IAA Journal of Arts and Humanities 12(1):44-48, 2025. www.iaajournals.org
©IAAJOURNALS ISSN: 2636-7297
https://doi.org/10.59298/IAAJAH/2025/1214448 IAAJAH121

Communicating Cybersecurity Laws to the Public

Kato Nabirye H.

Faculty of Business, Kampala International University, Uganda

ABSTRACT

As cyber threats evolve in complexity and scale, cybersecurity laws have proliferated to provide legal frameworks for protection and compliance. However, a critical challenge persists: the communication and public understanding of these laws. This paper examines the multifaceted problem of communicating cybersecurity legislation to the general public and relevant stakeholders. It examines the importance of public awareness, the challenges in conveying legal obligations, and the role of government agencies and private sector collaboration. Drawing on the Knowledge-Attitude-Acceptance (KAA) framework, the paper proposes strategic communication models to enhance legal literacy, increase compliance, and foster trust. It also reviews key laws, case studies, and public understanding metrics to propose a unified, adaptive approach to legal outreach. Ultimately, the paper emphasizes that the future of cybersecurity law communication depends on inclusive, localized, and continuous engagement from both public institutions and private actors.

Keywords: Cybersecurity laws, public awareness, legal communication, KAA framework, government outreach, compliance, cybercrime prevention.

INTRODUCTION

As dependence on technology increases, cybersecurity concerns grow. Cyber attacks are evolving, with potential attackers having greater access to resources. Wealthy nation-states possess advanced technology, making it challenging for individuals to stay engaged in combating such threats. Understanding and navigating cybersecurity laws is complex but essential for compliance. Users face numerous stakeholders seeking financial gains tied to compliance. Knowledge of the law aids in effectively communicating cybersecurity issues and fostering trust through discussions that clarify concerns. The rise of technology amplifies cyber attacks, heightening fear and regulations, while public knowledge of these laws remains insufficient. This gap hinders meaningful conversations about cybersecurity, leaving compliance seemingly unattainable. Without public and business buy-in on the significance of cybersecurity regulations, discussions remain ineffective. This creates a cycle where communication fails. Emphasizing public engagement could lead to better understanding of a typically complex topic. A model is proposed to bridge the knowledge gap related to cybersecurity laws, utilizing insights to effectively convey the intricate framework to various stakeholders, thereby nurturing a culture that prioritizes addressing the evolving nature of cyber threats [1, 2].

Importance of Public Awareness

Many laws affect people's life and freedom in many areas, such as parents' duty of care towards their children as a legal obligation, the illegality of drunk driving, and laws of e-commerce for businesses. Regarding cybercrime, laws for the prevention of computer crimes or cybersecurity laws in a broad sense are enacted. In addition, a few laws on people's guilt or duty, such as government agency obligations, are enacted after cybercrime occurs. Most laws are not widely known to the public. When someone breaches laws in society, it usually becomes a more serious issue than when it does not happen. When it comes to cybercrime, it usually captures huge attention when many people are exposed to security vulnerabilities. Cybersecurity disclosure reports of both private and public organizations are often news stories that make waves. In this uncertain and ambiguous societal environment, education and warning about laws and obligations on this matter are very important for individuals as well as organizations as a whole. Precautions should be taken in advance by promoting the society-wide discussion of what laws will be

enacted. Creating awareness of cybersecurity law is a duty that should be performed by government entities, in cooperation with legal experts, policymakers, and law enforcement agencies. Whereas enforcement of law is supposed to guarantee order in society, its enforcement ex post facto has limitations involving a lot of costs or risks. Thus, measures involving deterrence are needed for cybersecurity laws, as well as for other areas of law. Existing laws are not implied by or written down, and humans create law as an act of legitimacy. On the Internet, there are laws and regulations, with each application running under a specific set of rules. Law exists as a matter of fact with enough social awareness, and goes well with all actors' compliance, in order for it to come into being as a consensus. Education on cyber laws by governments is essential for law awareness to exist in society and for the efficacy and legitimacy of law in general. Cybercrime laws cannot be enforced if the majority of the relevant actors such as individuals and organizations do not know their existence [3, 4].

