FORUM:	United Nations Commission on Science and Technology for Development
ISSUE:	Developing measures to robust Data Privacy and protect cybersecurity in the Digital Age
STUDENT OFFICER:	Jin Kwon
POSITION:	President of UNCSTD

Introduction

Even the simplest tasks from checking information to buying products are done digitally in the modern society. Technology has now reached the domain where it highly interferes with people's lives. As traditional methods of completing tasks start to decline and shift to digital platforms, there are inevitable consequences that put a lot of people in danger, making the quote, "data is the new oil," an accurate way to depict the two-sidedness of the modern digital age, as data online could be innovative while it could also bring societal damages.

Depiction of the Complex Nature of the Digital Age

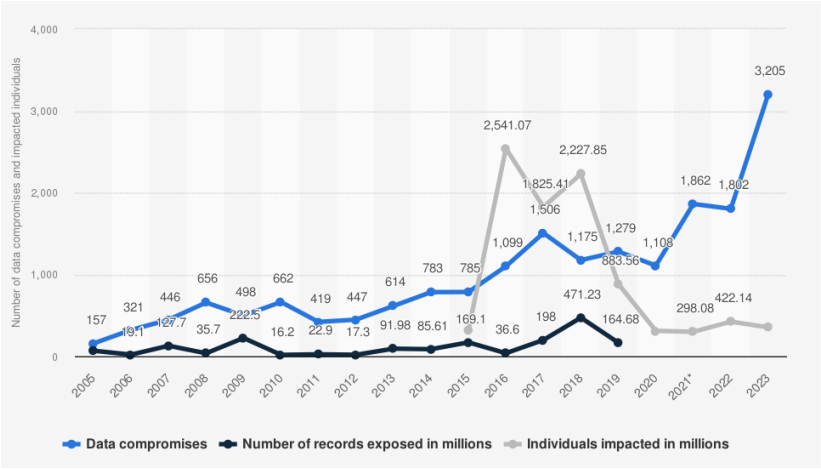
Data privacy is a hot issue these days because of the extensive usage of data in the contemporary society. Digital data handles critical personal information such as social security numbers, health records, and financial data, yet these are just the few major areas where people's information are exposed to. Due to a somewhat idiosyncratic characteristic of digital data, once a piece of information is on the internet, it is nearly impossible to get rid of its track, making some personal information easily transferred to the wrong hands. Unexpected data releases often lead to a mass digital attack, producing a massive number of victims whose released personal information could potentially lead to risks of identity theft, fraud, and other malicious activities. On the contrary to what the worst could happen from insecure data management, with sufficient digital privacy technology and management, people's data will be secure and corporations dealing with personal information will be able to build a reputation for reliability and integrity. Therefore, rather than criticizing for some incidences of data outflow, people should put in effort to maximize cybersecurity and minimize further unfortunate loses.

When it comes to developing new technologies especially in a digital age like the current one, the net benefit and the possible risks should always be the factors to be analyzed and assessed multiple times,

as it can potentially bring chaos to the human population. It is imperative that people talk about digital privacy—not only to safeguard individual freedoms and protect against potential threats but also to ensure that the technological advancements do not compromise the security and well-being of future generations. By prioritizing digital privacy with the discussions and policies for innovative technological advancements, a more secure, trustworthy, and equitable digital landscape for all can be formed.

Background

In the modern digital society, data privacy has emerged as a critical concern due to the pervasive nature of technology and the exponential growth of data collection. The importance of data privacy stems from its role in protecting individuals' personal information from malicious actions explained above. Information is crucial for companies or corporations for various reasons of their own, leading to a “race” to collect relevant and necessary private data from consumers to apply in their businesses. Data brokers, individuals who aggregate information and sell them at high prices through the process of extensive analysis and categorization, are massive in number these days, and the extent information they can find of people online makes them one of the most non-negligible factors in cyber security. Sold personal information is not only dangerous because of the out flow of personal information that can bring people financial problems but also because of the judgments people get due to the exposed information. For example, when companies with large data bases, or some dark influences of data brokers, are finding employees, they can filter out applicants for their recent transactions, habits, or simply for their personal philosophies. Although it can sound difficult to accumulate data of another person, it is an undeniable fact that it has become extremely easier to do so at recent times for those who have sufficient capacity and technology. The low security rate and easy accessibility of these personal information is what is causing all this problem, leading to a solution to reinforce cyber security.

