past year, is it observed the big cruel assaults, including in hospitals and major telecommunications firms as well as had major malware outbreaks of WannaCry (Esposito, 2017).

References:

Esposito, J., 2017. Tips to educate your staff on cybersecurity. [online] Kaspersky.com. Available at: [Accessed 13 February 2021].

**Peer Response-8-Craig**

Appreciating the points which have been arisen by Craige and Dinko in terms of IoT (Internet of things) and its significant impacts on very sectors of globalization and home gadgets. For instance- a multifunctional device can lead to effects negatively as well as risky to the entire house. Should Cyber security be implemented parallelly in each appliance of a certain house/commercial zone to eradicate the high vulnerabilities of security break down. The greater number of devices based on Artificial Intelligence, the higher risk to face data breaches, especially the business and mechanical inventors have no alternative option available to barricade their products. Certainly, these are expanding more risks due to insufficiency of security management, high-skilled professionals, and low-investment in cyber defense. Therefore, Iot might act as a shared ecosystem externally, whereas internally its multi-layered with its high level of protection to decline any malware, phishing or any further threats.

The motive of hack can vary from hacker to hacker and are being happened in several governmental organization, educational institution, private belonging namely cell phone, smartwatch, tv, four-wheelers. To illustrate, the young generation is likely to involve with hacking mass people’s credit card and the motive of these are nothing other than passion, contrarily, any government offices are being stolen to gain the confidential information about politics or religion of a certain country (Abomhara and Koien, 2015). This dangerous issue should be in account by the higher authorities of every corporation and the state administrators.

References:

Abomhara, M. and Koien, G., 2015. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility, [online] 4(1), pp.3.1. Available at: [Accessed 9 February 2021].

**Summery Post:**

Points outline leading perception and different observations from the early debates

Reputational Risk

Based on data-filled apps, businesses of all sizes need to be ready to defend against that will come on upcoming period to build a new economic operation that worth $13 trillion by 2030 (Gibbons, 2020). This means it is obvious, either to invest in security protocol to save the trust, reputation, and continuity of a company, or experience the bitter truth of cyber threats. I unquestionably concur with the mentioned perspective of Charlotte where it assumes that many privacy infringements inflict not only harm for the financial undertaking, but also a controversial image of that company which may or may not be resolved in a longer period (Wilson,2021).

Encrypted Protocol

It is being observed globally and was clarified by Anum about the fact of expansion of e-commerce business due to Covid-19 pandemic and resulted in increased online retail fraud, with more customers going into the usage of e-commerce sites leading to the shopping sites being closed (Rashid,2021). Furthermore, another point was well taken by Navaratnasingam about the payment card details and its unsecured way of transactions without CVV number (Arunanthy2021). Therefore, it is suggested not to store and save the purchaser details, there should be no middle man while sending/receiving the data and any entity that handles credit card transactions must meet PCI-DSS security criteria, regardless of sales or credit card volumes, in respect of cardholder records which are specified by the PCI Security Standards Council (PCI SSC) and adopted by credit card companies (Phillips, n.d.).

Human Factor

One of the most critical and major issues that have been discussed by Joseph is human negligence in Cyber Security which has led to data infringement, either consciously or indirectly, through incompetence and inability to act from time to time (Olaseni, 2021). It should be seen as necessary for all companies regardless of their scale and complexity to be able to develop good cyber safety behavior, yet, this is not the case from responses to the scale, because the pockets of people tend to be disengaged or unfit for adequate intervention (Hadlington, 2017).

To reiterate, the larger the company or institution, the massive the attacks are occurring nowadays. Certainly, the targets of breaches are the enriched global companies in terms of their private details, financial transaction, governmental confidentiality. Every aspect of our life is becoming machine-based and advance with the blessing of technology and innovation, thus cyber-crime has become its parallel obstacle whereas the solution relies on Cyberdefense by investing simultaneously securing with its high-skilled technicians.

References:

Gibbons, S., 2020. Why Investing In Cybersecurity Makes Sense Right Now. Forbes, [online] Available at: [Accessed 10 February 2021]

Wilson, C. (2021) Initial Post by Samiya Nova, 02 February Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=240199#p856883

Rashid, A. (2021) Initial Post by Samiya Nova, 05 February Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=240199#p856883

Olaseni, J. (2021) Initial Post by Samiya Nova, 06 February Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=240199#p856883

Arunanthy, N. (2021) Initial Post by Samiya Nova, 07 February Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=240199#p856883

Phillips, S., n.d. What You Need to Know About Securing Your Ecommerce Site Against Cyber Threats. [Blog] BigCommerce Blog, Available at: [Accessed 12 February 2021].

Hadlington, L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, [online] 3(7), p.11. Available at: [Accessed 13 February 2021].