Committee: United Nations Commissions on Crime Preventions and Criminal Justice (CCPCJ)

Issue: Fostering Public-Private Partnerships for Enhanced Personal Data Security

Student Officer: Yeonjo Ahn, Mirae Kim

Introduction

In the era of technological advancement and digitalization, sharing information online has become an indispensable part of our lives. As it has become easier to access personal data, privacy has emerged as a more critical factor than ever before. The rapid digitalization of society has brought several unprecedented benefits and challenges to personal data security. With the increasing sophistication of data breaches, cyber threats, and personal information leakage, cyber security problems have become a priority to both public and private sectors. PPPs are a strategic, collaborative approach to addressing this issue, each bringing unique strengths and resources to enhance data security frameworks.

Personal data infringement is continuously happening globally. MIT's overview of 2022 and 2023 statistics research shows that over 2.6 billion personal records were breached in 2021 and 2022, a threefold increase from 10 years ago. With 98 percent of organizations having a relationship with a business that experienced a data breach within the last four years, it is clear that personal data security is a topic we need to take seriously.

Fostering PPPs about personal data security will facilitate innovation, regulatory compliance, and robust security infrastructures. It is crucial to target policymakers, industry leaders, and other stakeholders committed to protecting personal data in a connected world to achieve consideration for successful practices and their actionable insights and recommendations.

Definition of Key Terms

Public Company

A public company is a corporation whose shares are owned by the general public, allowing shareholders to claim a portion of the company's assets and profits. These shares are freely bought and sold on major stock exchanges. Public companies often have greater access to capital through the sale of shares, which can fuel expansion and growth. However, they are also subject to more scrutiny and regulatory oversight compared to private companies.

Private Company

A type of business entity that is privately owned, either by an individual or a group. Private companies can still issue company stock and raise capital from outside shareholders, but their shares do not trade on a public stock exchange.

Public-Private Partnerships

A partnership between the public and private sectors to deliver a project or service traditionally provided by the public sector.

Data Security

The process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorised access.

Data Breach

A compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to protected data transmitted, stored, or otherwise processed.

Cyber Security

Technologies, practices and policies for preventing cyberattacks or mitigating their impact.

Customer Service

The assistance and advice provided by an organisation to its customers before, during, and after they purchase or use its products or services.

National Information Network

A centralized system that connects government agencies, institutions, and sometimes the public, enabling the secure sharing and coordination of data and information at the national level.

European Data Protection Board (EDPB)

An independent European body which ensures the consistent application of data protection rules throughout the European Union.

Cybersecurity and Infrastructure Security Agency (CISA)

A component of the United States Department of Homeland Security(DHS) is responsible for cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with U.S. states, and improving the government's cyber security protections against private nation-state hackers.

Criminal Offense Data

Information and records related to crimes that have been reported, investigated, or prosecuted. This data typically includes details such as the nature of the offense, the individuals involved, dates and locations, and outcomes of legal proceedings. It is used for law enforcement, legal, and statistical purposes to track and analyze criminal activity within a jurisdiction.

General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) is a statute which governs how the personal data of individuals in the EU may be processed and transferred.

History

Pre-rise and the beginning of Networking and data breaches

In the early days of computing, security focused primarily on physical access control over the data centres. Given the limited access available to a small number of users, the threat of data leakage was minimal. However as centuries passed, the development of more sophisticated encryption algorithms started opening up the era allowing a variety of approaches. In the 1980s the personal computer revolution brought computing to the masses, leading to increased data storage on personal devices. With a huge shift of accessibility, software based security measures, like passwords and anti-virus programs started to appear.

Beginning of the Data Breaches

In the 1990s the first major incident of data breaches began to emerge. Involving unauthorised access to sensitive personal information like card numbers, personal identification details, and more, companies and governments started to recognize the severity of data breaches and the need for robust data security measures.