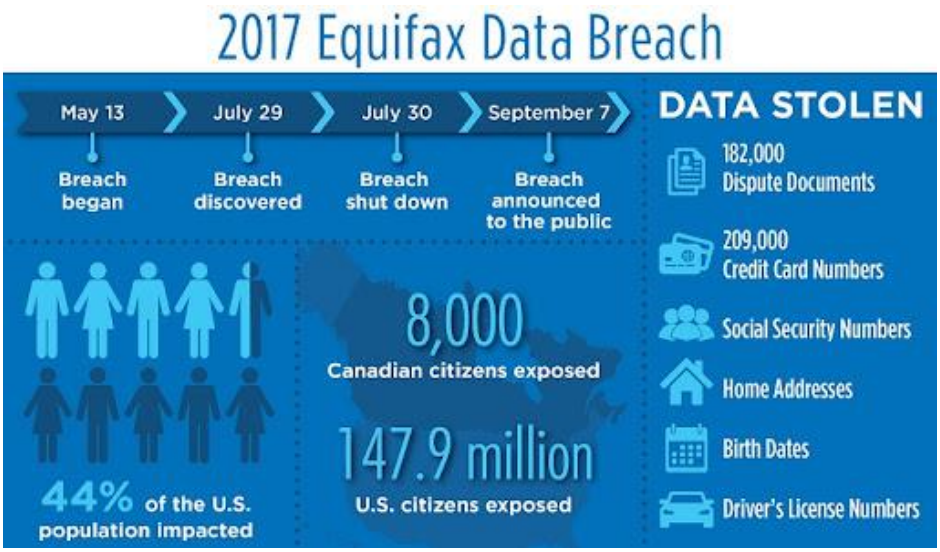


Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2023

The origins of the data privacy problem can be traced back to the advent of the internet and the rise of digital platforms in the late 20th century. As businesses, governments, and individuals began to

store and share information online, the need for robust data protection mechanisms became increasingly apparent. However, the rapid pace of technological advancement outstripped the development of corresponding privacy safeguards, leading to a landscape where vast amounts of personal data are routinely collected, often without adequate security measures or user consent. This disconnects between data collection practices and privacy protections has made data privacy a pressing issue, requiring urgent attention to ensure that the benefits of the digital age do not come at the cost of individual rights and societal trust.

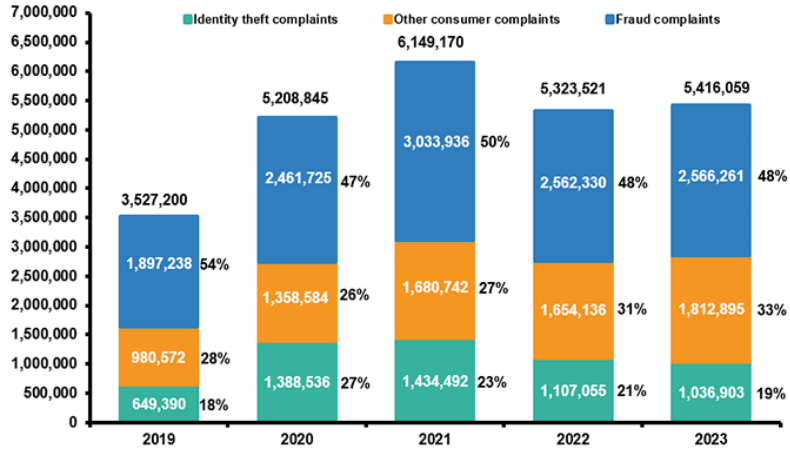
The potential danger of cyber insecurity can be seen from a fairly recent incident of the Equifax data breach. Equifax, one of the three largest consumer credit reporting agencies in the United States announced in 2017 that data, information regarding to names, addresses, phone numbers, dates of birth, and social security numbers, of approximately 150 million US citizens were released, brining those who got their credit card numbers released immense financial loses. One of the three major reporting agencies (CRAs) in the United States, Equifax is responsible for creating reports that give a detailed picture about a person's credit history. Identity theft like the Equifax incident can completely derail one's credit and their financial future, making victims suffer from being responsible for financial activities they did not conduct. Abusing other's financial credit leaves victims denied from credit cards and loans, unable to purchase or rent an apartment, increased interest rates, greater difficulty getting a job, and suffering severe mental distress and anxiety. The cause of this unfortunate incident was the vulnerability of their cyber security system which was later investigated and refined by multiple cybersecurity firms. The Equifax breach has captured the attention of many huge organizations of government scale and brought some changes, sending a message to the world of the importance of cybersecurity and appropriate legislations for the issue. It demonstrates how even large, well-resourced organizations can suffer devastating breaches if they do not prioritize and maintain robust cybersecurity measures.



