USE DATA OF STOLEN IN DATA BREACH

Students Name:

Course:

Date:

The use of data stolen in data breach

There is no denying the impact of technological development in the modern world. This development has made business processes more convenient; this is due to quick decision-making processes brought by effective communication systems such as tele and video-conferencing. Nonetheless, the other hand is not as pleasant as the positives. As human digital presence grows, so does the vulnerability of personal information. Due to the internet, private and confidential information is more vulnerable than ever. The technological devices store vast chunks of information that can be exposed in case of a data breach. A data breach is the theft of sensitive and confidential information either through negligence or hacking. Data breaches are on the rise. According to Edwards et al. (2016), cyber-attacks are growing by a rate of 62% annually. Given the pace of internet popularity in the world, this number is expected to keep growing, putting more people at the mercy of cybercriminals. Cybercriminals use stolen information in ways that can harm an individual's or organizational reputation, security, and financial well-being.

Targeted data

Internet users worldwide have grown and continue to rise. This growth is attributed to social media, online games and the growth of the internet. Nonetheless, this growth is also reflected in the growth of cybercrimes which present a significant threat to internet users (Ngo & Jaishankar, 2017). Some of the data that attackers target include credit card names, numbers, residential address, identifiable information, and social security number. Khan and Hoque (2016) argue that data servers are the leading avenues for data theft, and the motive behind is monetary.

Uses and re-use of stolen data

Fraudsters usually use stolen data in financial fraud in applying for counterfeit credit cards, bank loans, fraudulent online transactions (Edwards et al., 2016). Solove and Citron (2017) echo this argument as they argue that credit card information can be used to cause harm to the victim. This information can be used to take loans, shopping and transfer of funds. Funds transferred to oversee accounts can be used for all manner of ways, including funding terrorism. Besides financial fraud, cybercriminals can also use this information for identity theft.

Cybercriminals use stolen data from hacks or accidental breaches in identity theft. Identity theft involves the use of another person's identity profile, usually for financial fraud or at the expense of the owner. It is a common way of committing fraud without getting noticed. Just like other types of cybercrime, identity rise is also on the rise. A 2014 Symantec report indicates an increase of 10% in the number of significant data breaches as well as a 5% increase of the identities exposed in that period (Edward et al., 2016). Identities are disclosed in the form of bank details, personal profile and identifiable information, and online account logins. Account logins and emails usually leave a digital print that hackers can easily access. For example, in 2004, Anthem Inc. was attacked. In this attack, the attackers accessed personal information for over 80 million (Perlroth, 2019). In another incident, hackers attacked the Home Depot's corporate network acquiring credit card numbers for over 56 million users. These were used to create counterfeits (Edward et al., 2016). Fraudsters used this information to create fake ID's for purchase of medical equipment's and commit other crimes.

Despite the growing rate, the public is still unaware of some basic regulations to control this phenomenon, and their behavior constantly leaves them at risk of cyberattacks. Most people re-use their passwords, making it easy to access personal information from the web. This information enables the hacker to impersonate the victim and commit financial fraud as well as other crimes. Personal identifiable information theft is used for extortion to commit such crimes like breaking into peoples' accounts, identity and intellectual property theft. A perfect example of fraud is the recent hacking of Twitter accounts belonging to prominent people. The hackers impersonated these users for financial fraud. According to Guardian staff and AP (2020), $100,000 was stolen, in the form of bitcoins, from unsuspected Twitter users.

Stolen data is also used for espionage among business competitors, or by activist groups to tarnish the reputation of an individual or organization. The information acquired is used for trading secrets and exposing confidential information (Lending et al., 2018). Security breaches are costly and have adverse reputational effects which could affect the business relationship with shareholders and stakeholders (Lending et al., 2018). It also costs the business in terms of finances when it comes to damage control. On average, businesses incur a loss of 1% of the market share whenever there is a security breach. However, what is unknown is the long-term economic impact of these breaches, which seem to be substantial and dire. According to a report by McAfee Corporation, the worldwide cost of cyber-crime is around trillion US dollars (Ngo & Jaishankar, 2017). These funds can be used for purposes of product promotion or other areas of organizational development. Therefore, malicious attacks, with the aim damaging reputation, harm companies and individuals, both financially and in business connections; this affects corporate competitiveness.

Cybercriminals also sell the stolen confidential information to the dark web. Once in the dark web, criminals can use this information in blackmail and extortion. This phenomenon is whereby a hacker gets in the system, maybe take control of it, and ask for a ransom or favors. Blackmail can also involve the use of personal and confidential information found on the internet. According to Krisby (2018), this trend is on the rise it affects both individuals and organizations. These studies argue that the healthcare sector is the most affected. Krisby (2018) reports of an attack on Hollywood Presbyterian Medical Centre, that happened on February 5, 2016. In this case, the hacker encrypted all patient information and demanded $17,000 of ransom. The hospital was locked out of the system for a week. They decided to pay the ransom to avoid further damage.

Trends in acquiring data

Despite the growing awareness of data breach and hacks, the public and business institutions are still unable to prevent this crime. The fact that the internet is growing in popularity and new ways of phishing are still being devised makes it challenging to control this phenomenon. Some of the latest trends in acquiring data include remote attacks (Gravrock, 2019). Remote attacks involving cryptocurrency is predicted to continue growing with the popularity of the bitcoin. Also, smartphone attacks, due to the prevalence of these devices, are predicted to grow. Smartphone apps, such as *Tik Tok* and *Like,* might appear exciting, but they present avenues for cyberattacks (Gravrock, 2019). With the prevalence of Artificial Intelligence and robotic technology, hackers are expected to infringe these devices for ransom and blackmail as well as other malicious attacks.

In conclusion, cybercriminals use stolen information in ways that can harm an individual's or organizational reputation, security, and financial well-being. The data targeted in the breach include credit card names, numbers, residential address, personal identifiable information, and social security number. This information is used in financial fraud, identity theft, espionage and damage of reputation as well as blackmail and extortion. The popularity and prevalence of smartphone technology offer potential trends in data phishing. In addition, artificial intelligence technology will present new vulnerabilities for hackers to exhaust. Given the nature and growth of this crime, there is a need to control digital information access and sharing. For now, cybercriminals and hackers continue to terrorize the public, gathering and stealing personal information that they use in various ways to hurt the victims.

References

Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity*, *2*(1), 3-14.

Gravrock, E. (2019). Here are the biggest cybercrime trends of 2019. *World Economic Forum.* https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/

Guardian staff and AP. (2020). Twitter hack: US and UK teens arrested over breach of celebrity accounts. *The Guardian.* https://www.theguardian.com/technology/2020/jul/31/twitter-hack-arrests-florida-uk-teenagers

Khan, S., & Hoque, A. (2016). Digital health data: A comprehensive review of privacy and security risks and some recommendations. *Computer Science Journal of Moldova*, *71*(2), 273-292.

Krisby, R. M. (2018). Health care held ransom: modifications to data breach security & the future of health care privacy protection. *Health Matrix*, *28*, 365.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review*, *53*(2), 413-455.

Ngo, F., & Jaishankar, K. (2017). Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. *International Journal of Cyber Criminology*, *11*(1).

Perlroth, N. (2019). Two From China Are Charged in 2014 Anthem Data Breach. *New York Times*. https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html

Solove, D. J., & Citron, D. K. (2017). Risk and anxiety: A theory of data-breach harms. *Tex. L. Rev.*, *96*, 737.