The Rise of Cybercrime and Growing Threats

The early 2000s witnessed the advent of organized cybercrime, which capitalized on vulnerabilities in rapidly expanding digital networks. With the growth of the internet and e-commerce, hackers began to target organizations to steal financial information, intellectual property, and consumer data. High-profile breaches, such as the theft of millions of credit card details from major retailers, highlighted the potential for significant financial and reputational damage. Governments and private entities began investing heavily in cybersecurity measures, yet these efforts often operated in silos, reducing overall effectiveness.

Emergence of Public-Private Collaborations

As cyber threats evolved, the realization grew that neither public institutions nor private companies could tackle the problem alone. In the late 2010s, public-private partnerships (PPPs) began to emerge as a strategic response. Governments initiated collaborations with tech companies, financial institutions, and other industries to share threat intelligence, develop advanced security technologies, and establish standards for data protection. For example, initiatives like the Cybersecurity and Infrastructure Security Agency (CISA) in the United States worked closely with private organizations to strengthen national defenses against cyberattacks.

The Age of Regulation and International Cooperations

Legislative frameworks such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) set benchmarks for data protection. These regulations encouraged private entities to adopt stricter security measures while fostering transparency and accountability. International organizations, including the United Nations, started addressing cybercrime and data breaches as global issues requiring multilateral cooperation.

Challenges in Current Approaches

Despite progress, challenges persist. Divergent priorities between the public and private sectors often hinder effective collaboration. Governments prioritize national security and public welfare, while businesses aim to protect profits and minimize operational disruptions. Furthermore, the lack of a unified global framework limits the effectiveness of cross-border data protection efforts. This underscores the need for strengthened partnerships that balance diverse interests to safeguard personal data more effectively.

Key Issues

Frequent Data Leakage

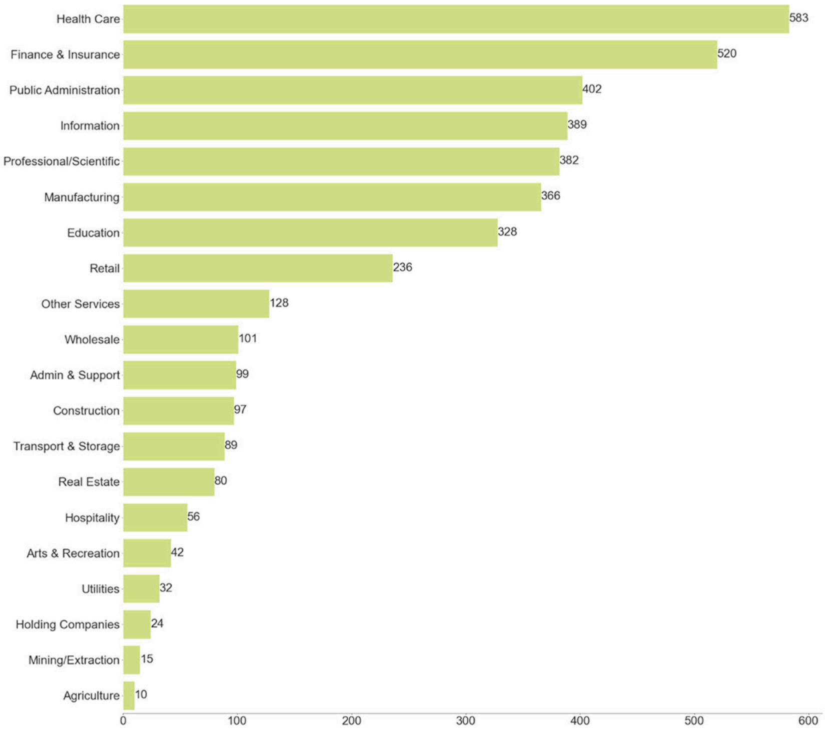
Data breaches are security events where confidential and sensitive information is accessed by unauthorized parties. As life on online rapidly develops and spreads across the globe, the frequency of data leakage is substantially increasing. In the first quarter of 2023, 6.41 million data records were compromised in global data breaches, affecting millions of individuals. These breaches can happen through the internet, Bluetooth, and text messaging. Such incidents have profound implications for individuals, organizations, and government entities.

