National and Enterprise Cybersecurity Countermeasures

Zichun Zhao(✉)

Information Technology, The University of Sydney, Sydney, Australia
zzha8472@uni.sydney.edu.au

Abstract. With the development of information technology, the number of cyber-threats and cyber-attacks has increased significantly. Based on research cases in the United States and Japan, this paper analyzes the current cybersecurity situation, government and corporate responses to cybersecurity countermeasures, and the corresponding system security and asset-liability. Results demonstrate the government and enterprises should cooperate against cyber security attacks.

Keywords: component · cyber-attacks · cybersecurity situation · cybersecurity countermeasures

1 Introduction

Because of the rapid development of information technology, people's lives and work can break the constraints of distance and time, thus improving work and production efficiency and promoting the economy and social progress [1]. However, advanced information technology has also brought negative impacts. With the increasing maturity of artificial intelligence, big data, 5G, and other technologies, a growing number of cyber threats and attacks are faced by countries and enterprises. Cyber-attacks were included in the top five global risks for the first time in the World Economic Forum's Global Risks Report 2018, making it the third most important global risk factor in 2018, and the Covid-19 also facilitated cyber-attacks. Against the backdrop of the ongoing global epidemic, companies and universities worldwide changed from offline offices and education to online work, classes, and online socializing. These activities have led to a significant reliance on critical digital infrastructure. It expanded the scope of cyber-attacks several times, with ransomware, phishing attacks, data breaches, etc., and increased the number of cyber-attacks by hacker groups on health care systems and national health institutions where data is sensitive. In this paper, the United States and Japan are selected for discussion, focusing on how governments and companies should respond to cyber threats in the current context and their corresponding responsibilities.

C. F. Peng et al. (Eds.): MMET 2022, ASSEHR 703, pp. 180–187, 2023.
https://doi.org/10.2991/978-2-494069-51-0_24

2 U.S. Cybersecurity Case

2.1 Background Information

U.S. intelligence agencies assessed global threats in 2013 and identified cybersecurity attacks as the number one global threat. In 2018, the United States suffered multiple cyber-attacks, where governments, businesses, and individuals were significantly impacted. Although governments and companies increased their focus on cybersecurity and invested more money, the number of cybersecurity incidents increased, and their corresponding impacts cannot be ignored [2]. In June 2018, hacking groups were identified by Symantec Corporation to conduct cyber-attacks against telecommunications, satellite communications, military systems, and geospatial capture imaging services in the United States and Southeast Asian countries. In September 2018, Facebook was attacked, exposing the personal private information of more than 50 million users at risk. In November 2018, the U.S. government announced that repeated attempts by hackers had compromised the U.S. election system. In March 2019, Atlanta was subject to a cyberattack when information systems and official websites went down, and the exercise of government functions was severely compromised. In July 2019, much of customers' personal information owned by Bank of America First Capital Financial Corporation was learned by hackers. In April 2020, the U.S. Small Business Administration (SBA) announced that a PII data breach disclosed 8,000 emergency loan applicants' interests. In June 2020, Amtrak customer PII was stolen, and hackers accessed Amtrak guest rewards accounts. In September 2020, ransomware attacked a school in Nevada, U.S. In May 2021, Shankolonier, the largest fuel transportation pipeline in the U.S., was cyber-attacked, and 5,500 miles of pipeline were damaged to suspend delivery service.

These are just a few cybersecurity incidents affecting the United States government and businesses over the past couple of years, but the cybersecurity threat grows daily.

In addition, data related to multinational companies need to transfer and flow between different regions, and there are differences in regulatory requirements in different countries and regions. As countries and regions around the world begin to pay attention to and regulate cross-border data, multinational companies have begun to face various challenges in conducting global business with cross-border data flows. For example, the U.S. supports free-flowing cross-border data governance rules, while the EU supports intra-regional data flows with high levels of extra-regional protection requirements, and negotiations between the EU and the U.S. on cross-border data flows have oscillated between consensus and disagreement until March 2022, when the U.S. and the EU agreed on a new Trans-Atlantic Data Privacy Framework reached an agreement in principle (Table 1).

Meanwhile on February 2022, the European Commission officially released the Draft Data Act, which aims to unlock the economic and social potential held by data and technologies that are consistent with EU rules and values. The bill introduces new requirements around data sharing, public agency access, international data transfers, cloud switching and interoperability, with significant potential implications for the global digital economy and data governance (Table 2).

