FORUM:	Commission on Science and Technology Development
ISSUE:	Measures to Combat International Cybersecurity Attacks
STUDENT OFFICER:	KyungChan Min
POSITION:	Deputy President of Commission on Science and Technology Development

Introduction

The rapid advancement of technology is identified as a primary factor contributing to the escalation of international cybersecurity attacks. The increasing complexity and expertise of cybercriminals in exploiting vulnerabilities within digital systems are evident as technology continues to advance. The susceptibility of our networks to cyberattacks is heightened by their interconnectivity and the dependence on digital infrastructure across diverse sectors, including finance, energy, healthcare, and transportation.

The prevalence of cybersecurity attacks has emerged as a significant concern in the contemporary global landscape characterized by extensive interconnectivity. The proliferation of technology and the internet has led to a heightened vulnerability to cyber-attacks, posing significant concerns. The aforementioned attacks present significant challenges to the overall stability of global systems. In order to protect national interests and maintain the integrity of the interconnected global community, it is imperative to implement appropriate measures to counter international cybersecurity attacks. Various entities, including government institutions, private enterprises, and individuals, face susceptibility to cyber threats that possess the potential to compromise sensitive data, disrupt essential infrastructure, and pilfer valuable intellectual assets. An instance of a cyberattack targeting a power grid has the potential to result in the disruption of electricity provision to an entire city or region, leading to extensive blackouts and substantial disturbances to critical services such as healthcare facilities, communication networks, and transportation infrastructures.

Background

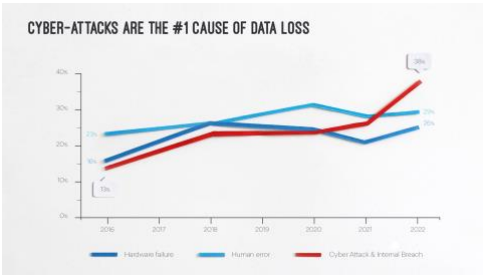
Financial loss due to Cyberattacks from 2017 – 2021

In the last ten years, there has been a notable rise in both the occurrence and intricacy of cybersecurity breaches, thereby presenting an escalating peril to individual users. The scope of these attacks varies, encompassing instances where individual hackers aim to compromise personal information or financial assets, as well as situations where cybercriminals employ sophisticated methods to exploit vulnerabilities in online platforms and devices. The potential ramifications for individuals can be severe, encompassing more than just monetary setbacks. Instances of personal data breaches have the potential to result in identity theft and the unauthorized acquisition of confidential data. Furthermore, it is worth noting that individuals have the potential to encounter reputational harm and a decline in trust in online services, which can have significant implications for their digital existence and interpersonal connections. In light of the ever-growing digital environment and the pervasive integration of technology into our everyday routines, it is imperative for individuals to accord utmost importance to cybersecurity measures. By doing so, they can effectively shield their digital identities and shield themselves from potential risks and detrimental consequences. Failure to prioritize cybersecurity can expose both individuals and organizations to the pervasive and constantly evolving risks present in the digital domain.

Problems Raised

Data Leakage

The compromise of sensitive information has emerged as a significant issue resulting from cybersecurity attacks. Instances of unauthorized access to government databases, corporate networks, and educational institutions have resulted in the illicit acquisition and improper utilization of personal and classified data. Not only does this expose individuals to the potential dangers of identity theft and financial harm, but it also presents a significant risk to the security of the nation. Although nations may experience a relatively smooth recovery process, ordinary individuals who fall victim to such attacks may encounter significant financial setbacks, including the necessity of engaging in extensive legal and financial assistance in order to regain stability.



Key Factors of Data Loss

Lack of International Cooperation

The absence of global collaboration and synchronization in countering cybersecurity attacks poses difficulties as a result of the divergent policies and strategies implemented by different nations in confronting these vulnerabilities. The variations in environmental conditions and network infrastructure pose challenges in achieving a cohesive and synchronized response. As a result, it is possible that there could be delays or conflicting perspectives in the dissemination of necessary information aimed at mitigating the occurrence of comparable attacks in the future. Nonetheless, the significance of collaboration persists as it facilitates the sharing of defensive strategies and methodologies, thereby assisting nations in enhancing their defensive capabilities within their distinct environments and network infrastructures, despite any disparities that may exist.