Drawbacks of Data Leakage

Recovering the Data leakage incident by restoring the beached data and compensating customers has a substantial financial impact on victim companies and institutes. The global average data breach cost in 2023 was aggregated as $4.45 million USD, and the shift to remote work has added an estimated $137,000 USD to the financial toll of each incident. The Ponemon Institute of UNDRR identified notable points associated with the impact of data breach incidents, including: the more records lost, the higher the cost of the data breach; the faster the data breach can be identified and contained, the lower the costs; hackers and criminal insiders cause the most data breaches; incident response teams and extensive use of encryption reduce costs; and third-party involvement in a breach and extensive cloud migration at the time of the breach increases the cost.

Industries targeted by data breaches

Finance and healthcare are some of the most significant industries vulnerable to data leakage. As banks and insurance companies store a vast amount of sensitive and crucial data and financial resources, and the overall healthcare institution duties incorporate managing and analyzing sensitive information, these industries show higher possibilities of data-leaking crimes and abuses.



Caption #1: Number of breaches by economic sector, reported by EOY 2021

Data Leakage prevention

Assorted nations and institutions endeavour for effective data leakage prevention. In 2017, the UN released its second Global Cybersecurity index (GCI), and the International Telecommunication Union (ITU) reported that about 38% of countries have published cybersecurity strategy and an additional 12% of governments are in the process of developing one (United Nations, 2017; ITU, 2020a). Current prevention suggestion to reduce data breach hazards reported by UNDRR includes: having an incident response team; having extensive use of encryption; having employee training and their participation in threat sharing; developing processes for business continuity management; using cyber analytics; using systems for data loss prevention; and appointing professionals such as Chief Privacy Officer Technology, Computer, Computer Security with Board level involvement for leadership in managing data breach reduction (Ponemon Institute, 2017).

Major Parties Involved and Their Views

US

Department of Homeland Security(Cybersecurity and Infrastructure Security Agency - CISA)

The Department of Homeland Security is a federal department of the United States government responsible for ensuring the safety and security of the United States from a wide range of threats. Established in response to the September 11, 2001, terrorist attacks, DHS coordinates efforts to protect the country against terrorism, manage border security, enforce immigration laws, safeguard cyberspace, and respond to natural and man-made disasters.

Google

Google is a leading global technology company known for its search engine and diverse services like cloud computing, software, and hardware. In cybersecurity, Google enhances protection through its platforms, including Google Cloud, Android, and Gmail. It plays a key role in securing user data and advancing encryption standards. Google also contributes to global cybersecurity with initiatives like Project Zero, which identifies software vulnerabilities. These efforts help safeguard billions of users from cyber threats worldwide.

Germany

Federal Office for Information Security (BSI)

The Federal Office for Information Security (BSI) is a German government agency dedicated to IT security. It plays a crucial role in safeguarding critical infrastructure from cyber threats by certifying IT products to meet security standards and offering support during cyber incidents. The BSI also works to increase cybersecurity awareness and conducts research to address emerging threats, helping to enhance the overall security landscape in Germany.

SAP

SAP is a leading global enterprise software provider that helps organisations manage various business operations efficiently. Known for its robust solutions, SAP emphasises data protection and cybersecurity, integrating advanced security features to ensure customer data remains secure and compliant with global standards. The company's innovative technologies support businesses in driving growth and achieving operational excellence.

United Kingdom

National Cyber Security Centre (NCSC)

The National Cyber Security Centre (NCSC), part of GCHQ, is the UK's authority on cybersecurity, established in 2016 to protect against cyber threats. It prevents attacks, responds to incidents, and supports both public and private sectors with cybersecurity guidance. The NCSC also advises the government on strategy and collaborates internationally to strengthen global cyber resilience. Additionally, it provides resources and training to enhance the cybersecurity capabilities of organisations across the UK.