Table 1. Cross-border data business challenges (Table credit: Original)

Data Governance Rules Fragmentation	The fragmentation of data governance rules among countries is exacerbated by the wide divergence in the ways and means of governance of cross-border data across countries.
Vague and uncertain security exceptions	Security exceptions are a basic prerequisite for countries to support cross-border data flows, but vague and uncertain security exceptions have a large impact on multinational companies.
System design deviates from practice	Data governance involves both security and development dimensions, but there is currently no mature model to follow globally.
Globalization and Localization Dilemma	Globalization is a fundamental characteristic of multinational corporations, and except for the United States, which generally supports the free flow of data across borders, all other major countries and regions have varying degrees of data localization constraints.

Table 2. Core elements of the draft data law (Table credit: Original)

Data access and sharing rights	Detailed explanation of the rights and obligations of users, third parties, and small, medium and large companies in terms of data access and sharing
Contractual Obligations	Clarified the realization path of data sharing among enterprises to promote the data circulation and sharing among enterprises in the industrial value chain
Used by public institutions	Public institutions have the right to access and use relevant necessary data held by the private sector (except micro and small businesses) in response to emergencies such as terrorist attacks, public health, natural disasters, or to fulfill legal obligations
Cloud Switching and Interoperability	Data processing service providers need to take measures to remove commercial, technical, contractual or organizational barriers to switching service providers, and should make their interfaces freely available to the public and ensure interoperability specifications or compatibility with European standards
International transmission of data	Data processing service providers shall take all reasonable technical, legal and organizational safeguards, including contractual arrangements, to prevent the unlawful transfer of non-personal data to non-EU or non-EEA Member States

The President of the United States believes cyber-attacks pose a severe threat to national security. In this situation, the U.S. state and businesses should pay more attention to cybersecurity and use several countermeasures to deal with threats.

2.2 National Cybersecurity Countermeasures

U.S. government needs to strengthen cybersecurity to deal with the current cybersecurity threats [3]. The U.S. invested $3.4 billion in cybersecurity in 2012, rose this fund to $10.3 billion in 2013, and this funding increased gradually until 2020. In the proposal made by the U.S. House of Representatives Appropriations Committee, the attention and capacity reserve should be developed to respond to cyber-attacks. The committee also specifically proposed a budget of $2.42 billion for CISA for the fiscal year 2022, $400 million higher than CISA's budget for 2021, to address cybersecurity-related issues. In addition, the government and enterprises should actively remove the information-sharing barriers between them. The executive order also makes requirements for each IT service provider: the government has the right to request providers to disclose relevant security data and report whether they are under cyber-attack. Information sharing can effectively prevent cybersecurity incidents, improve response capabilities, and protect government and corporate information security.

The U.S. government should enhance its ability to train cybersecurity personnel. U.S. President Joe Biden emphasizes fostering cybersecurity talents, and several government officials are involved in cybersecurity. In addition, the U.S. government provides high salaries to attract these talents. According to Reuters, Biden began recruiting a group of national security veterans with deep cyber expertise to assist in responding to cybersecurity incidents. In May, the U.S. government released plans to recruit 200 cybersecurity professionals to address cyber threats and attacks within two months.

The U.S. government should also improve cybersecurity development techniques and strengthen cybersecurity modernization in government departments. To deal with new cybersecurity threats, the U.S. needs to keep pace with artificial intelligence technology and economic digitization as they continue to advance. On the one hand, Biden signed an executive order requiring department heads to adjust existing departmental structures and programs, prioritize cloud technologies, and apply modern cybersecurity tools. Multiple authentications must be used to ensure national cybersecurity. Meanwhile, the U.S. Department of Homeland Security recruited professionals to develop a platform on 5G and IoT situational awareness, with the potential to enhance the ability to predict cyber threats. It could efficiently discover 5G components and risky IoT devices, find vulnerabilities, and track cyber-attacks.

2.3 Enterprise Cyber Security Countermeasures

To cope with cyber security threats, enterprises should establish security departments, invest more in security prevention and allocate more resources to cyber security. Network security incidents occur increasingly frequently, and many corporations have set up their security departments to manage enterprises' network security from formal control, informal control, and technical control. Dell's survey showed that most IT decision-makers worldwide have or plan to enhance their investment in cybersecurity and employee education [4]. Employees' accidental operations can easily lead to cyber threats, so educating employees about security can effectively reduce related risks through phishing and email, for example.

