IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

Cybersecurity Collaboration: Building Trust and Resilience through Information Sharing

Mr. Mohamed Bahar[1], Dr. Mohammad Muqeem[2], Dr. Omkar Pattnaik[3]
MTech Student, School of Computer Science and Engineering, Sandip University, Nashik, India[1]
Professor, Department of Computer Science and Engineering, Sandip University, Nashik, India[2]
Associate Professor, Department of Computer Science and Engineering, Sandip University, Nashik, India[3]

Abstract: *This paper focuses on the pivotal role of information sharing practices for capacity building competences in the field of cybersecurity. It analysis the necessities and limitations of information sharing, aiming to boost a secure and resilient cyberspace that installs trust. The paper identifies the different types of information that can be shared and outlines the channels that support this exchange. By proposing five applications of information sharing in cybersecurity, it focusses on education and warning in order to enforce people competencies. High-level recommendations are proposed in conclusion for the establishment of a platform for information sharing and analysis.*

Keywords: Information sharing, cyber resilience, education, multidisciplinary approach, cybersecurity culture, trust, privacy.

I. INTRODUCTION

With globalization and the modernization of societies, our world is undergoing an unprecedented transformation, that of digitization. It is found in all services and makes it possible to be very competitive thanks to extremely rapid technological and market developments. However, this change is taking place in a very complex environment, due in particular to systems with particular languages, a multitude of stakeholders and ever more stringent legal requirements. The development of appropriate skills therefore seems necessary in order to build a reliable digital ecosystem, secure by default and from the design stage. These skills should also enable managers to adopt consistent behaviours that protect privacy and ensure user trust. Digital and cybersecurity culture is based on sharing information and providing the knowledge necessary to build skills in the disciplines of politics, economics, management, sociology, law and technology (Fig. 1). Information Sharing & Analysis Centre's (ISACs) are mainly concerned with technical information. They constitute a type of information exchange platform related to cybersecurity knowing that others should exist to cover all the related security needs in particular those related to legal compliance.

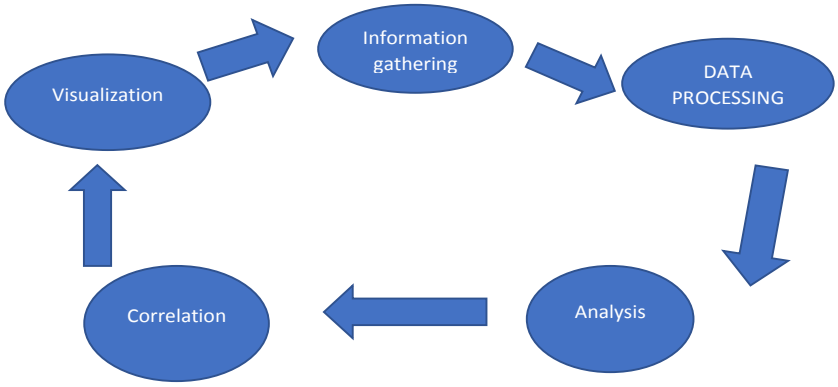

Fig (1): Information sharing

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

A good knowledge of the mechanisms of economic interference with regard to the facilities offered by the digital world contributes to maintaining the competitive advantages of organizations. This contributes to the adequate protection of the country's scientific, technical, economic and industrial capital and to the good health of the economic center. In all these areas, appropriate information sharing is necessary and must be accompanied by risk prevention and asset protection measures.

Legal risk must be carefully considered in view of the development and increasing severity of regulations relating to the protection of personal data. In Europe, for example, since May 2018, with the implementation of the GDPR (General Data Protection Regulation [1]), entities have been risking financial penalties of up to €20 million or 4% of the company's worldwide turnover in the event of non-compliance with the regulation. These legal requirements must be known to technical staff, particularly since an obligation to ensure the security of the information held is now in force. Indeed, according to Article 5 letter f of the regulation, data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’). Legislative compliance is therefore an essential step for organizations, especially in the context of information sharing, where each partnership must be strictly controlled.

II. LITERATURE REVIEW

Information sharing is considered an important approach to increasing organizational efficiency and performance. With advances in information and communication technology, sharing information across organizations has become more feasible. In the public sector, government agencies are also aware of the importance of information sharing for addressing policy issues such as anti-terrorism and public health. However, information sharing can be a complex task. Identifying factors that influence information sharing is critical. In the literature, research in information sharing focuses on the interpersonal, intra-organizational, and inter-organizational levels. This paper reviews the current information-sharing research, discusses the factors affecting information sharing at the three levels, and provides summative frameworks. These frameworks provide a means to discover future research opportunities, and a systematic way for practitioners to identify key factors involved in successful information sharing.