Vodafone

Vodafone Group plc is a major British telecommunications company headquartered in London. Established in 1984, it operates globally, providing mobile and fixed-line services across Europe, Africa, the Middle East, and Asia. Known for its technological innovations and extensive network, Vodafone plays a key role in the telecom industry, focusing on both connectivity and digital services. The company also emphasises sustainability and social responsibility in its operations. As a major global telecommunications provider, has several initiatives and strategies in place to contribute to cybersecurity, both for its customers and the broader digital ecosystem.

Japan

Ministry of Internal Affairs and Communications (MIC)

The Ministry of Internal Affairs and Communications (MIC) in Japan oversees government operations, public safety, and telecommunications. It regulates and supports the development of communication networks, manages digital infrastructure, and ensures data protection and cybersecurity. MIC plays a key role in shaping policies to enhance the efficiency and security of Japan's public services and communication systems.

Sony

Sony is a leading global technology and entertainment company, renowned for its innovative consumer electronics, including TVs, smartphones, and cameras, as well as its PlayStation gaming consoles. It also has major entertainment divisions, such as Sony Pictures and Sony Music. Sony prioritizes cybersecurity and data protection to ensure the safety of user information across its wide range of products and services. Additionally, Sony invests in cutting-edge technologies to enhance user experiences and stay ahead in the competitive tech and entertainment markets.

South Korea

Korea Internet & Security Agency (KISA)

The Korea Internet & Security Agency (KISA) is a South Korean government organisation dedicated to improving cybersecurity and ensuring the safe use of the internet. KISA develops and enforces internet security policies, responds to cyber threats, and provides support to both public and private sectors. It also plays a key role in promoting digital innovation, managing domain registration, and enhancing overall internet infrastructure to protect South Korea's digital environment.

Samsung

Samsung is a global technology leader known for its extensive range of products, including smartphones, electronics, and home appliances. The company emphasises data security across its diverse product lineup, integrating advanced security features to protect user information and ensure privacy. Samsung's commitment to cybersecurity involves implementing robust measures and regular updates to safeguard against threats, reflecting its dedication to providing secure and reliable technology solutions to consumers worldwide.

Australia

Australian Cyber Security Centre (ACSC)

The Australian Cyber Security Centre (ACSC) is the national authority for cybersecurity in Australia, focused on protecting against cyber threats. It supports government, business, and public sectors with guidance, incident response, and threat intelligence. The ACSC works to enhance Australia's cyber resilience through strategic advice, policy development, and international collaboration. Additionally, the ACSC offers resources and training to help organizations and individuals improve their cybersecurity practices.

Atlassian

Atlassian is a leading software company renowned for its project management and collaboration tools, including popular products like Jira and Confluence. The company emphasises robust data protection and security measures to safeguard user information across its platforms. Atlassian integrates advanced security features and complies with industry standards to ensure the integrity and confidentiality of data, reflecting its commitment to providing secure and reliable solutions for businesses and teams worldwide.

Canada

Canadian Centre for Cyber Security (CCCS)

The Canadian Centre for Cyber Security (CCCS) is Canada's national cybersecurity authority, focused on protecting digital infrastructure from cyber threats. It offers guidance, support, and resources to government, businesses, and individuals, while monitoring and responding to cyber incidents. The CCCS also shares threat intelligence and develops strategies to enhance national cyber resilience and safeguard critical systems.

Shopify

Shopify is a leading e-commerce platform that prioritises data security by implementing advanced measures to safeguard user and merchant information. It employs robust encryption, secure payment processing, and continuous security updates to protect against cyber threats and ensure data integrity. Shopify's commitment to security helps create a safe and reliable online environment for businesses and their customers.

Israel

National Cyber Directorate (INCD)

The National Cyber Directorate (INCD) is Israel's government agency tasked with strengthening cybersecurity. It develops policies, coordinates incident responses, and supports both public and private sectors in protecting national infrastructure from cyber threats. The INCD also works on enhancing cyber resilience through research, awareness, and international collaboration. Additionally, it provides specialised training and resources to help organisations better prepare for and respond to cyber incidents.