Companies should cooperate with the government to promote cybersecurity under the guidance and share cybersecurity intelligence with the government and other companies. Businesses are an essential source of a country's economy, thus making their cybersecurity critical. Also, the government encouraged companies to share cybersecurity, actively removing information-sharing barriers between the government and companies and reducing potential risks of cybersecurity attacks. The "2020 Counterintelligence Strategy for America," signed on January 8, 2020, has already begun to align the U.S. government's cyber information sharing practices with businesses.

Enterprises should adopt active defense strategies to deal with cyber security threats. In the past years, enterprises usually used traditional passive defense strategies: firewalls, intrusion detection technologies, and information encryption technologies can detect and stop cyber-attacks, but they cannot manage deeply disguised cyber-attacks. The U.S. government agrees and incentivizes companies to apply more active defense strategies to address cybersecurity threats. Active defense refers to proactive cybersecurity measures between traditional passive defense and offense [5]. By selecting and implementing appropriate proactive defense strategies, an organization can improve its ability to combat cyber threats.

2.4 Responsibility for Security Systems and Assets

U.S. enterprises own the majority of security system development and production departments and nearly 90% of critical cyber infrastructure in the nation. Security systems are composed of four main components: assets, vulnerabilities, threats, and incidents, to protect information assets and build proactive security operations capabilities. At the same time, the government plays a pivotal role in using and promoting security systems. The government holds many information assets and controls critical infrastructure and server production. The probability of cyber security incidents is increasing, so both governments and enterprises are responsible for using security systems, therefore maximizing their cyber security.

Both national and corporate assets are critical economic lifelines for the country. Economic motivations are the reason for a large portion of cyber-attacks so that the financial sector can be easily targeted. In 2012, 26 major U.S. banks suffered consecutive DDoS attacks over four months, resulting in significant financial losses. Cyber-attacks can also target valuable intellectual property, and securing information assets is essential to maintaining a sound market economy. In 2013, the Intellectual Property Committee reported that IP-intensive industries cover 20% of U.S. jobs and that theft of industry IP can negatively impact other industries and pose a threat to U.S. economic security. Despite varying cybersecurity capabilities across sectors, problems within an industry can significantly affect the whole. The economic threat posed by cyber-attacks has already led to a significant risk to U.S. security. Recent estimates suggest that the cost of a cyber-attack on a private business is between 0.64% and 0.9% of U.S. GDP. If these estimates are accurate, cyber-attacks cost the United States between $120 billion and $167 billion.

As cyberattacks proliferate, this trend is likely to continue if left unchecked. Cybersecurity can only be indeed achieved if governments and businesses share responsibility for cybersecurity and cooperate to promote it since both play an essential role in addressing cyber threats.

3 Japan Cybersecurity Case Study

3.1 Background Information

As one of the most advanced countries in information technology and one of the most concerned countries with information security, Japan has implemented information technology for national economic sectors and social life for a long time. However, since 2020, cyber hackers have continuously attacked various Japanese companies. International security firms surveyed security departments of large companies in multiple countries, finding that more than half of the 200 Japanese companies surveyed experienced cyberattacks. More seriously, 33 of them paid an average of 123 million yen to criminal networks to prevent the leakage of password-protected data. The cyber-attack caused a global business interruption that severely impacted Honda's business operations. A Japanese video game company was fined a ransom of 1.1 billion yen for the stolen data. Japan is facing more and more cyber security threats and attacks with age. The country and companies should adopt appropriate strategies to address cyber security issues.

3.2 National Cybersecurity Countermeasures

Japan should strengthen its communication and cooperation with other countries to deal with the cyber security problem. Since the cybersecurity network problem has become a non-traditional security issue worldwide, global collaborations between countries can effectively combat cybersecurity crimes and maintain cybersecurity [6]. In addition to cooperation, Japan also provides cybersecurity services to enhance its national influence. Japan and the United States engaged in multi-level dialogue and collaboration on both strategic and policy fronts. Moreover, Japan developed bilateral cybersecurity cooperation with European countries such as the UK and France to share experience in governing cybersecurity and combating cybersecurity criminals. At the multilateral level, Japan joined multilateral institutions to facilitate cybersecurity governance in its own country. On the other hand, against the backdrop of the global outbreak of Covid-19, the Japanese government has teamed up with ASEAN countries to undertake a cybersecurity project to enhance national capabilities to deal with cyber threats, while Japanese cybersecurity experts mentor ASEAN professionals to carry out the project.