(1). Intrapersonal information sharing

This section focuses on how and why individuals share information within the context of interpersonal relationships. Interpersonal relationships occur within many contexts: neighbors, classmates, friends, or members of a community. Information-sharing research at the interpersonal level focuses on individual behaviors such as motivations, approaches, and channels for an individual to share information with others. Information sharing can be a volunteer behavior to provide information to other.

(2). Intra-organizational information sharing

Within organizations, there is a trend to encourage groups to share information and knowledge, however information flows in organizations are strictly controlled. With limited access to and sharing of information and knowledge, organizational members lack the capability to develop integrated solutions to problems. Often members of an organization do not share information scattered among organizational.

(3). Inter-organizational information sharing the interoperability across organizations represents cross-boundary information sharing. Researchers have recognized the importance of cross-boundary information sharing, especially in the area of e-Government. Information assurance is the practice of protecting against and managing risks related to the use, processing, storage, and transmission of data and information systems. The U.S. Department of Defense has promulgated the Five Pillars of Information Assurance model that includes the protection of confidentiality, integrity, availability, authenticity, and non-repudiation of user data. Information technology industry is one of the most innovative and dynamic industry in the whole world; on the one hand, the cyberspace applies new technological trends in order to reduce risks, on the other hand, criminals also adapt to new technologies. So, cybersecurity strategy should be flexible with new technologies, vulnerabilities and threats. However, all strategies should strike a balance between

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

cybersecurity issues and information technology innovations. Thus, an effective cybersecurity strategy should support research and development of information security solutions and encourage technical innovation in cybersecurity. Finally, a cybersecurity strategy cannot be effective without technologies progress. Individuals, organizations and states are confronted with cyber risks and the need to strengthen their security and resilience postures. From now on, the sovereignty of the nation depends on the control of cyber risks and on its ability to prevent and react to cyber-attacks, of which the whole society can be victims, including critical infrastructures and vital services. The major functions of the State can be disrupted by a lack of effectiveness, efficiency and comprehensive global approach of cybersecurity requirements. this is particularly true in the fields of national defense and security, diplomacy, policing, public safety, democracy and national economy. In a connected world, dependent upon digital infrastructures and services, national's economic performance depends to a large extent on the proper functioning of the digital ecosystem and its cybersecurity. Some actors, according to particular motivations and circumstances, know how to use the capacities offered by the cyberspace to harm, destabilize, influence, control, spy, steal, illegally enrich themselves and, project power.Protecting, preventing and defending values, detecting and managing incidents and crises, correcting security deficiencies, optimizing security and defense measures in an effective and efficient manner is a complex and difficult exercise for which information sharing is one of the elements of response

III. PILLAR FOR AN EFFECTIVE CYBERSECURITY STRATEGY

Nowadays, information is the most important value for each society and the protection of this patrimony must be a necessity for national security. However, this obligation was generalized cybersecurity support especially with the strong presence of information systems in private and public sectors. Generally, any cybersecurity strategy - consists to protect individuals, organizations and government digital assets- should be specific to the protected value. However, an effective national cybersecurity strategy conforms to international standards preserves organization's information assets. Our main aim is to support a cybersecurity consistent approach including legal, technological and organizational dimensions, as more cybersecurity is mainly based on technology, management procedure, organizational structure, laws and human competence. Though, strike the balance between a three fundamental pillars: Organizational, legal and technological means a greater awareness of information security.

Pillar of Cybersecurity

A. Organizational

As an organization increases in size and complexity, the number of stakeholders and their competing interests grow as well. These factors work in combination to define the form of corporate governance that works best to support a particular organization. The foundation of comprehensive and holistic approach to cybersecurity. This pillar focuses on the human element of cybersecurity, including employee education, awareness, and training. It is essential to ensure that employees understand the importance of cybersecurity and are equipped with the necessary skills and knowledge to identify and respond to potential threats.

B. Legal

The internet world is not protected against crimes, so there is a greatest need for a common legal framework which introduces public and private actors. This legal framework for cybersecurity purpose is to define a legal model adopted and approved in internal law and conform to international standard, which introduced from the national culture in collaboration with governmental and private actors in order to identify and treat all digital risks.

C. Technologies

Information technology industry is one of the most innovative and dynamic industry in the whole world; on the one hand, the cyberspace applies new technological in order to reduce risks, on the other hand, criminals also adapt to new technologies. So, cybersecurity strategy should be flexible with new technologies, vulnerabilities and threats. The technological pillar encompasses the tools and systems used to detect, prevent, and respond to cyber threats. It includes firewalls, intrusion detection systems, encryption, and other technologies that help protect the organization's digital assets.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

IV. RELATED WORK

A. Applications of Information Sharing in Cybersecurity

Cybersecurity and privacy are becoming more critical with digital transformation. The increasing sophistication of threats, including Advanced persistence threats (APT), nation hacktivism, makes it vital for organizations to have robust cybersecurity measures in place. However, cybersecurity is not just about preventing threats; it also plays a crucial role in robust trust across a spectrum of stakeholders. Companies that prioritize cybersecurity and privacy while building customer trust are more likely to succeed in today's interconnected world.

