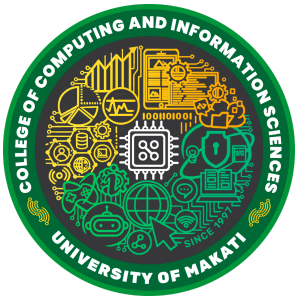

University of Makati

J.P. Rizal Ext., West Rembo, Makati City
College of Computing & Information Sciences

Data Breach and Cyber Security

Claire Jane Dela Cruz

Hans Dominic Arcilla

Carl Angelo Jamero

Aaron Paul Balleta

Edmhar Mauhay Olarte

CCIS COMPUTER SCIENCE

PROFESSOR Niño Narido

PROFESSOR Mary Ellaine Cervantes

Sep 19, 2023

DATA BREACH & CYBERSECURITY

TABLE OF CONTENTS

I. INTRODUCTION

A data breach is the intentional or inadvertent exposure of confidential information to unauthorized parties. In this era we live in today, data has become one of the most critical pieces of information of an organization or individual in any state of the world. Data leakage poses serious threats to all of us, including significant reputational damage and financial losses. The large increase of users on the internet has given rise to frequent cyber attacks, specifically data breach. Cyber security ensures the protection of information systems including software and hardware and information (data).

Since the first Cyber attack in 1988 by the Morris Worm, many cyber attacks have been created, attempting to infiltrate, steal and destroy data from other computer systems while being unauthorized, which is why cyber security is implemented to protect private data especially in the age of internet where our lives are increasingly dependent on online shopping, banking, and socializing. Data breaches pose a great threat to users all around the world, every second of every hour, hundreds of companies, businesses, and individuals suffer from data breaches. Cybersecurity methods have become more complex and advanced than they were years ago, and various tactics have been implemented to combat the dangers of data breaches. Some notable instances of data breaches are Sony's PlayStation Network data breach in 2011, American store chain Target in 2013, and Microsoft and Facebook also suffering from data breaches in 2021.

According to *Trend Micro*, a data breach is an incident involving stolen data from unaware users and system owners, including credit card data, user data, confidential documents, and the likes. In order to combat this threat, different measures of security have been implemented to keep users safe, such as log-in methods like two-factor

authentication, fingerprint detection, OTPs or one-time passcodes, and etc. According to *Kaspersky*, cybersecurity is the practice of protecting computer systems from malicious attacks. Cybersecurity is very critical in today's interconnected digital world, as cyber attacks and threats continue to evolve and become more sophisticated. According to *RiskBased Security*, a number of 7.9 billion records have been exposed by data breaches in the first nine months of the year 2019, which is double the number of exposed records in the first nine months of 2018, with medical facilities, public entities, and retailers experiencing the highest amount of data breaches, targeted for their medical and financial data. To combat users all over the world from this danger, various security methods have been implemented, such as two-factor authentication, fingerprint detection, facial recognition, and the likes. There have been improvements in anti-virus systems as well to prevent data loss from cyber attacks, like trojan virus detections, DDoS (Distributed Denial of Service) preventions and scam website protection. In this paper, we will discuss data breaches and its effects, and how cybersecurity works to circumvent this type of attacks from users worldwide.

II. MAIN

Data Breaches and Cyber Security go hand in hand or in other words they are both closely connected in the world of information technology and digital security. Data breaches are incidents that highlight vulnerabilities in an organization’s integrity in which Cyber Security comes in. Cyber security measures multiple lines of defense that prevent, detect, respond to, and recover from possible data breaches, ultimately ensuring the protection of large companies, individuals, governments, and states sensitive data.

How does Data Breach happen?

Everyone is vulnerable to data breaches, not only megacorporations housing millions of data under their servers but also everyday users like us can be victims to this type of cyber attack. For instance, this attack can be triggered when you connect on a public wifi at a coffee shop or at an airport and not use VPNs or Virtual Private Networks. How this happens is the hacker gets your IP address and then proceeds to hack your machine. Data breaches can also happen when someone who is anonymous sends a link or file to you and when you open that link or file, a virus will work its way onto your machine and get your information. If your device has been breached, the hacker can browse through

your information freely without getting caught and they may have access to your personal data, credit card info, bank accounts, and other similar sensitive data.