Key Cybersecurity Laws

The NIST and CISA's TIC 3.0 guidance emphasizes Zero Trust security principles, advocating for modernizing DHS and CISA infrastructures to enhance data analysis capabilities. CISA should launch outreach campaigns to involve state and local officials in cybersecurity efforts, supported by federal investments tailored to their needs. New Hampshire exemplifies a potential national model for local cybersecurity improvements. Cybersecurity threats evolve as new tactics emerge, allowing criminals to exploit networks without facing major barriers. The criminal underground discourages compliance with cybersecurity laws, making noncompliance financially easier than adhering to regulations. Detecting threats is insufficient; regulatory frameworks must also tackle noncompliance factors. Real-world issues like security through obscurity and DMCA misuse exacerbate compliance challenges. Key cybersecurity laws were reviewed for their purpose, applicability, requirements, and penalties. Many current laws impose high costs on compliant entities while offering minimal investment from the unregulated sector. To balance this, the government should encourage compliance by providing liability protections and adjusting accounting rules to facilitate better loss disclosures [5, 6].

Challenges in Communication

Communicating cybersecurity measures to the public is complex and challenging. Political actors and institutions often opt to pass laws without adequately explaining them to the general population, resulting in a significant communication gap. Globally, numerous cybersecurity-related laws have been enacted with little public understanding. For example, discussions about cybersecurity measures in the public domain started nearly eight years after their enactment. Similarly, in the Philippines, it took over four years post-implementation for stakeholders to address the Cybercrime Prevention Law's requirements. Public reception of laws varies widely based on the socio-political context, leading to backlash in some regions and acceptance in others, which should guide communication strategies. The timing of these communications often falls behind legal developments, as some areas are only now considering how to address the regulations' impacts years later. Thus, explaining laws may necessitate ongoing efforts involving various actors and institutions even after implementation [7, 8].

Effective Communication Strategies

To address the challenge of raising public awareness about cybersecurity laws, it is crucial to develop effective communication strategies that enhance understanding. Knowledge is the basis of acceptance, with the understanding level influencing acceptance. Based on this relationship, the knowledge-attitude-acceptance (KAA) framework helps create effective communication strategies. The KAA framework hypothesizes that increasing public knowledge about cybersecurity laws leads to a more positive attitude towards these laws, thus enhancing the acceptance of such laws, and vice versa in the opposite direction. It consists of two main components: a theoretical framework and practical modes for implementing different variables. Public understanding creates a better acceptance of laws regarding special issues related to the internet and information technology (IT). Evidence for this statement can be easily found in the interaction between the general public and governments. Many scholars and investigators have studied measures for raising the public's understanding about cybersecurity laws. An interesting topic raised by these governments and scholars is how to enhance the public understanding of cybersecurity laws so that a higher acceptance of these laws can be achieved. This question is not only interesting, but also non-trivial. One challenge is that there is little empirical evidence in the literature that demonstrates this issue. To address this challenge, a frame is explored to study possible modes for enhancing the public knowledge of cybersecurity laws. This frame is proposed in the KAA framework. It consists of widely accepted knowledge, attitude and acceptance theories, which explain the relationship between the three variables of knowledge, attitude and acceptance. Based on the KAA framework, practical modes are

discovered in the frame of the KAA framework to enhance the public understanding of cybersecurity laws [9, 10].

Role of Government Agencies

Governmental and federal law enforcement agencies must lead the way in communicating the laws to the public, given their extensive resources. Agencies have different missions regarding legislative public communication. Their agencies' missions should be broadly interpreted to allow aggressive outreach. It is pivotal to introduce a single statute that codifies all cyber-related offenses in one place, which could then have statutory elements corresponding with which agency should outreach to which type of cybersecurity offense. Outreach is about educating the public on the legislation or laws, but once a single code is introduced, additional technical assistance should be provided by agencies to provide clarity. This would ensure that the public understands what types of acts are prosecutions in a single body of laws and how to prevent against them. New agencies or offices could be created to handle these laws or existing agencies' responsibilities could be altered. Whether existing or new, staffing should include a mélange of communication experts, criminalists, behavioral scientists, and policy-makers that can thoroughly and effectively outreach to the public. Outreach staff should also be incredibly localized. It is erroneous to infer that "one-size fits all" outreach strategies would work that covers broad topics. Each country, city, and town has different characteristics. Outreach staff must be rooted in the communities they serve. Translators familiar with the local culture and social mores should also be hired because as with the law, communication can be culture-specific. Moreover, the crime prevention must be overtly and uniquely synonymous with the agency's mission. Crime prevention is not unique to cyber offenses, each agency must take ownership and identify themselves as an agency dedicated to preventing, investigating, and enforcing cyber laws. This might mean some jurisdictional cooperation to ensure the public does not fall into the trap of thinking that cyber protections are a federal concern only, as is often the case with gun crime or financial-related crime [11, 12].