Equifax Data Breach Statistics

Problems Raised

Identity Theft and Damaged Financial Industry



Statistics On Recent Incidents on Data Breaches

Weak cybersecurity can lead to unauthorized access and theft of personal information, such as social security numbers, addresses, and credit card details in addition to any identifying data. Using one's name and identity to commit a crime can cause a serious problem, as it can have long-lasting consequences that can affect one's reputation. Increasing cybercrime rates are noticed throughout the years; in 2023, for example, FBI announced an Internet Crime Repot in which had reports claiming for a loss of an astonishing 12.5 billion USD by cybercrime. The Federal Trade Commission's (FTC) Consumer Sentinel Network also reported that 20% of cybercrimes were identity thefts, 40 percent of which was credit card fraud.

Cybersecurity risks notably affect the banking sector. Cybercriminals view banks and other financial organizations as high-value targets because they keep sensitive consumer information along with financial data. Companies may suffer significant financial losses and reputational harm as a result of data breaches. Over 100 million customers were impacted by a major data breach that Capital One had in 2019, which resulted in a $100 million punishment from authorities. This breach not only exposed sensitive personal information, such as Social Security numbers and bank account details, but it also highlighted the vulnerabilities in cloud-based infrastructures that many financial institutions increasingly rely on. The incident serves as a stark reminder of the growing sophistication of cyber threats and underscores the critical need for robust, proactive cybersecurity measures to protect both the integrity of financial systems and the privacy of millions of customers.

Unsafe Environments for Small Businesses

Six months after a cyberattack, 60%Opens a new window of small businesses close, according to a National Cyber Security Alliance study. This is caused in part by the expense of fixing harm and reputational harm. Small companies might not consider cybersecurity to be their primary priority, but they should. By making the right cybersecurity investments, businesses may shield their staff, clients, and revenue from expensive cyberattacks. Furthermore, the consequences of a cyberattack can last longer than just the money lost right away, which puts small firms at risk of long-term harm. This entails a

decline in consumer confidence, legal ramifications, and the possible disclosure of private company data. It is imperative that small firms take a proactive approach to cybersecurity since, in a highly competitive industry, even one security compromise can have catastrophic consequences. Strong security measures that are put in place, such data encryption, frequent software upgrades, and personnel training, may greatly lower the likelihood of a cyberattack occurring and guarantee the long-term viability of the company.

International Actions

The European Union General Data Protection Regulation (GDPR)

GDPR is the most prominent data privacy and security laws in the world. While its main purpose is to protect data, it has significant implications for cybersecurity, mandating organizations to implement robust security for protection and report immediately after attempts of breaches. The law aims to give consumers control over their own personal data by holding companies responsible for the way they handle and treat this information. The regulation applies regardless of where websites are based, which means it must be heeded by all sites that attract European visitors, even if they don't specifically market goods or services to EU residents. This law makes it difficult for consumers to be misled during their visit to the website; websites are supposed to notify visitors for data collection, request consent for gathering personal information, and notify the visitors that their data is breached if there are any attempts to do so. To strengthen compliance, organizations must also regularly assess and update their security measures to adapt to new threats and vulnerabilities. Failure to comply with GDPR can result in substantial fines, which can be as high as 4% of a company's annual global revenue or €20 million, whichever is greater. This regulation has set a global standard for data protection, influencing privacy laws in other regions and prompting companies worldwide to reevaluate how they handle personal data.