How can data breaches be prevented?
There are a number of ways you can protect yourself from data breaches, and that number only goes up as technology advances over time. Here are some preventive measures that every user can do to protect their personal data:

- **Change your passwords regularly**

  Although changing your passwords can be laborious, it is one of the most effective precautions you can use to prevent data breaches. By changing your passwords, you can reduce the amount of time a hacker spends browsing and obtaining information from your account, which can also reduce the amount of harm they can cause. Be aware that it's recommended to change your passwords to something unique using numbers and special characters whenever you do so.
- **Use two-factor authentication**

  Using two-factor identification reduces the likelihood that a hacker will gain access to your account because it requires additional information that only the account owner can provide. Two-factor authentication is typically performed by delivering a code to a user's mobile phone or email address. More recent methods of two-factor authentication utilizes biometrics, such as fingerprint scanning, voice recognition, or retinal scans.
- **Update your system software**

  Updating the software system is not only to update and get new features on your device, but it's also about updating the security system. Every 2-4 months, there may be a new update to the system to be much safer and up to date to fix some bugs and security flaws.
- **Monitor your accounts**

  Keeping an eye on your accounts, may it be your email, bank accounts, or social media accounts, is essential to avoiding risks of data breaching. Suspicious activities like password reset requests that you did not request, phishing links posing as legitimate links, and the likes, are some of the most

common ways attackers execute data breaches, that is why we should always be vigilant with our accounts.

- **Be aware of security notifications and alerts**

  Sometimes having too many notifications and alerts can be exhausting, and there may be instances where we disregard notifications, and to some extent important ones as well. We should always be aware of alerts regarding the security of our accounts and devices. This way, we are in control of our data and we limit the damage attackers can do once we get an alert, may it be from our banks, our email providers, or our anti-virus software.

Cybersecurity in the U.S.-Philippine alliance: mission seep

Study examines the integration of cybersecurity within the U.S.-Philippine alliance.The growth of new forms of international conflict, like cybersecurity, occur below the threshold of a traditional armed attack and pose a direct challenge to security alliances designed to rebuff conventional military threats. Using a process-tracing approach, this article investigates the evolution of cybersecurity within the U.S.-Philippine relationship and how it has met this new challenge. It finds that despite mutual concern over cybersecurity, divergent approaches to the digital domain as a policy area has stymied alliance development. This finding highlights how issues like elite political discord, different threat perceptions, and divergent institutional preferences can hinder cyber cooperation between partners and stymie alliance development.

Understanding both data breach and cyber security is vital to stopping cyber attacks all across cyberspace

A law that protects citizens from this cybercrime has been passed by the government in the Philippines to prevent the increasing risk of data breaches. The Data Privacy Act of 2012, officially known as Republic Act No. 10173, prevents and addresses data breaches in the entire country. The management of a citizen's personal data corresponds to this law's obligations. In the event of a breach, organizations are required to immediately notify the National Privacy Commission and the affected individuals. Additionally, it establishes requirements for data protection and requires data privacy impact assessments (DPIAs) for high-risk processing activities. Furthermore, the law controls cross-border data transfers to guarantee that data is secured when leaving the Philippines. Also, this law attempts to reduce the risk of data breaches and guarantees

that any breaches that do happen are handled effectively and transparently. In general, the duties of this law include providing a thorough framework for data protection, establishing security standards, mandating accountability, and detailing sanctions for non-compliance.

III. EXAMPLES

Data breaches are a significant concern in the realm of cybersecurity, as they can lead to the exposure of sensitive and confidential information. Here are some cybersecurity threats that are often connected to data breaches:

1. **Hacking**: Skilled hackers use various techniques to gain unauthorized access to computer systems and networks, allowing them to steal sensitive data. This can include exploiting software vulnerabilities, brute force attacks, and using stolen credentials.
2. **Phishing**: Phishing attacks often lead to data breaches when individuals are tricked into revealing their login credentials, which attackers can then use to access systems and data.
3. **Malware**: Malicious software, such as keyloggers, spyware, or Trojans, can be used to steal data directly from infected systems, leading to data breaches.
4. **Insider Threats**: Employees or insiders with access to sensitive data may intentionally or accidentally expose that data through actions like data theft, sharing confidential information, or falling victim to social engineering attacks.
5. **Third-Party Breaches**: When a third-party vendor or partner experiences a data breach, it can potentially expose data of the organizations that use their services or share data with them.
6. **Weak or Stolen Credentials**: Weak passwords or the use of compromised credentials can make it easier for attackers to gain unauthorized access to systems and data.
7. **SQL Injection**: Attackers exploit vulnerabilities in web applications to execute malicious SQL queries, potentially allowing them to access, modify, or extract sensitive data stored in databases.
8. **File Upload Vulnerabilities**: Insecure file upload mechanisms on websites or applications can allow attackers to upload malicious files or scripts that can lead to data breaches.

9. **Inadequate Encryption**: Data that is not properly encrypted is more vulnerable to theft if attackers gain access to the underlying storage or transmission mechanisms.
10. **Unpatched Software**: Failure to keep software and systems up-to-date with security patches can leave them vulnerable to known exploits, potentially leading to data breaches.
11. **Data Exfiltration**: Attackers may use various techniques to exfiltrate data once they gain unauthorized access to a network, including transferring it to remote servers or hiding it within seemingly innocuous network traffic.
12. **Misconfigured Cloud Storage**: Improperly configured cloud storage services can expose sensitive data to the public internet, leading to data breaches.
13. **Ransomware**: In addition to encrypting data, ransomware attackers often threaten to publicly release sensitive information if a ransom is not paid.
14. **Data Interception**: Attackers intercept and capture data as it moves across networks, potentially exposing sensitive information during transit.
15. **Data Leaks**: Careless or negligent handling of data by employees or contractors can result in accidental data leaks.

Reports and publications from cybersecurity organizations and agencies like:

- The United States Computer Emergency Readiness Team (US-CERT)
- The Federal Bureau of Investigation (FBI) Cybercrime Division
- The Cybersecurity and Infrastructure Security Agency (CISA)
- Symantec (now NortonLifeLock)
- McAfee
- TrendMicro
- Palo Alto Networks

  These agencies and organizations have suffered greatly because of the threats shown earlier in Cyber Security Threats that are connected to Data breach.

The PlayStation Network Data Breach

In 2006, as the release of the much-awaited successor of the very popular PlayStation 2 video game console, the PlayStation 3, was nearing, tech giant Sony unveiled plans for a multi-player online network, dubbed the “PlayStation Network Platform”. It is designed to keep PlayStation 3 users connected online and give them a way to connect and share about their gaming experiences and host online game parties in the comfort of their living

room. Sony revealed this online service at the Tokyo Game Show in the same year. On the 20th of April, the year 2011, Sony's PlayStation network suffered an external security intrusion initiated by "hacktivist" group Anonymous, which forced the tech giant to suspend operations temporarily. A reported total of 77 million registered users have been affected, which sparked concerns about users having their credit card information stolen by the attackers. Sony reported that the intrusion focused on taking user data. While they cannot prove that users' credit card information has not been compromised, out of caution they have advised users that there is a possibility that it has also been stolen during the attack. As compensation for the service being down for a total of 23 days, Sony allowed PSN subscribers who joined before the 20th of April to download 3 PlayStation 3 games and 2 PlayStation Portable games for free. Users have also been given 30 days of PlayStation Plus, the online premium subscription service for PSN, while already-subscribed users before the 20th of April are given 60 days instead.

Palo Alto Networks

One of the globe's leading cybersecurity companies and an undisputed leader in the cybersecurity sphere specializing in threat detection and prevention, it boasts next – gen approach to cybersecurity. Located in the northwest corner of Santa Clara County, California and was founded in 2005 by Nir Zuk a former EIR or entrepreneur in residence at Greylock and a successful serial entrepreneur and a network security expert, he is now the CTO or Chief Technology Officer of the Company. Last year 2022 Palo Alto Networks product called Prisma SD – WAN became the overall winner of CRN'S 2022 SD – WAN Product of the year award and has achieved the highest scores in technology and customer needs. Prisma SD - WAN is the industry's first next-generation SD-WAN solution that provides exceptional user experience while also simplifying operations with improved security outcomes. According to Palo Alto Network's SASE SD - WAN web page that Prisma SD – WAN has flexible connectivity and zero routing complexity and also natively applies best - in - class security to branches with Zero Trust Network Access 2.0 or ZTNA 2.0, helping reduce breaches by 45%, while also ensuring application availability and delivers 10x improvement in performance.