Check Point Software Technologies

Check Point Software Technologies is a global leader in cybersecurity, offering advanced solutions to protect data and networks for businesses worldwide. Its comprehensive security products, including firewalls and threat prevention tools, help organisations safeguard against cyber threats and maintain data integrity. Additionally, Check Point is known for its innovation in cybersecurity research, frequently updating its technologies to address emerging threats and vulnerabilities.

France

National Cybersecurity Agency of France (ANSSI)

The National Cybersecurity Agency of France (ANSSI) is responsible for national cybersecurity, focusing on protecting critical infrastructure, providing guidance, and responding to cyber incidents. It supports both public and private sectors and promotes cybersecurity research and best practices to enhance France's digital resilience. Additionally, ANSSI collaborates with international partners to strengthen global cybersecurity efforts and address cross-border cyber threats.

Check Point Software Technologies

Check Point Software Technologies is a global leader in cybersecurity, offering advanced solutions to protect data and networks for businesses worldwide. Its comprehensive security products, including firewalls and threat prevention tools, help organisations safeguard against cyber threats and maintain data integrity. The company also provides ongoing threat intelligence and updates to ensure its solutions stay effective against evolving cyber threats.

Singapore

Cyber Security Agency of Singapore (CSA)

The Cyber Security Agency of Singapore (CSA) enhances national cybersecurity by developing strategies, supporting public and private sectors, and responding to cyber incidents. It also promotes cybersecurity awareness and collaborates internationally to strengthen Singapore's digital resilience. Additionally, the CSA invests in research and development to advance cybersecurity technologies and address emerging threats.

Grab

Grab is a leading technology company in Southeast Asia, widely recognized for its ride-hailing and digital payment services. The company places a strong emphasis on data security, implementing robust measures to protect user information and financial transactions. Grab integrates advanced security technologies and practices to ensure the safety and privacy of its users, reflecting its commitment to maintaining a secure and reliable platform across its diverse range of services.

Netherlands

National Cyber Security Centre (NCSC-NL)

The National Cyber Security Centre Netherlands (NCSC-NL) enhances national cybersecurity by providing guidance, threat intelligence, and support for addressing cyber incidents. It works with public and private sectors to develop strategies and promote best practices to protect the Netherlands' digital infrastructure. Additionally, NCSC-NL conducts regular training and exercises to improve the preparedness and resilience of organizations against cyber threats.

Booking.com

Booking.com, a leading online travel platform, focuses heavily on user data protection by investing in advanced cybersecurity measures. The company utilizes cutting-edge security technologies and practices to safeguard personal and payment information, ensuring that users experience a secure and private environment while booking accommodations and travel services. Additionally, Booking.com regularly reviews and updates its security protocols to adapt to emerging threats and maintain high standards of data protection.

India

Ministry of Electronics and Information Technology (MeitY)

The Ministry of Electronics and Information Technology (MeitY) is an Indian government agency responsible for advancing IT and electronics sectors. It develops policies to enhance digital infrastructure, drive innovation, and support e-governance, while also focusing on cybersecurity and data protection to improve public services and promote technological growth. Additionally, MeitY collaborates with industry stakeholders and international partners to address emerging technology trends and challenges.

Tata Consultancy Services (TCS)

Tata Consultancy Services (TCS) is a global IT services company that delivers comprehensive cybersecurity solutions to protect data across diverse sectors. It provides advanced services such as threat detection, risk management, and data protection, leveraging its extensive expertise to enhance security. TCS supports clients in safeguarding their digital assets and ensuring robust security measures as part of their broader IT and digital transformation strategies.