.

Development of New Technology

As new technologies emerge and cybercriminals find more sophisticated ways to exploit vulnerabilities, it becomes crucial for governments and organizations to constantly update their cybersecurity strategies and systems. Failure to keep pace with these advancements can leave individuals, businesses, and governments vulnerable to cyber attacks. It is therefore essential for countries to invest in research and development, as well as foster collaboration and knowledge-sharing among industry experts and organizations, in order to stay one step ahead of cyber threats. So that by staying one step ahead of cybercriminals, countries can safeguard their citizens, businesses, and critical infrastructures from dynamic cyberattacks.

International Actions

Budapest Convention

The Budapest Convention is a globally recognized international treaty that seeks to strengthen intergovernmental collaboration in the detection, investigation, and prosecution of cybercrimes. The convention establishes guidelines pertaining to legislation, law enforcement practices, and mutual assistance, thereby aiding countries in addressing cyber threats through a cohesive global approach. Cyberattacks frequently emanate from transnational regions, thereby necessitating collaborative efforts among nations to effectively combat this pervasive global menace. Through the establishment of such agreements, nations have the opportunity to collaborate and exchange knowledge, expertise, and resources in order to strengthen their capabilities in the field of cybersecurity.

Budapest Convention

This process can facilitate the identification of emerging threats, the analysis of attack patterns, and the formulation of suitable defense strategies.

International Organization for Standardization

The International Organization for Standardization (ISO) has released several cybersecurity standards, such as ISO/IEC 27001, which presents a methodical framework for information security management, and ISO/IEC 27002, which presents recommended guidelines for implementing the controls outlined in ISO/IEC 27001. These standards assist organizations on a global scale in implementing a comprehensive cybersecurity framework, thereby diminishing the probability of achieving successful cyberattacks. Through the adoption and implementation of these standards, nations have the potential to bolster their overall cybersecurity stance, thereby increasing the complexity for cyber assailants to exploit vulnerabilities. Furthermore, the implementation of standardized regulations across multiple nations would greatly enhance the exchange of information, promote compatibility among different technologies, and foster collaborative efforts in responding to incidents.

The ISO

Cybersecurity Capacity Buildings

Numerous nations, encompassing both advanced and emerging economies, allocate resources towards the establishment of cybersecurity capacity building initiatives with the aim of bolstering their capacities to effectively counter cyber threats. These programs prioritize the education and skill development of law enforcement personnel, the formulation of effective cybersecurity strategies, the establishment of national computer incident response teams (CIRTs), and the promotion of public awareness. These programs enhance the capabilities of nations, thereby contributing to a collective defense against cybersecurity attacks of an international nature. Investment and development initiatives play a crucial role in the prevention and mitigation of cybersecurity attacks on a global scale.

Key Players

United States of America

The United States, being a prominent global leader in the field of technology and a significant target of cyber attacks, assumes a vital role in the efforts to address and mitigate cybersecurity threats. The nation has successfully cultivated sophisticated cybersecurity capabilities and actively promotes

collaborative efforts on an international scale to bolster global cyber resilience. The United States of America has established several organizations with a primary focus on cyber-related matters, including the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA). These organizations strive to improve cybersecurity practices, foster collaboration with industry partners, and safeguard critical infrastructure against cyber threats. In general, the United States of America fosters a climate that promotes and supports research and innovation within the realm of cybersecurity, with the aim of maintaining a competitive edge against constantly evolving threats. The allocation of resources towards research funding, cybersecurity competitions, and educational programs is given precedence in order to cultivate a proficient workforce and foster advancements in the field of cybersecurity.

