CYBERSECURITY

THE HUMAN COST OF CYBER ATTACKS: STORIES FROM THE FRONTLINES

In the world of cybersecurity, the focus often rests on statistics and technical details, highlighting the latest breaches and vulnerabilities. However, behind these headlines often lie the stories of overlooked victims of cyberterrorism. The impact of cyber-attacks extends far beyond financial losses and data theft, delving into the loss of trust, invasion of privacy, and an unsettling feeling of being watched. For those on the frontline – cybersecurity professionals, employees, and individual users – this is a daily reality. They are the initial defense against cyber threats, relying on technology to fulfil their roles. When their systems or data are compromised, it not only disrupts vital services but can also pose risks to lives. This article will delve into their experiences, revealing the loss of trust and determination amidst the evolving landscape of cybersecurity.

DEFINITION OF CYBER ATTACK

According to Cisco, a cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network. In fact, cyber attackers frequently focus on industries such as healthcare, government, non-profit organizations, and finance companies, etc. Additionally, cyberattacks are not always driven by financial motives; some aim to destroy or obtain access to crucial data.

IMPACT OF DATA BREACHES AT LARGE SCALE

Large-scale data breaches not only affect the targeted companies, institutions, and organizations but also have repercussions for individuals on a personal level. Even if individuals are not directly targeted, they can suffer collateral damage if the organizations they trust with their personal information fall victim to breaches. The consequences can be severe and long-lasting, including financial losses, reputational damage, legal action, loss of stakeholder trust, decline in business, and challenges in attracting talent. Below, we will examine some of these negative impacts as following:

- **Temporary Shut Down:** For companies, the detrimental effects of data breaches extend far beyond the instantaneous financial burdens, as they also contend with the

persistent long-term fallout.

- **Financial loss:** According to industry surveys, Gartner concludes that the cost of operational downtime can be around $5,600 per minute and can quickly accumulate to $300,000 per hour if breaches are not promptly resolved.
- **Reputational Damage:** This is a major concern for companies that experience large-scale data breaches. Such damage can lead to revenue loss and have long-term impacts on the company. When a company's reputation is tarnished due to a history of data breaches, people are less likely to trust the company with their payment information, and they may choose to take their business elsewhere.
- **Loss of Private Data:** According to Selfkey website, hackers usually target sensitive data and intellectual property in a cyber attack. Sensitive data, such as personal information of customers, patients, and employees, as well as private company emails containing health

history, addresses, and payment details etc. Whereas for intellectual property, hackers target such as designs, strategies, and blueprints, which, when stolen, can give competitors an advantage and harm a company's competitive edge. Industries like manufacturing and construction are especially vulnerable to these cyber threats.

Two notable real-life events have been illustrated on the effects of cyber-attack that occurred in the Sony Pictures and JP Morgan case. Both cases underscore the profound impact cybercrime can have on both businesses and individuals, highlighting the urgent need for robust cybersecurity measures and vigilance in the digital age.

1. THE SONY CASE

In November 2014, Sony Pictures reported an external breach has occurred in which the leaking of confidential data included over 30,000 internal documents, 170,000 emails, social security numbers of Sony employees, personnel reviews, unreleased movies, and more.

The cyber-attack disrupted all of Sony's systems, making the online stock footage database unsearchable, the telephone system non-functional, and rendering computers and servers unusable. The FBI described this attack as an "unprecedented digital assault" that would have severely impacted 90% of companies. In response, Sony had to replace many of its systems, establish an identity fraud hotline, provide psychological counseling for employees, and conduct seminars on data security.

Consequence of the attack, Sony employees received threatening emails regarding their families, their credit card information was sold on Dark Net

markets, and some experienced their bank accounts surpassing credit limits. A survey by the Identity Theft Resource Center revealed that victims of identity theft experienced a range of emotions including denial, frustration, rage, fear, betrayal,and powerlessness. Class-action lawsuits were filed by employees, either due to Sony's failure to notify those affected by the breach or concerns about the potential misuse of leaked personal information. This also led to the departure of key staff members, and the press uncovered Sony's diversity issues extensively discussed in the leaked emails.