The country should focus on cultivating talents in cybersecurity, but a severe shortage of cybersecurity personnel exists in Japan. Figures from the Ministry of Economy, Trade, and Industry (METI) showed that in 2020, the shortage of personnel in cybersecurity would be as high as 193,000, meaning half of the Internet companies lack information security engineers. According to the international e-A.M. Advisory Bureau survey, Japanese cybersecurity professionals have skill gaps, from chief security officers to analysts. All of these positions face understaffing problems. The government has enacted policies to strengthen talent training to solve the issues. In March 2017, Japan released the Cybersecurity Human Resources Development Plan, which emphasizes that maintaining cybersecurity is a costly expenditure but contributes to creating new business value, improving companies' international competitiveness, and encouraging employees to raise cybersecurity awareness and adopt cybersecurity measures. Japanese government departments conducted training courses for cybersecurity personnel to enhance their abilities. The Ministry of Economy and Production also established a Center of Excellence for Cybersecurity under the Information Technology Promotion Bureau to provide mid-career training and senior management training for human resources.

3.3 Corporate Cybersecurity Countermeasures

Japanese companies should put more effort into cybersecurity research and development to cope with their current cyber security situation [7]. Japanese companies have developed new artificial intelligence technologies that can automatically predict cyber-attacks and examine the impact after being subjected to cyber-attacks. Fujitsu Japan has developed new artificial intelligence technology that can screen and capture attack logs from operation logs and then display them in real-time, processing them in a timely and effective manner to protect corporate data security. It can also extend the database by extracting a small amount of attack data while retaining attack characteristics. The new technology, combined with Deep Tensor AI technology, has been conducted rigorous testing by Fujitsu on a cyber-attack elicitation platform jointly operated with the Japan Information and Communication Research Agency to address enterprise cyber security issues.

The basic principle of Japan's cybersecurity strategy is to promote collaboration between the government and enterprises. In 2006, the Japanese government adjusted the cooperation model and gradually changed from private-led to government-led, and the role of the government changed from participant to leader. The Cybersecurity Strategy (2015 edition) pointed out that "all subjects in cyberspace should fulfill their respective responsibilities and obligations and strengthen integrated cooperation". The Cybersecurity Strategy (2018 edition) put forward the essential roadmap for cybersecurity construction and cross-sectoral measures for the government-business cooperation model, emphasizing the global importance of government-civilian cooperation in cybersecurity. At present, Japan has carried out comprehensive and practical official-civil collaboration mainly in cybersecurity system co-construction, cybersecurity information sharing, and cybersecurity resource mutual education and sharing, actively promoting cybersecurity system and establishing a large-scale and complex cybersecurity sharing mechanism.

3.4 Security System and Asset Responsibility

Security systems can detect cyber-attacks and handle them promptly to protect the nation's cyber security. Both national and corporate assets are related to the country's economy and remain essential. Therefore, regardless of the change in Japan's cybersecurity strategy and layout, maintaining cybersecurity is an indispensable shared responsibility between the government and enterprises to protect the security of Japan's information society.

4 Conclusion

By analyzing cybersecurity cases in the United States and Japan, cybersecurity threats have affected governments and enterprises in various countries worldwide. Cyber threats continue to grow despite the country's emphasis on cybersecurity. To deal with the current cybersecurity situation, the government and enterprises should strengthen cooperation to share cybersecurity information and responsibility, thus reducing cybersecurity incidents. Both the government and enterprises should support cybersecurity research, develop key technologies and maintain cyberspace equipment. Training cybersecurity talents and recruiting more cybersecurity talents is also essential to combat cyber threats.

References

1. Xin, X. (2014). Network security status quo and countermeasures. Network Security Technology & Application, 07.
2. Spidalieri, F. (2015). State of the States on Cybersecurity. Pell Center for International Relations.
3. Contreras, J. L., DeNardis, L., & Teplinsky, M. (2012). Mapping today's cybersecurity landscape. Am. UL Rev., 62, 1113.
4. Watkins, B. (2014). The impact of cyber attacks on the private sector. Briefing Paper, Association for International Affair, 12, 1-11.
5. Bartlett, B. (2018). Government as facilitator: How Japan is building its cybersecurity market. Journal of Cyber Policy, 3(3), 327-343.
6. Aikawa, W. (2020). Japan's Cybersecurity Policy. In Telecommunications Policies of Japan (pp. 133–148). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-1033-5_7
7. Nitta, Y. (2014). Review of the Japan Cybersecurity Strategy. ISPSW Strategy Series: Focus on Defense and International Security, Issue, (290).