The following are the key competence needs for cybersecurity trust and privacy:

Trustworthy Cybersecurity Measures

The first step towards gaining consumer trust is to have a comprehensive cybersecurity program in place to prevent risks and threats. This includes implementing cybersecurity network, monitoring, and regular audits, ensuring the security posture of the organization is always up-to-date.

Awareness and Training

Raising awareness and training of threats and risks among employee's and stakeholders in the digital ecosystem, Training employees is critical for building cybersecurity awareness and promoting information security practices. Employees need to receive regular training on best practices, emergency response procedures, and the importance of keeping their devices and networks secure. giving them ideas for responsible behavior and precautionary, protective and defense measures, is part of information sharing. Overall, this contributes to better cybersecurity, cyber resilience and it contributes to effectiveness of the fight against cyber threats.

Privacy

Privacy is an important part of cybersecurity. Organizations need to have robust privacy protections in place to ssafeguard their products, services and data. This includes implementing privacy policies, ensuring compliance with applicable data protection regulations, and providing users with control over their data.

Transparency

Transparency is necessary for building trust with stakeholders. Companies need to be open and honest about their cybersecurity and privacy practices, including data collecting and sharing policies. They need to communicate their security policies and procedures clearly and effectively, and be prepared to address any concerns or questions that arise.

Incident response

Incident response refers to process or approach taken by organization's that address and manage security incidents for detecting and responding to cyberthreats, security breaches, or cyberattacks. Organizations need to have a well-defined incident response plan in place to handle cybersecurity incidents. This includes procedures for identifying threats, containing the incident, recovering systems, and communicating with stakeholders.

V. CONCLUSION

Nowadays, information is the most important value for each society and the protection of this information must be a necessity for national security. However, this obligation was generalized cybersecurity support especially with the strong presence of information systems in private and public sectors. Generally, any cybersecurity strategy - consists to protect individuals, organizations and government digital assets- should be specific to the protected value. the main aim of this project to support cybersecurity consistent approach including legal, technological and organizational dimensions, as more cybersecurity is mainly based on technology, management procedure, organizational structure, laws and human competence. To strike the balance between a three fundamental pillars: Organizational, legal and technological means a greater awareness of information security. Cybersecurity trust and privacy are critical for building and maintaining customer trust. The most effective way to achieve this is by having a comprehensive cybersecurity program that includes these key competence needs.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

VI. ACKNOWLEDGMENT

The paper discusses the fundamental pillars for effective cybersecurity strategy. Here are thekey takeaways, Identify the actors, purposes and benefits of information sharing in short, medium and long term (infrastructure providers, services, users' groups, resources sharing), Specify the means of evaluating expected gains, define performance evaluation indicators (performance and management indicators). Define the scope of sharing (intra-organization, inter organization, sectoral international level). organizations, national, carry out the partnerships to be set up by defining the measures that will make them work, while considering legal, regulatory and budgetary constraints and Identify and adapt existing organizational structures that can contribute to information sharing or set up new IT structures and infrastructures for effective and efficient information sharing.

REFERENCES

[1] Regulation (eu) 2016/679 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[2] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf.
[3] https://www.whitehouse.gov/wp-content/uploads/2018/09/National- Cyber-Strategy.pdf.
[4] https://www.isb.admin.ch/dam/isb/en/dokumente/ikt- vorgaben/strategien/ncs/Nationale_Strategie_Schutz_Schweiz _vor_C yber-Risiken_NCS_2018- 22_EN.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_ Cyber-Risiken_NCS_2018-22_EN.pdf.
[5]https://www.gov.uk/government/uploads/system/uploads/attachment_ data/file/567242/national_cyber_security_strategy_2016.pdf.
[6] S. Ghernaouti, Cyberpower, Crime Conflit and Security in Cyperspace. EPFL Press – CRC Press 2013, p. 275.
[7] https://www.europol.europa.eu/sites/default/files/documents/fr_ql011 3549frc.pdf.
[8] https://www.mitre.org/.
[9] https://cve.mitre.org/.
[10] https://www.enisa.europa.eu/publications/information-sharing-and- analysis-center-isacs-cooperative-models.
[11] Operational guidance for the EU's international cooperation on cyber capacity building. European Commission, 2018.
[12] http://www.enisa.europa.eu/act/res/policies/good-practices- 1/information-sharing-exchange/incentives-and-barriers-to- information-sharing/at_download/fullReport