Cybersecurity Tech Accord

With the cooperation with Partnership Against Cybercrime and the Global Centre for Cybersecurity, the World Economic Forum (WEF) launched several initiatives to reinforce global cybersecurity. These initiatives enhance public-private cooperation, developing a stable framework and promoting the best practices across industries. In the tech industry, for example, over 100 technology companies including Microsoft, Cisco, and HP signed the Cybersecurity Tech Accord to pledge to protect their customers from cyberattacks, regardless of the attacker's motivations or origins. The accord fosters a stable and strong defense system that protects data loses and displays a greater transparency in the security ecosystem. These initiatives are essential to establishing a cohesive worldwide response to the growing dangers in cyberspace and guaranteeing that enterprises can work together efficiently to mitigate cyber risks. Additionally, the World Economic Forum stresses the need for ongoing innovation in cybersecurity defenses and exhorts companies to keep ahead of new dangers. These programs seek to increase sectoral resilience by promoting a shared responsibility culture, which will protect vital infrastructure and preserve public confidence in digital systems.

Key Players

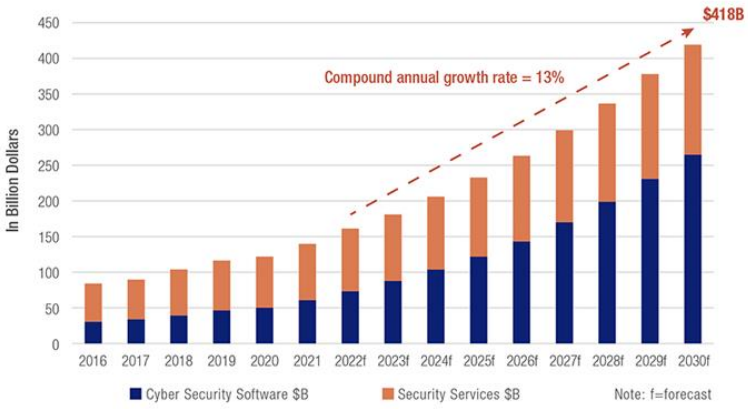
World Economic Forum (WEF)

The WEF is exists to foster collaboration between governments, businesses, and civil societies to resolve global challenges. The primary purpose of the WEF is to promote private-public cooperation, gathering leaders from all around the world to discuss about solutions to major global problems such as economic inequality, climate change, and cybersecurity. As the WEF believes that the power of collaboration between the government and the private sector is massive, it emphasizes on creating partnerships to drive economic growth and improve social inclusion while minimizing the effects of those that impedes it from achieving its goals. The WEF views the issue on cybersecurity as a danger to the economic ecosystem, bringing unbalance and banking frauds alongside the release of personal data. The WEF has started a number of projects to combat these concerns and seeks to improve international collaboration in tackling cyber threats. The WEF aims to strengthen the digital economy by supporting cybersecurity innovation and best practices.

Cybersecurity Firms

Cybersecurity firms like NortonLifeLock, Palo Alto Networks, and CrowdStrike have key roles because they are responsible for protecting organizations, governments, and individuals from cyber

threats. The firms play a key role in minimizing the damage of cybercrimes by showing expertise and innovation, possessing specialized knowledge and technology, such as fire walls, encryption, and intrusion detection system, that are essential for combating cyber threats. These firms continuously monitor cyber landscapes for emerging threats and vulnerabilities. They provide threat intelligence services that help organizations detect, prevent, and respond to cyberattacks in real-time, minimizing damage and ensuring business continuity. Acknowledging their importance to the field of cybersecurity, firms constantly invest on their Research and Development (R&D) sector for a secure and safe cyber environment. NortonLifeLock's Norton Security and its successor Norton 360, for example, are examples of a cyber security program that are continuously being improved to provide the best safety services. NortonLifeLock is renowned for its award-winning defense programs that are considered an innovation in the field of cybersecurity. Their commitment to staying ahead of cybercriminals involves not only technological advancements but also a focus on educating the public and raising awareness about cyber risks. By providing training programs and certifications, cybersecurity firms help to cultivate a skilled workforce capable of defending against ever-evolving cyber threats.



Investment Trends on Cybersecurity

Possible Solutions

Strengthen Legal Frameworks and Regulations

Establishing a global standard for data protection similar to the EU's GDRP can ensure that personal information is secured across borders. A cybersecurity framework is a set of guidelines that outlines standards to define the processes and procedures that an organization must take to assess, monitor, and mitigate cybersecurity risk. A cybersecurity framework provides a common language and set of standards for security leaders across countries and industries to understand their security postures and those of their vendors. This helps organizations know what type of security is need so that everyone has the same level of security and protection from breaches. With sufficient global scaled law enforcement, immediate reports of cyber incidents enable others to prepare for further attempts. Due to the fact that cyber breaches are border-neglecting, attempts to make a global legal framework end up with multiple countries cooperating to solve an unanimously suffering problem.