Collaboration With Private Sector

Cybersecurity is a shared responsibility requiring involvement from various stakeholders. Private entities must implement measures that correspond to the risks they face and those affecting society. The behavior of these entities is shaped by the incentives provided by the larger ecosystem, comprised of federal, state, and local governments, private sector firms responsible for cybersecurity, and new players without formal responsibilities. Understanding how to engage these actors, their behaviors, and the incentives influencing them is crucial for mobilizing effective responses and mitigating negative impacts. Recognizing the growing cybersecurity risks, the US Government has promoted public-private partnerships to protect Critical Information Infrastructures over the past decade. However, these partnerships pose challenges. They require alignment between public and private interests and effective pathways for collaboration. A solid connection between cyber policy and technical solutions is necessary, as the two sectors may not share cohesive cybersecurity visions. Brief interactions among computer scientists, national security experts, economic actors, and lawyers in these partnerships can create long-lasting effects. Additionally, private entities may resist government involvement when they feel capable of defending themselves, opting for partnerships outside government visibility. Concerns about effectiveness may affect compatibility, leading actors valuing private sector initiatives to prefer minimal federal engagement [13, 14].

Case Studies

The implementation of cybersecurity laws is primarily the responsibility of both the public and private sectors, with the public sector comprising governmental organizations. In the last decade, the rise in data breaches has heightened the focus on improving the public sector's cyber hygiene. States are seen as having a special obligation to uphold their cyber hygiene by providing the necessary technology and clarifying law enforcement responses, apart from educational efforts. Recommended practices for enhancing compliance with cybersecurity laws include ensuring lawyers receive timely, detailed information that emphasizes the nature and urgency of new laws and regulations. Additionally, legal education needs to stress the significance of cybersecurity protections at appropriate stages. Laws should be accessible for regular lawyer review, accompanied by online resources outlining best practices. Keeping attorneys updated about improvements is also crucial for effective implementation, alongside explaining how updates are communicated and the group's expectations. Some concern exists regarding the clarity of commercial website "terms of use," which can obscure laws and lead to misunderstandings, particularly regarding cloud service privilege revocations. Lawyers are encouraged to engage with drafting groups to clarify ambiguities before legal actions are initiated, which can influence outcomes significantly. However,

the mechanisms in place aren't infallible; advocates must routinely seek improved practices that facilitate favorable litigation results. While private sector self-regulation is beneficial, it does not replace the necessity for effective regulatory statutes, which are still pending discussions in Congress [15, 16].

Measuring Public Understanding

Public understanding is vital for the successful implementation of cybersecurity laws, as many countries now have national legislation affecting a larger global population. It is crucial to assess the comprehension of both domestic and international audiences to ensure adherence to obligations. The Cybersecurity Capacity Portal, launched in December 2021, conducted a review of existing frameworks and tools, adopting a composite index to gauge public understanding. This framework is based on four dimensions: 1) Knowledge; 2) Awareness; 3) Public perception and attitudes; 4) Information sources used. It led to twenty-two indicator questions aimed at evaluating individuals' mindsets regarding cybersecurity laws, covering six areas of understanding: 1) Applicable laws; 2) Relevant governmental institutions; 3) Non-government organizations; 4) Non-compliance consequences; 5) Improvement recommendations; 6) Sustaining understanding. Concrete measures for understanding cybersecurity legislation include various indicators. Assessment methods often involve self-reporting questionnaires and pre- and post-surveys, while other quantitative and qualitative inquiries can also be utilized. Linking public understanding to interest in cybersecurity provides a basis for identifying potential improvements [17, 18].

Future of Cybersecurity Law Communication

The future of cybersecurity law communication demands collaboration among companies, governments, experts, civil societies, and the media for effective solutions. Governments should avoid framing cybersecurity laws as punitive and instead communicate solidarity with affected companies. Early engagement with industry before drafting laws can yield valuable insights. Multinational corporations should consider establishing dedicated legal and media relations teams in every country to effectively share cybersecurity expertise and foster collaboration. Regulations should encourage compliance and ensure that fines correspond to potential damages, applying preset penalties only where adherence is impractical. Cross-border cooperation among governments and private sector compliance experts is essential. Legislation must prioritize substantive obligations over bureaucratic hurdles and should not solely aim to penalize negligence. Changing government perceptions and practices regarding cybersecurity regulation poses a challenge. Often, legislation is crafted without adequate understanding of its potential negative impact on those it regulates, leading to opaque processes. Global firms operating in developing countries may face significant reputational harm, especially following high-profile breaches where both the company and government issue statements that prompt inquiries, but the company often retracts from further comments [19, 20, 21].

