1 Differences in Global Cybersecurity Culture and Practices

A Social and Cultural Analysis of The United States, The United Kingdom, China, and Taiwan

Megan Erasmus

Department of Computer Science, Western Washington University, Bellingham, WA, USA, erasmum@wwu.edu

ABSTRACT

The United States, the United Kingdom, China, and Taiwan each exhibit unique cybersecurity cultures shaped by social, cultural, and geopolitical factors.

In the United States, individualism, innovation, and technology optimism influence the culture, with a strong focus on personal responsibility. The United Kingdom emphasizes practical solutions, legal compliance, and education. China's collectivist culture fosters shared responsibility and adherence to government regulations. Taiwan's geopolitical context underscores national security concerns.

These distinct characteristics drive diverse approaches to cybersecurity, ranging from individualism and innovation to collectivism and government authority. Understanding these differences is crucial for effective global cybersecurity strategies.

CCS CONCEPTS

Security and privacy • Social and professional topics

2 Introduction

Cybersecurity culture refers to the idea that organizations or groups have a collective set of attitudes and responsibilities related to cybersecurity. This culture can specifically refer to the standard of values, beliefs, norms, and policy adherence that are upheld at every level. Effective cybersecurity culture expresses a strong commitment to the protection of systems, projects, and sensitive information on an individual and organizational level, which leads to prevention and preparedness of cybersecurity risks from doing harm.

On a broader scale, national cybersecurity culture is affected by the specific governmental policies and rulings, international regulations, and overall social culture of that country. This includes the overarching social understanding and education of secure cyber practices. Countries that display strong cybersecurity culture often have a collectivist attitude, giving individuals a sense of responsibility within society to maintain a standard of security which propagates a culture of accountability for being secure. The cybersecurity practices of countries who have higher rates of education are often stronger [1], with higher education and exposure to the digital world leaving individuals with greater knowledge of the importance of privacy and security digitally. These examples of social and cultural factors and more all contribute and can affect cybersecure practices on a global level.

3 Social and Cultural Factors for the United States

The cybersecurity culture of the United States is influenced by several important American cultural aspects. The nation has a strong history of progress and innovation, with the US leading in technological advancements for years. Because of this, there has emerged a culture that values technology and its potential to improve people’s lives. This positive lens over technology, however, introduces a sense of naïve optimism that can leave cybersecurity as more of an afterthought.

Another element that contributes to the cybersecure culture of the United States is the emphasis on individualism within American society. Americans value freedom, independence, and individualism [2], which can occasionally disagree with the necessity for adherence to security measures. Within an individualistic society, individuals can be inclined to feel a sense of self confidence in the degree of security currently implemented, failing to consider that community members may not be upholding the necessary security measures to uphold the safety for the whole group. Individualism can also contribute to individuals wanting security measures to be implemented in a specific way, therefore, there might be some reluctance to adopt security protocols that could be seen as infringing upon the individual's thoughts, rights, or privacy.

Moreover, due to the entrepreneurial spirit prevalent in the US there can be a focus on innovation at times, at the expense of prioritizing security. These factors have collectively shaped a cybersecurity culture in America that places importance on innovation and personal freedoms but may exhibit cautiousness towards security matters.

In terms of legality, there are several pieces of legislature that impose restrictions on American Cybersecurity and information protection. FISMA, or the Federal Information Security Management Act, was enacted in 2002. FISMA defines standards for protection of government information and requires specific security procedures and programs to do so [3]. CISA, or the Cybersecurity Information Sharing Act, was enacted in 2015 to provoke sharing of information regarding the investigation of cyberattacks [4]. Sharing information about attacks gives situational awareness to those given this information and can increase effectiveness and speed of a response to these attacks. HIPAA, the Health Insurance Portability and Accountability Act, was enacted in 1996 and federally created national standards for the protection of protected health and personal identifying information (PHI and PII) [5] HIPPA created a stricter set of guidelines on data protection, forcing organizations who handled PHI or PII to increase their cybersecurity measures to prevent this data from being leaked. These legal regulations force a new standard of security throughout the country, one that previously was not required by anyone to follow, increasing the national security standard.

The American ideology of independence and freedom can disagree with the concept of cybersecurity, but at the same time it can foster an individual yearning for protection over what is personal. The combination of American ideology and imposed governmental regulations on cybersecurity gives a diverse culture of cybersecurity, with levels of security having the ability to be flexible within the legal requirements and regulations.

4 Social and Cultural Factors for the United Kingdom

The United Kingdom has a distinct set of factors that contribute to its cybersecurity culture. One aspect is the historical British idea of structure, pragmatism, and problem-solving. This British ideology is prevalent in their approach to cybersecurity, where consideration is put into risk management, threat evaluation, and being solution ready. This mindset encourages proactivity, with organizations and individuals encourages to continuously evaluate threats, consider risks, and take preemptive steps to reduce cyberattacks. [6]

The UK's school and educational system has a strong focus on science, technology, engineering, and math (STEM) subjects. The UK is also known for having various world-renowned Universities that uphold a high standard of educational excellence. The high education standard allows for a higher number of individuals to become educated professionals, many of which becoming professionals in cybersecurity. These factors contribute to a thoughtful cybersecurity culture. Additionally, the government actively supports efforts to promote cybersecurity education and awareness, helping the UK maintain a strong and educated collective cybersecurity culture.