Timeline of Relevant Resolutions, Treaties and Events

Date	**Description of event**
1980	OECD Guidelines of the Protection of Privacy and Transborder Flows of Personal Data; issued the first international standards for data protection
1995	EU Data Protection Directive; the EU established foundational principles for data protection within its member states
2000	United Nations Global Compact; launched an initiative encouraging business to adopt responsible data privacy policies
2001	Council of Europe Convention on Cybercrime (Budapest Convention): the first international treaty addressing cybercrime was adopted
2004	APEC Privacy Framework; introduced a framework for consistent data privacy protection across its members
2007	OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy
2013	UN General Assembly Resolution 68/167 on the Right to Privacy in the Digital Age; affirmed that privacy rights must be protected online
2016	EU-U.S. Privacy Shield; framework to regulate data exchanges between EU and the U.S. established

2018	General Data Protection Regulation (GDPR); the EU implemented a comprehensive data protection law
2019	G20 Osaka Leaders' Declaration; emphasized data security through public-private partnerships
2021	OECD Recommendation on Enhancing Access to and Sharing of Data
2022	Declaration for the Future of the Internet; over 60 countries signed a declaration to promote a secure and open internet.
2023	UN Resolution on Cybersecurity and Personal Data Protection

Evaluation of Previous Attempts to Resolve the Issue

The history of addressing personal data security closely follows the development of technology. Early efforts were made in the 1980s with the OECD Guidelines on the Protection of Privacy, establishing the first international standards for data protection. Next, the EU Data Protection Directive (1995) outlined the legal basis of data protection throughout the territories of the European Union. This document primarily emphasized the need for strong privacy regulation.

In the 2000s, the theme was expanded to focus on cybersecurity and international partnerships. The Council of Europe Convention on Cybercrime (2001) which first addressed cybersecurity as a large-scale legal issue, highlighted the necessity of global cooperation. The APEC Privacy Framework (2004) and the OECD Recommendation on Cross-border Cooperation (2007) further stressed the importance of consistent data privacy protection and stronger cross-border enforcement.

The 2010s saw further development with the adoption of the EU-U.S. Privacy Shield (2016) and the General Data Protection Regulation (GDPR) (2018), which led to significant advancements in data protection and reinforced the role of public-private partnerships. The G20 Osaka Leaders' Declaration (2019) and the OECD Recommendation on Data Sharing (2021) emphasized the importance of data security in a globally connected world, promoting collaboration between governments and businesses.

More recently, the Declaration for the Future of the Internet (2022) and the UN Resolution on Cybersecurity (2023) have stressed the need for international cooperation and public-private partnerships to tackle emerging data security challenges. Despite the progress made, the rapid evolution of technology and the increase of cyber threats mean that these partnerships must continue to adapt and strengthen to effectively protect personal data.

Possible Solutions

Establishing a regulatory framework for data security standards can help align public and private sector practices to safeguard personal information. By setting universal requirements for data encryption, access control, and storage, this framework would facilitate better coordination and compliance across sectors.

Incentivizing private sector compliance through public-private partnerships is also essential; governments can offer benefits like tax breaks, subsidies, or certifications to companies that adhere to these standards. Joint training initiatives could further enhance data protection practices and build mutual accountability.

In addition, fostering international cooperation is crucial for addressing cross-border data issues. Through collaboration with global organizations, nations can create shared guidelines for data transfer and protection, enabling smoother and safer data flow. This approach would strengthen global data security efforts, ensuring that both sectors work together to protect personal data from emerging threats.

Bibliography

1. United Nations Office on Drugs and Crime
   Global Cybersecurity Index (GCI) 2017. United Nations, 2017
2. Ponemon Institute
   Cost of Data Breach Study: Global Analysis. UNDRR, 2023
3. Cybersecurity and Infrastructure Security Agency
   CISA, U.S. Department of Homeland Security, www.cisa.gov
4. Council of Europe Convention on Cybercrime
   Council of Europe, 2001, https://www.coe.int/en/web/cybercrime/the-budapest-convention
5. Declaration for the Future of the Internet
   Global Partnership on Artificial Intelligence (GPAI), 2022, https://futureoftheinternet.org
6. Cybersecurity in Asia-Pacific: Insights and Frameworks
   Asia-Pacific Economic Cooperation (APEC), 2004, www.apec.org