2. THE JP MORGAN CHASE CASE

JP Morgan Chase, a leading bank in the United States, reported that the malicious actor obtained administrator privileges to multiple servers. This breach led to the theft of details such as names, phone numbers, emails, and physical addresses of 76 million households and seven million small businesses. Just prior to the attack, JP Morgan had announced an increase of $250 million per year in their cybersecurity budget.

Following the breach, the bank had to overhaul most of its IT systems, a process that was both time-intensive and disruptive to daily operations. Additionally, more than 1000 new employees were hired to monitor the company's systems. The aftermath of the hack brought about two significant long-term effects. Many affected customers had to closely monitor their finances due to fear of fraud, often falling prey to fake emails directing them to fraudulent websites. The second major consequence was the replacement of the chief information security officer due to perceived inadequate cooperation with federal authorities during the investigation, which aimed to contain the breach and minimize the leaked information.

IMPACT OF DATA BREACHES AT PERSONAL LEVEL

Personal level data breaches often stem from carelessness in the digital realm and inadequate security practices. Individuals may inadvertently disclose sensitive information on unsecured websites or become targets of phishing scams, leading to the compromise of login credentials. Weak passwords and neglecting software updates can also expose personal devices to hacking. Some of the negative impacts circulating around personal level are the following:

1. **Identity Theft:** Identity theft is a severe crime with devastating consequences for victims. When criminals obtain personally identifiable information like names, Social Security numbers, and birthdays, hackers can cause chaos on their financial and personal lives. Victims may have bank accounts drained, credit histories damaged, and possessions stolen. Some notable examples of identity theft

including:

- In 22th June 2022, Kosmo reported, a carpenter at a furniture factory in Seberang Perai named Ang Siang Ping, 27, is now living in distress after claiming that his identity was stolen and misused by unknown parties for the past five years. The victim is said to have caused financial loss to a homeowner in the area, who had to bear a high electricity bill

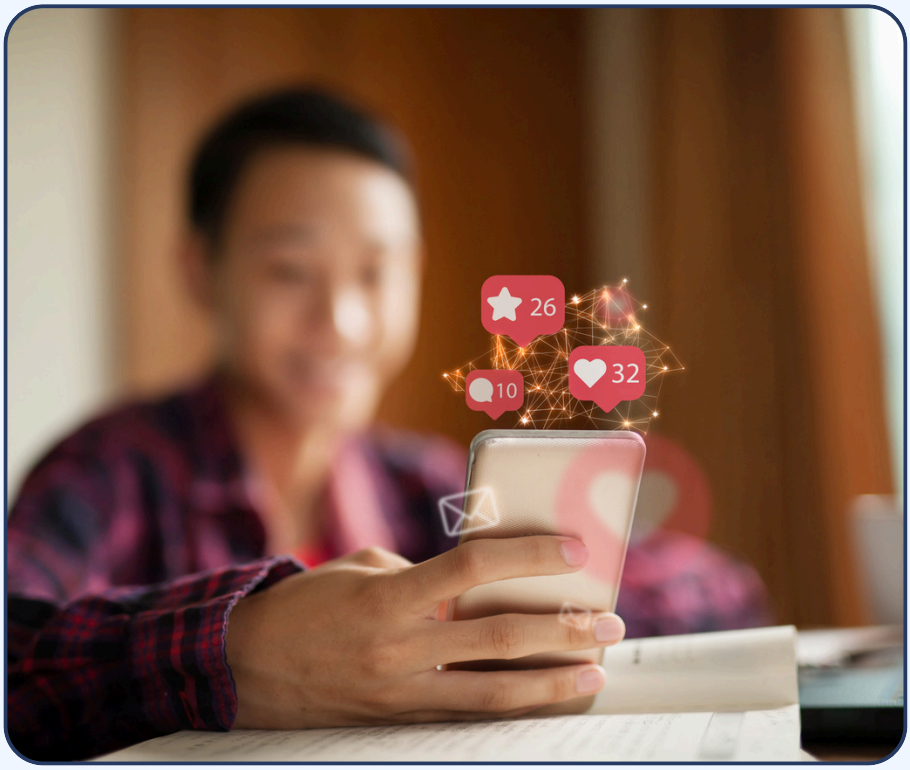
- In October 2020, the largest criminal case of cyberattack in Finland was the case of Vastaamo, a Finnish psychotherapy service provider, reporting a data breach where their patient database was hacked. Extortionists demanded 40 bitcoins (around 450,000 euros) from Vastaamo to avoid publishing patient records. When this failed, they targeted clients directly, threatening to publish their sensitive data unless ransoms were paid. Roughly 30,000 victims received these ransom demands.