China

The Great Firewall of China

China has emerged as a significant participant in the field of cybersecurity as a result of its notable technological progress, swift digital transformation, and extensive online environment. Nevertheless, China's approach to cybersecurity diverges from that of the United States, with notable disparities evident in several key initiatives. China implements a comprehensive internet censorship and monitoring system known as the "Great Firewall," which effectively regulates access to foreign websites and services. The notion of "Internet Sovereignty" is underscored, wherein a country asserts its authority to govern the realm of cyberspace within its territorial boundaries and advocates for a managed and supervised internet environment. In general, China's perspective on cybersecurity is centered on the preservation of societal equilibrium, safeguarding national interests, guaranteeing information security, and regulating the transmission of digital data within its territorial boundaries. The focal point lies in striking a balance between the preservation of cybersecurity and the promotion of internet openness, while concurrently implementing rigorous regulations and control measures.

Possible Solutions

Strengthening International Cooperation

The exchange of information and collaborative efforts between public and private entities can significantly contribute to the prevention of cyberattacks. The act of disseminating threat intelligence, attack patterns, and vulnerabilities can facilitate the readiness and safeguarding of other systems against comparable threats. Therefore, through the collaborative sharing of resources, technology, and

intelligence, there is potential to significantly augment the global capacity to address and mitigate international cybersecurity threats. In general, the implementation of more stringent regulations and enhanced international collaborations represents a viable approach to addressing the issue of international cybersecurity attacks. These measures serve to establish explicit guidelines and expectations for organizations, foster a sense of accountability, and facilitate the exchange of knowledge and resources.

Law Enforcement Procedures Across the EU

Promotion of Secure Coding Practices

Secure coding practices encompass the utilization of optimal methodologies and principles in the development of software and applications, thereby fortifying their resilience against potential cyber threats. Organizations can establish a robust cybersecurity framework by prioritizing secure coding practices, thereby mitigating the risk of exploitable vulnerabilities for potential attackers. Governments have the potential to engage in collaborative efforts with industry experts in order to formulate comprehensive and contemporary secure coding standards that can be universally implemented. These standards would serve as a set of guidelines for software developers, ensuring adherence to appropriate coding practices throughout the development lifecycle. Examples of existing standards in the field encompass the OWASP secure coding practices and the CERT secure coding guidelines.

Glossary

Cybersecurity

The practice of defending computers, servers, mobile devices, electronic systems, networks, and data from digital attacks or unauthorized access.

Malicious actors

Individuals or groups engaged in unauthorized or illegal activities, including cybercriminals and state-sponsored hackers.

Vulnerabilities

Weaknesses or gaps in computer systems and networks that can be exploited by malicious actors.

Sources

"Top 30+ Ethical Hacking Tools and Software for 2023 | Simplilearn." Simplilearn.com, 3 Sept. 2012, www.simplilearn.com/top-5-ethical-hacking-tools-rar313-article.

"What Is Cybersecurity?" Cisco, www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

"Common Cybersecurity Issues That Organizations Face | Maryville Online." Maryville Online, 20 Feb. 2017, online.maryville.edu/blog/cybersecurity-issues.

"Secure Industrial Facilities." siemens.com Global Website, www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html.

"Biggest Cyber Security Challenges in 2023 - Check Point Software." Check Point Software, www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/biggest-cyber-security-challenges-in-2023.

"What Is a Website Defacement Attack | Examples and Prevention | Imperva." Learning Center, www.imperva.com/learn/application-security/website-defacement-attack.

Carreiro, Alison. "8 Common Hacking Techniques That Every Business Owner Should Know About." OceanPoint Insurance, 3 Feb. 2020, www.oceanpointins.com/ri-business-insurance/cyber-liability-insurance/8-common-hacking-techniques.

"IBM Policy." IBM Policy, www.ibm.com/policy/to-combat-cross-border-cyber-threats-cooperation-is-key."Hacking Examples (2023): The 10 Worst Attacks of All Time." SoftwareLab, softwarelab.org/blog/hacking-examples.

"Hacking Examples (2023): The 10 Worst Attacks of All Time." SoftwareLab, softwarelab.org/blog/hacking-examples.

"ISO - International Organization for Standardization." ISO, 19 July 2023, www.iso.org/home.html.

"ISO/IEC 27001 Standard – Information Security Management Systems." ISO, 30 May 2022, www.iso.org/standard/27001.

"ISO/IEC 27002:2022." ISO, 26 Mar. 2018, www.iso.org/standard/75652.html.