CONCLUSION

The effectiveness of cybersecurity laws is closely tied to the public's ability to understand and comply with them. Current legal frameworks are often complex, poorly communicated, and inconsistently enforced, creating a disconnect between legislative intent and public behavior. Bridging this gap requires strategic, inclusive, and localized communication efforts spearheaded by government agencies and supported by the private sector. The Knowledge-Attitude-Acceptance (KAA) framework provides a valuable foundation for crafting communication strategies that enhance public understanding and foster regulatory acceptance. Successful outreach demands the integration of behavioral science, community-based communication, and cross-sector collaboration. Future efforts should prioritize education, simplify legal messaging, and ensure that cybersecurity laws are not only enforceable but also socially legitimate. By building a legally literate society, we can create a more resilient and cooperative digital ecosystem.

REFERENCES

1. Catal C, Ozcan A, Donmez E, Kasif A. Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Education and Information Technologies. 2023 Feb;28(2):1809-31. springer.com
2. Marune AE, Hartanto B. Strengthening personal data protection, cyber security, and improving public awareness in Indonesia: Progressive legal perspective. International Journal of Business, Economics, and Social Development. 2021 Nov 7;2(4):143-52. rescollacomm.com
3. Nielsen LB, Albiston CR. The organization of public interest practice: 1975-2004. NCL Rev.. 2005;84:1591.
4. Rosenbloom DH, Kravchuk RS, Clerkin RM. Public administration: Understanding management, politics, and law in the public sector. Routledge; 2022 Jan 27.

5. Oluomachi E, Ahmed A, Ahmed W, Samson E. Assessing the effectiveness of current cybersecurity regulations and policies in the US. arXiv preprint arXiv:2404.11473. 2024 Apr 17.
6. Garcia M, Forscey D, Blute T. Beyond the network: A holistic perspective on state cybersecurity governance. Neb. L. Rev.. 2017;96:252.
7. Lukings M, Habibi Lashkari A. Comparative Legal Strategies. InUnderstanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective 2022 Oct 15 (pp. 181-204). Cham: Springer International Publishing.
8. Creemers R. Cybersecurity Law and regulation in China: Securing the smart state. China Law and Society Review. 2023 Mar 17;6(2):111-45.
9. Khan SK, Shiwakoti N, Stasinopoulos P, Chen Y, Warren M. The impact of perceived cyber-risks on automated vehicle acceptance: Insights from a survey of participants from the United States, the United Kingdom, New Zealand, and Australia. Transport policy. 2024 Jun 1;152:87-101. sciencedirect.com
10. Eze VH, Ugwu CN, Ugwuanyi IC. A Study of Cyber Security Threats, Challenges in Different Fields and its Prospective Solutions: A Review. INOSR Journal of Scientific Research. 2023;9(1):13-24.
11. Trivedi SK, Patra P, Srivastava PR, Kumar A, Ye F. Exploring factors affecting users' behavioral intention to adopt digital technologies: The mediating effect of social influence. IEEE Transactions on Engineering Management. 2022 Jun 29.
12. Al-Tarawneh A, Al-Badawi M, Hatab WA. TRANSLATING GOVERNANCE AND LEGAL COMPLIANCE: EXPLORING THE ROLE OF TRANSLATION IN FACILITATING CORPORATE REPORTING AND POLICY IMPLEMENTATION. Corporate Law & Governance Review. 2024 Sep 1;6(3). [HTML]
13. Mishra A, Alzoubi YI, Anwar MJ, Gill AQ. Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security. 2022 Sep 1;120:102820.
14. McCarthy DR. Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order. Politics and Governance. 2018 Jun 11;6(2):5-12.
15. Sedenberg EM, Dempsey JX. Cybersecurity information sharing governance structures: An ecosystem of diversity, trust, and tradeoffs. arXiv preprint arXiv:1805.12266. 2018 May 31.
16. Calcara A, Marchetti R. State-industry relations and cybersecurity governance in Europe. Review of International Political Economy. 2022 Jul 4;29(4):1237-62.
17. AlDaajeh S, Saleous H, Alrabaee S, Barka E, Breitinger F, Choo KK. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security. 2022 Aug 1;119:102754. uni-augsburg.de
18. Schneider GB. The Importance of Cybersecurity in Digital Government Implementations. COGNITIONIS Scientific Journal. 2025 Jan 30;8(1):e585-.
19. Bokhari SA. A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan. Social Sciences. 2023 Nov 10;12(11):629.
20. Balitzer S. What Common Law and Common Sense Teach Us About Corporate Cybersecurity. U. Mich. JL Reform. 2015;49:891.
21. Knight R, Nurse JR. A framework for effective corporate communication after cyber security incidents. Computers & Security. 2020 Dec 1;99:102036.

CITE AS: Kato Nabirye H. (2025). Communicating Cybersecurity Laws to the Public. IAA Journal of Arts and Humanities 12(1):44-48. https://doi.org/10.59298/IAAJAH/2025/1214448