amounting to RM230,611.30 throughout that period until last March. He also received a civil court summons from Tenaga Nasional Berhad (TNB) for a bitcoin mining activity in Butterworth, amounting to RM234,747.50 around November last year. He suspects that his identity was stolen and misused, possibly due to the loss of his identification card, other documents, and cash in an incident back in 2017.

3. Financial loss: Once malicious actors acquire your personally identifiable information (PII), they can potentially use it to harm your credit rating and engage in financial fraud. A diminished credit score can create obstacles for the victim to obtain personal loans, secure mortgages and affect job opportunities. Moreover, individuals perpetrating identity fraud can open new bank accounts in your name, deplete your existing accounts, and commit check fraud. For example:

- On 23rd April 2022, a man named Md Nor Izzudin Hamzah, posted on Facebook that he had fallen for the MyMaidKL scam after seeing a Facebook ad offering a Hari Raya Promotion for cleaning services. Upon chatting with the scammer, victims were directed to book through an Android app. Through the app, victims made payments on a fake online system, unknowingly sending their banking details to the attacker. As a result,

2. Personal Health Information: According to the Aura website, the theft of personal health information (PHI) holds significant value on the Dark Web as much as $1000, often surpassing the worth of stolen credit card details by more than 200 times. This carries severe consequences, such as hackers are able to sell stolen PHI to other criminals, who can use it for various illicit purposes. For example:



- On 25th December 2022, Kosmo reported there was a viral on social media of an anonymous parent revealing their children's Telegram which was contacted by an individual impersonating to be a doctor, allegely representing their school teachers for health examinations. The individual contacting these students is suspected to have hacked into another Telegram account to mask their true identity and requested the child to share pictures of their private parts for the purpose of health examinations.

5. Emotional and Mental Health impact: A personal data breach can have a profound emotional and mental impact on victims, with recovery often taking a long time depending on the severity of the attack. Apart from reputational harm, victims may face extensive efforts and costs to mitigate the fallout. Such as victims may spend hours dealing with banks, replacing stolen documents, addressing criminal charges in their name, and etc. Failing to repair compromised information can also leave victims vulnerable to repeated attacks. The long-term consequences, especially if the PII or PHI of the victim end up on the Dark Web. The information could be in circulation there indefinitely, making them the attackers conducted illegal transactions totaling over RM 18,000.

4. **Impersonation on Social Media:** Cybercriminals can exploit your digital identity for harmful activities, such as phishing for credentials from contacts, damaging your reputation with inappropriate online posts, and extorting you with sensitive photos or videos, causing emotional and financial harm.

vulnerable to further harm.

COMBATING HUMAN COST

Organizations can significantly enhance their cybersecurity posture by implementing a well-defined Information Security Management System (ISMS) and Business Continuity Management System (BCMS). An ISMS provides a systematic approach to managing information security risks, ensuring data confidentiality, integrity, and availability. A BCMS establishes a framework for recovering from disruptive events, minimizing downtime and ensuring critical business functions continue even during a cyberattack.

Furthermore, by conducting regular security assessments, be it of the organization's processes, technology, or focusing on information security awareness training for employees, plays a vital role. Periodical assessments identify vulnerabilities and gaps in security, allowing for proactive measures to be taken. Security awareness training empowers employees to recognize and avoid cyber threats, forming a human firewall against social engineering and phishing attacks.

By adopting a comprehensive approach that integrates technical safeguards, human-centric strategies, and continuous improvement, organizations can significantly bolster their defenses and build a more secure digital environment for everyone.

CONCLUSION

Cyber attacks are not just about numbers and statistics. The effects they bring on individuals and businesses can be devastating. When personal information is compromised, individuals face a myriad of challenges, from the fear of identity theft to the emotional distress of privacy invasion.

