As cyber threats have gradually increased, the legal frameworks that govern cybersecurity have become the focus of maintaining national security, economic strength, and privacy. The legal framework, which includes laws, regulations, and policies focused at protecting digital infrastructure, which has created numerous social implications. The laws are developed by the combination of social, cultural, and digital factors, and their execution has effects on social relations, civil liberties, and global governance. This paper will help explore the social implications of cybersecurity frameworks, analyzing the factors that lead to the making , the social consequences of its request, and how cultural influences have on the making of cybersecurity laws.

Social Factors which Leads to the Cybersecurity Framework

The development of a complete cybersecurity legal framework has been handled by several social factors, which includes the increase of digitalization of society, the rapid growth of cyber threats and attacks, and the concerns over privacy and data protection. One important factor is the widespread incorporation of virtual technologies into our daily lives. The internet, social media, and the Internet of Things (IoT) devices that created a network of interconnected systems, which has caused an increased number of cyberattacks on individuals, organizations, and government agencies. Also including more critical services like healthcare, transportation, financial services, and more that rely on virtual infrastructures. Which raised the stakes socially now that cybersecurity is constantly growing.

Known cybersecurity attacks like the 2017 Equifax breach, 2016 DNC email hack, and the 2020 SolarWinds cyberattack that exposed the vulnerabilities of both private businesses and public institutions. These attacks have caused tremendous amounts of financial and reputational damage, which caused more urgency for robust cybersecurity laws. With the incidents that happened, governments have responded by developing laws and regulations like the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in the United States, and the Cybersecurity Intelligence Sharing Act (CISA), which focuses on securing essential infrastructure, safeguarding personal information, and promoting information-sharing between the public and private sectors (Schneier, 2020).

Another important factor the legal framework is constantly growing is that cybersecurity is a cross-border issue that requires global cooperation. Cyberattacks constantly span multiple jurisdictions, and the international nature of the internet makes it much more difficult to help share information of cyber threats within the confines of national legal frameworks. However, with international efforts, the creation of Budapest Convention on Cybercrime, have regulated legal decisions to cybersecurity throughout the world, which has allowed for better cooperation in helping tackle cybercrime and securing global digital infrastructure (Wicki-Birchler, 2020).

Social Consequences of Cybersecurity Framework

Cybersecurity legal framework has a wide range of social consequences, which can be both beneficial and harmful. In a positive way, strengthening the endurance critical systems and preventing cyberattacks, the legal framework helps improve national security. Cyber laws like the United States National Cybersecurity Protection Act (CISA) which helps promote the cooperation between public and business organizations, which makes it easier to recognize threats and respond to them more quickly. This cooperation is vital to help decrease the negative impact on society and the economy of cyberattacks.

Data protection laws such as the GDPR have helped grow the confidence of the consumers with more control over their individual data, expanding the trust in digital systems and meeting the global guidelines for privacy(Wicki-Birchler, 2020). However, many concerns about privacy rights are being taken because of laws like the USA PATRIOT Act and CISA allowing surveillance powers, which goes against the individual privacy rights. Therefore, cybersecurity observations can become a burden on smaller businesses, worsen inequality and focusing power in larger businesses. The global cyber laws like GDPR have developed jurisdictional issues and tensions between national legal systems, which makes it difficult to cooperate internationally to fight cyber attacks and/or threats. This issue underlines the importance of social and economic impacts of cybersecurity laws.

Cultural and Subcultural Influences

Cultural and subcultural influences have a very vital role in shaping cybersecurity legal framework. In the Western democracies, strong priority on individual rights and privacy has

influenced the development of data protection laws like the GDPR and CCPA, which reflects the trust that privacy is a fundamental human right. The GDPR is shaped by the certain concerns over the misuse of data in authoritarian regimes. The law prioritizes transparency, accountability and user consent, which shows the commitment to privacy Europe is trying to enforce (Jack, 2023). In contrast, U.S. cyber laws, like USA PATRIOT Act and CISA, focus on protecting national security, even sacrificing individual freedoms, which causes a divide between civil libertarians and security advocates over government surveillance (Schneier, 2020). Subcultures within the cybersecurity environment, especially ethical hackers and the open software movement, have also had an impact on shaping legal framework. These groups encourage transparency, collaboration and crowdsourced solutions, such as bug bounty programs. Which have influenced policies and guidelines like the CISA.

Conclusion

The legal structure surrounding cybersecurity has major social implications both beneficial and harmful. Laws securing individual information, critical infrastructure and national security have been developed as a consequence of social issues because of the growing digitalization of society, frequent cyberattacks, and increased concerns over privacy. These laws continue to raise concerns about privacy violations, social disadvantages and jurisdictional problems while they improve cybersecurity, secure rights of individuals and help promote international cooperation. The legal community has been shaped majorly by cultural and subcultural factors. The social implications of these rules will continue to be a vital discussion point and debate as cyber threats evolve.

References

Jack, H. (2023, November). *Comparative Approaches to Cyber Law: Legal Theories and Societal Implications*. researchgate.net. https://www.researchgate.net/profile/Harper-Jack/publication/385590742_Comparative_Approaches_to_Cyber_Law_Legal_Theories_and_Societal_Implications/links/672ba87477f274616d60a78f/Comparative-Approaches-to-Cyber-Law-Legal-Theories-and-Societal-Implications.

Schreider, T. (2020). *Cybersecurity Law, Standards and Regulations, 2nd Edition*. Rothstein Publishing.

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? *International Cybersecurity Law Review*, *1*, 63-72.