The legal system in the UK also plays a large role in shaping the cybersecurity culture there. The NCSC, or the National Cyber Security Centre, acts as a bridge between the cyber industry and the government, acting as an extremely helpful resource for management of cybersecurity principles [7]. The UK GDPR, General Data Protection Regulation, has strict expectations regarding acting and managing risks and threats. The 2018 Data Protection Act also provides strict regulation on how data should be handled and ensures appropriate safety for personal data.

The UK’s general socio-cultural ideology of practicality, high educational standards, and cohesion between industry and government all contribute to a well-rounded national focus on secure cyber culture and implementation of cybersecurity.

5 Social and Cultural Factors for China

The Confucian history of China is visible in many cultural aspects, including their cybersecurity culture. Values such as respect for authority, adherence to rules and authority, and a sense of duty towards the greater societal good are key aspects of Confucianism. In the realm of cybersecurity, these values show adherence to rules and regulations to protect information. Chinese individuals are inclined to follow guidelines set by authorities as it aligns with historical core cultural values to do so to ensure safety of the greater good. Due to rapid technological innovation and advancement in China, specifically with the rise and success of the BAT trio (the search engine Baidu, ecommerce Alibaba, and technology company Tencent), there have been a rise in advancements in cybersecurity and digital safety [8]. With China becoming more prevalent in the technology and cyber world, it is evident that there is much encouragement for further investment in cybersecurity and secure principles, committing to a welfare of the industry.

Legal regulations that have been set regarding cybersecurity have been successful, due to the previously mentioned cultural norm of adherence to authority and regulation. Chinese Cybersecurity Law, more formally known as the Cybersecurity Law of the People’s Republic of China, was enacted to tighten constraints regarding data protection and cybersecurity. Within this law are many articles, each proposing differing regulations. Article 27, for example, regulates network infringement resulting in endangerment of network security, and prohibits stealing network data [9].

China’s Confucianist history’s core values allow the regulations set by authorities to be successfully adhered to, emphasizing individual responsibility towards maintaining of the country’s security. The rise of their technology industry and consistent growth of cybersecurity culture allows China to have a successful and secure culture regarding cybersecurity and data protection.

6 Social and Cultural Factors for Taiwan

The complex geopolitical relationship between Taiwan and China shapes the country’s social and cultural factors. This relationship allows for a strong emphasis on national security and cyber defense, preventing unwanted access to important national information. The tense security concerns of Taiwanese government stem from this fear of data leakage, as if sensitive information were to be exposed, there could be potentially catastrophic results.

Much like China, the Confucian values that have prevalence in Taiwanese culture contribute to its cybersecurity culture and practices. Respect for authority to benefit the greater good. as advocated by Confucianism, still applies strongly in Taiwan. Consequently, Taiwanese citizens follow a strong inclination to adhere to government regulations and guidelines, meaning adherence to regulations related to cybersecurity [10]. The commitment to social order and national stability is often extended to the digital realm, where following cybersecurity measures is seen as a collective responsibility to protect the nation's best interests.

Taiwanese legislation such as the Cybersecurity Management Act for governmental agencies and those providing critical support to the country’s infrastructure [11] stipulate a standard for the country that is closely followed by the Taiwanese citizens, despite the act not being mandatory for other agencies and organizations.

In recent years there has been much improvement in the global ranking regarding the cybersecurity of Taiwan, specifically due to pledges from authorities to make improvements [12]. Taiwan has improved in knowledge, technology, and future readiness as well, with improvements to education regarding cybersecurity and individual compliance with these improvements [13].

7 Difference Analysis

The cybersecurity cultures of the United States, the United Kingdom, China, and Taiwan are shaped by a varying combination of cultural, political, and economic factors. While there are aspects that are shared when it comes to the importance of cybersecurity and secure cyber culture, each country has their own specific approach to doing so.

In the United States, the American idea of individualism has an impact on cybersecurity culture. The focus on freedom and excitement over advancements can lead to naivety. The US Government's strong legal traditions and democratic system contribute to data protection regulations and laws that safeguard privacy by instilling new regulations periodically to continue to protect data and information. Additionally, the Unites States' dedication to continuously wanting technological innovation drives education and research in cybersecurity. These varying factors and approaches involving both individuals and collective efforts has fostered a diverse cybersecurity culture in the U.S.

The approach to cybersecurity in the United Kingdom is both educational and practical. The country prioritizes finding solutions and managing risks, which leads to an emphasis on protection and security. The educational system in the UK encourages students to pursue STEM subjects, including cybersecurity education, which significantly contributes to developing a skilled workforce. To create a sense of responsibility towards cybersecurity throughout the UK, the government has implemented regulations for data protection and privacy to allow society to continue its commitment to maintaining a secure cyber culture.