For businesses, the repercussions can be equally severe, often resulting in significant financial setbacks, damage to reputation, and loss of customer trust. They have a significant human cost, impacting individuals and communities in profound ways. Recognizing this human dimension is crucial for building a more secure and resilient digital future. By prioritizing both technical solutions and human well-being, we can work towards minimizing the devastating impact of cyber attacks on our lives.

AUTHORS

- HASNIDA BINTI ZAINUDDIN
- IKMAL HALIM BIN JAHAYA
- AMIROUL FARHAN BIN ROSLAINI
- ALIYA FARHANA BINTI MOHD NASRAN

REFERENCES

- Australian Institute of Criminology. (2023). Cybercrime in Australia 2021. https://www.aic.gov.au/subject/cybercrime
- The Global Cyber Alliance. (2023). Bystander Effect: The Human Cost of Cybercrime.
- National Center for PTSD. (2023). Understanding PTSD. [https://www.ptsd.va.gov/understand/related/index.asp]
- Cyberattacks & Data Breaches recent news. (n.d.). Dark Reading. http://www.darkreading.com/attacks-and-breaches/sony-data-breach-cleanup-to-cost-/$171-million/d/d-id/1097898
- Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. M. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1). https://doi.org/10.1093/cybsec/tyy006
- CrowdStrike. (n.d.). Most Common Types of Cyber Attacks. Retrieved from https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/
- Coursera. (n.d.). Types of Cyber Attacks. Retrieved from https://www.coursera.org/articles/types-of-cyber-attacks
- Cisco. (n.d.). Common Cyber Attacks. Retrieved from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
- Hern, A. (2023, April 4). TikTok fined in UK for data protection law breaches. The Guardian. https://www.theguardian.com/technology/2023/apr/04/tiktok-fined-uk-data-protection-law-breaches
- Cimpanu, C. (n.d.). KFC, Pizza Hut owner discloses data breach after ransomware attack. BleepingComputer. https://www.bleepingcomputer.com/news/security/kfc-pizza-hut-owner-discloses-data-breach-after-ransomware-attack/
- Atlassian. (n.d.). Cost of Downtime: How Much Does Downtime Cost Your Business? Retrieved from https://www.atlassian.com/incident-management/kpis/cost-of-downtime#:~:text=The%20average%20cost%20of%20downtime%20is%20%245%2C600%20per%20minute%2C%20according,company%20size%20and%20industry%20vertical
- Office of Justice Programs. (n.d.). Identity Theft. Retrieved from https://www.ojp.gov/sites/g/files/xyckuh241/files/archives/factsheets/ojpfs_idtheft.html#:~:text=Identity%20theft%20has%20profound%20consequences,crimes%20they%20did%20not%20commit.
- Albrecht, S. (2018, November 1). Understanding the Scope of Identity Theft. Fraud Magazine. https://www.fraud-magazine.com/article.aspx?id=4294978560
- SelfKey. (n.d.). Data Breaches: Risks and Consequences. Retrieved from https://selfkey.org/data-breaches-risks-and-consequences/
- Aura. (n.d.). The Dangers of Identity Theft: 12 Things You Should Know. Retrieved from https://www.aura.com/learn/dangers-of-identity-theft#12.-Your-personal-data-could-circle-on-the-Dark-Web-forever

REFERENCES (CONT.)

- CBS News. (n.d.). Protect against medical ID theft. Retrieved from https://www.cbsnews.com/news/protect-against-medical-id-theft/
- Reuters. (2020, October 26). Tens of thousands' psychotherapy records hacked in Finland. The Guardian. https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland
- Oxford Treatment Center. (n.d.). Stress and Substance Abuse. Retrieved from https://oxfordtreatment.com/substance-abuse/co-occurring-disorders/stress/
- National Sleep Foundation. (n.d.). Stress and Insomnia. Retrieved from https://www.sleepfoundation.org/insomnia/stress-and-insomnia
- Painted Brain. (n.d.). The Psychological Impact on the Lives of Cyber Attack Victims. Retrieved from https://paintedbrain.org/blog/the-psychological-impact-on-the-lives-of-cyber-attack-victims
- Kosmo. (2022, December 25). Menyamar jadi doktor, minta gambar tak senonoh. https://www.kosmo.com.my/2022/12/25/menyamar-jadi-doktor-minta-gambar-tak-senonoh/