Yahoo 3 Billion Account Data Breach

Yahoo uncovered a major breach of data in 2014 that involved Russian hackers which allowed them access to at least 500 million accounts' sensitive user data. Yahoo continued monitoring the hackers despite detecting the security flaw and concealing it from Verizon and the general public. Even reports claimed that Yahoo user credentials that had been stolen were being sold on the dark web. Yahoo's stock price fell by 3% as a result of the breach, and the company's market capitalization decreased by $1.3 billion. Yahoo has updated its data breach statement twice since September 2016, and a federal court in California partially denied a petition to dismiss class-action lawsuits. In 2017, Yahoo revealed that all 3 billion accounts were probably hacked beginning in August 2013.

IV. CONCLUSION

As digital technology increasingly evolves, so does the risk of cybercrime as a result of hackers who prey on the system's data storage, raising serious concerns for users, organizations, and society across the globe. Cybercrime, such as data breaches, has been a major concern for society since they disclose private information to unauthorized users online. Another danger it poses is that it has numerous methods to infiltrate a user's account or the system. This requires organizations and governments to adapt to the change and improve cybersecurity measures to ensure that they can protect our data privacy and battle emerging security threats. As users, it is also our duty to protect both our personal information and ourselves online. Only by accepting change and keeping vigilant will we be able to survive in this evolving digital world.

V. REFERENCES

Data breach. Definition. (n.d.). https://www.trendmicro.com/vinfo/us/security/definition/data-breach

Kaspersky. (2023, August 17). *What is cyber security?*. www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

PlayStation Network and Qriocity Outage FAQ. PlayStation.Blog. (2011, April 28). https://blog.playstation.com/archive/2011/04/28/playstation-network-and-qriocity-outage-faq/

Thorsen, T. (2005, May 16). *PlayStation 3 announced for 2006*. GameSpot. https://web.archive.org/web/20150111192304/http://www.gamespot.com/articles/playstation-3-announced-for-2006/1100-6124681/

Adlakha, R., Sharma, S., Rawat, A., & Sharma, K. (2019, October 11). Cyber Security Goals, Issues, Categorization & Data Breaches. IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8862255

Enterprise data breach: Causes, challenges ... - wiley online library. (n.d.). https://wires.onlinelibrary.wiley.com/doi/full/10.1002/widm.1211

Winger, G. H. (2022, August 21). Cybersecurity in the U.S-Philippine Alliance: mission seep. Taylor & Francis Online. https://www.tandfonline.com/doi/full/10.1080/09512748.2022.2112064

Implementing rules and regulations of the Data Privacy Act of 2012. National Privacy Commission. (2023, June 15). https://privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/

Prisma SD-wan wins CRN's 2023 SD-Wan Tech Innovation Award. Palo Alto Networks Blog. (2023, August 2). https://www.paloaltonetworks.com/blog/sase/prisma-sd-wan-wins-crn-2023-sd-wan-tech-innovation-award/#:~:text=We%20are%20excited%20to%20share,in%20technology%20and%20customer%20need.

8 ways to protect your identity against a data breach. Equifax Personal. (2023, August 28). https://www.equifax.com.au/personal/8-ways-protect-your-identity-against-data-breach

Kaspersky. (2023, August 30). *How data breaches happen*. www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/data-breach

Kaspersky. (2023, August 30). *How often should you change your passwords?*.

https://usa.kaspersky.com/resource-center/preemptive-safety/how-often-password-change

The Hacked & the Hacker-for-Hire: Lessons from the Yahoo Data Breaches (So Far). (n.d.). The National Law Review. https://www.natlawreview.com/article/hacked-hacker-hire-lessons-yahoo-data-breaches-so-far