In contrast to the United States and United Kingdom, Chinas collectivist culture stemming from Confucianist roots promotes a collective responsibility for cybersecurity. Individuals see themselves as part of a greater community and importance, thus their commitment to safeguarding the collective's interests is visible. China's rapid technological advancement growth drives investments in cybersecurity awareness, growth, and research, further showcasing the nations dedication to security.

Taiwan's unique geopolitical position plays a role in shaping its cybersecurity culture. Given its relationship with China there is an emphasis on security within the nation. This fosters an increased awareness of the importance of cybersecurity culture in maintaining the nation's interests. The values of Confucianism, continue to greatly influence how Taiwanese people follow government regulations, maintaining order and stability much like China.

In summary, the United States and the United Kingdom emphasize innovation and legal compliance. China places a strong emphasis on collective responsibility and government authority, while Taiwan's cybersecurity culture is influenced by national security concerns. China and Taiwan share the socio-cultural idea of acting towards the greater good, fostering a strong sense of individual responsibility regarding security. Each of these nations reflects its distinct social and cultural values in its approach to cybersecurity, showcasing the diversity of approaches to cybersecurity and cybersecure culture globally.

8 Conclusion

The cybersecurity cultures of the United States, the United Kingdom, China, and Taiwan are uniquely shaped by their social, cultural, and geopolitical contexts. The United States' culture is marked by individualism and a strong belief in technological innovation, albeit sometimes at the expense of cybersecurity. In contrast, the United Kingdom prioritizes practical solutions and risk management, with a robust legal framework and a focus on STEM education. China's collectivist culture fosters shared responsibility for cybersecurity, driven by Confucian values and a commitment to technological excellence. Taiwan's complex geopolitical situation places a strong emphasis on national security and a collective responsibility for protecting sensitive information. Taiwan's core Confucianist values also contribute to their collectivist outlook, much like China, encouraging national ideas of collaboration to improve safety of the nation's information.

While these nations share a commitment to cybersecurity, their approaches vary, emphasizing individualism, practicality, collectivism, and national security. Recognizing these differences is essential for global cybersecurity strategies that consider the varying social, cultural, and political factors that shape each nation's cybersecurity culture. By understanding and respecting these diverse approaches, global change can be incurred to effectively devise methods to enhance cybersecurity on a global digital scale, increasing the overall level of safety of personal data and the cyber world.

REFERENCES

[1] Berki, E. et al. (no date) A comparative study of cyber-security knowledge in higher education institutes of five countries, EDULEARN17 Proceedings. Available at: https://library.iated.org/view/BERKI2017ACO (Accessed: 29 October 2023).

[2] Partners healthcare® (no date) U.S. Culture - Individualism | Partners (PIPS). Available at: https://pips.partners.org/life-in-the-united-states/american-culture/individualism.aspx (Accessed: 29 October 2023).

[3] Anon. Federal Information Security Management Act (FISMA). Retrieved October 20, 2023a from https://security.cms.gov/learn/federal-information-security-management-act-fisma

[4] Anon. Retrieved October 20, 2023 https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf

[5] Office for Civil Rights (OCR). 2023. Hipaa Home. (August 2023). Retrieved October 20, 2023 from https://www.hhs.gov/hipaa/index.html

[6] Stevens, T. (2022) United Kingdom: Pragmatism and adaptability in the Cyber Realm, SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4031473 (Accessed: 29 October 2023).

[7] Anon.Retrieved October 20, 2023b from https://www.ncsc.gov.uk/

[8] Franco Yau. 2023. High tech industry in China - moore - MS advisory. (September 2023). Retrieved October 20, 2023 from https://www.msadvisory.com/high-tech-industry-in-china/#:~:text=Key%20Tech%20Players%20in%20China,and%20other%20cutting%2Dedge%20technologies.

[9] Global Legal Group. Cybersecurity laws and regulations report 2023 China. Retrieved October 20, 2023 from https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china#:~:text=Article%2027%20of%20the%20Cybersecurity,network%2C%20and%20stealing%20network%20data.

[10] Admin (2013) Analysis of Elements in Modern Taiwanese Society that Preserve Traditional Confucian Values, Journal of Undergraduate Research. Available at: http://jur.byu.edu/?p=7898 (Accessed: 29 October 2023).

[11] Anon. Taiwan jumps to 11th in IMD World Digital Competitiveness Ranking 2020-achieves maximum performance. Retrieved October 20, 2023a from https://www.ndc.gov.tw/en/nc_8455_34453

[12] Nick Beckett. 2017. A guide for businesses to China’s first Cyber Security Law: Computer Weekly. (November 2017). Retrieved October 20, 2023 from https://www.computerweekly.com/opinion/Chinas-first-cyber-security-law-what-it-means-for-companies

[13] Anon. Research of cyber security industry in Taiwan - RVO. Retrieved October 20, 2023b from https://www.rvo.nl/sites/default/files/2020/07/Research-of-Cyber-Security-in-Taiwan.pdf