In addition to the widespread General Data Protection Regulations (GDPR), there are many other international frameworks such as the ISO 27001 and the ISO 27002 developed by the International Organization for Standardization, the Service Organization Control Type 2 (SOC2) developed by the American Institute of Certified Public-Accountants (AICPA), and the North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC-CIP) that show great examples of the global efforts taking place to address this issue.

Promoting Public-Private Partnerships

Macron holding a emergency cybersecurity meeting

With the severity of the issue rising, cybersecurity issues are serious problems not only to the government and corporation level but also to the civilians. It is important for governments to acknowledge the fact that the digital age requires digital solutions, and there is no difference between countries that governments do not possess the ability to solve all problems, especially for those that require extensive skill and knowledge on the field of cybersecurity. It is highly encouraged and recommended that government organizations cooperate with private cybersecurity firms to resolve this issue through developing advanced defense programs. With government-scale investment and support and the skill of cybersecurity firms, cybersecurity issues will be reduced. Additionally, public awareness campaigns led by both government and industry can educate citizens on how to protect their personal data and recognize potential threats. Ultimately, this united approach not only strengthens national security but also fosters a safer and more secure digital environment for everyone.

Sources

Center, Electronic Privacy Information. “Epic - Equifax Data Breach.” *Electronic Privacy Information Center*, archive.epic.org/privacy/data-breach/equifax/. Accessed 25 Aug. 2024.

“Facts + Statistics: Identity Theft and Cybercrime.” *III*, www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime. Accessed 25 Aug. 2024.

Husain, Osman. “The Benefits of Data Privacy: Why It’s Meant to Be Taken Seriously.” *Data Privacy Compliance Software for Apps, Websites, & SaaS*, Enzuzo, 12 July 2023, www.enzuzo.com/blog/data-privacy-benefits.

“The Importance of Data Privacy and Security.” *Algolia*, www.algolia.com/blog/product/what-are-data-privacy-and-data-security-why-are-they-critical-for-an-organization/. Accessed 25 Aug. 2024.

Limited, Cecure Intelligence. “Analyzing the Roots, Impacts, and Remedies of Global Cyber Insecurity.” *LinkedIn*, 6 July 2023, www.linkedin.com/pulse/analyzing-roots-impacts-remedies-global-cyber-insecurity.

Liu, Henry, and Staff at the FTC. “Equifax Data Breach Settlement.” *Federal Trade Commission*, 24 July 2024, www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.

“Nortonlifelock Continues Its Award Winning Streak with Three AV-TEST Institute Wins.” *Business Wire*, 20 Mar. 2020, www.businesswire.com/news/home/20200320005093/en/NortonLifeLock-Continues-Its-Award-Winning-Streak-With-Three-AV-TEST-Institute-Wins.

Ravaioli, Edoardo. “Tech Accord Urges Changes in Flawed Final Draft of UN Cybercrime Convention, to Safeguard Security, Tech Workers, and Uphold Data and Human Rights.” *Cybersecurity Tech Accord*, 5 Aug. 2024, cybertechaccord.org/tech-accord-urges-changes-in-flawed-final-draft-of-un-cybercrime-convention-to-safeguard-security-tech-workers-and-uphold-data-and-human-rights/.

Team, The Investopedia. “General Data Protection Regulation (GDPR): Meaning and Rules.” *Investopedia*, Investopedia, www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp. Accessed 25 Aug. 2024.

Technologies, Veritas. “The Importance of Data Privacy and Compliance: A Comprehensive Guide.” *Veritas*, www.veritas.com/information-center/data-privacy. Accessed 25 Aug. 2024.

Tobin, Donal. “What Is Data Privacy-and Why Is It Important?” *Integrate.Io*, Integrate.io, 2 Mar. 2024, www.integrate.io/blog/what-is-data-privacy-why-is-it-important/.

“The Top 5 Cybersecurity Threats and How to Defend against Them.” *ISACA*, www.isaca.org/resources/news-and-trends/industry-news/2024/the-top-5-cybersecurity-threats-and-how-to-defend-against-them. Accessed 25 Aug. 2024.