p-ISSN : 2685-9106
e-ISSN : 2686-0384
ADI International Conference Series

Investigating the impact of cybersecurity culture on employees' cybersecurity protection behaviours: A Conceptual Paper

Laksana Budiwiyono Lie[1], Prio Utomo[2], P.M. Winarno[3]

laksana.budiwiyono@umn.ac.id[1], prio.utomo@umn.ac.id[2], pmwinarno@umn.ac.id[3]

Faculty of Business, Universitas Multimedia Nusantara, Tangerang, Indonesia[1,2,3]

To cite this document:
Lie, L. B., Utomo, P. ., & Winarno, P. . (2021). Investigating the Impact of Cybersecurity Culture on Employees' Cybersecurity Protection Behaviours: A Conceptual Paper. Conference Series, 3(2), 295–305. https://doi.org/10.34306/conferenceseries.v3i2.598

Abstract

As technology and digital applications increase in volume and complexity, organization is facing greater security risks in cyberspace more than ever before. However, organizational cybersecurity requires more than just the latest technology. All the technology available to secure systems will not keep an organization secure if the people in the organization make bad or unexpected decisions that open up the system to attackers. To secure an organization, all employees of the organization must act positively to reduce company risks from cyberattacks. All leaders have a main responsibility to understand and align with the entire organization with cybersecurity objectives. Leaders need to keep continue to invest in security technologies and also need practical solutions for dealing with the human error of cybersecurity. The conceptual paper presented in this paper describes cybersecurity culture, external influencing factors, and organizational mechanisms, the elements that contribute to each employee of the organization that having protection behaviour from cyberattacks.

Keywords: cyberattack; digital resilience; protection motivation theory; cybersecurity culture; cybersecurity protection behaviour.

1. INTRODUCTION

Cyberattack has increased significantly, with a number of cybersecurity incidents, hacking attacks and data breaches reaching the news recently and even over the last few years. Many organisations are transforming to digital platform and they cannot survive without securing

their information. They really need to be very serious about protecting their digital and information assets [1]. Definitely every organisation wants to secure and protect its assets from hackers or cyber-attackers.

Even using the most advanced technological cybersecurity, an organisation cannot protect from a cyber breach if the people in the organisation are not careful and protective. Organisations are potentially vulnerable to cyberattacks because employee or people in the organisation are not aware of cyber risks and its impacts. It is mandatory and important thing for any organisation for having an information security solution [2]. According to Ponemon Institute, Cost of a Data Breach Study in 2018, the average cost of each lost or stolen record containing sensitive and confidential information has increased to US$148.

An organisation's success or failure in implementing information system security not just depends on security technology they adopt, but most important are depends on the actions of its employees and how danger they behave when they are online to the system. One of the most overlooked aspects of cybersecurity in organisations is the human factor [2]. An organisation's success in information system security can be improved by focusing on employee behaviour [3]. To reduce the risk of security failures, organisations should focus more on employee behaviour. Educating an cybersecurity awareness and culture will decrease risk to information assets [3].

The need for cybersecurity is becoming increasingly important due to our dependence on Information and Communication Technology (ICT) across all aspects. In today's cyber era, by clicking on a phishing email, it provide an bad guy or attacker an entry point into their critical business application and it can be make their system compromised. Once inside, an attacker can lock up critical information and data or bring down critical infrastructure, with commonly result is a data breach incident.

Another issue, insider threat from human behaviour is one of the most difficult aspects of information security to control and protect, because they are authorized person. to access their systems. Building a culture of cybersecurity within an organisation guides employee behaviour and help increases cyber resilience. A culture of cybersecurity motivates employees in the organisation to use the practices, policies and "*unwritten rules*" in their day-to-day activities.

A common goal can be said for cybersecurity; every employee in the organisation must act in ways that keep the organisation secure from cyber risks and attacks. Building a protection behaviour of cybersecurity where the cybersecurity culture, external influences and management commitment align with organisational goals of cyber resilience is of significant interest to managers and leaders in charge of cybersecurity in organisations today. To build a cybersecurity protection behaviour at organisations, we examined three important components: cybersecurity culture, external influences, and organisational mechanisms.

2. LITERATURE REVIEW

1. External Influencing Factors

The culture of an individual or an organisation about cybersecurity are also shaped by external influencing factors. The more the public press reports on cybersecurity incidents, the more aware individuals become of cyber risks. Furthermore, for certain industries, the government or regulatory body orders how companies must prepare and defend against cyber threats, otherwise they will get penalties. For example, General Data Protection Regulation (GDPR) regulations that applies to organisation operating within European Union (EU), require organisations to have a data protection officer (DPO). In this case, organisations subject to this regulation will be more influenced than others. For external influences component, we examine two components which are (1) External Rules and Regulations and (2) Peer Institutions.

1.1. External Rules and Regulations

In the organisation, external rules and regulations refers to the laws, guidelines, and regulations that enforced by government and other industry authorities. Given the significant externalities in cyber security domain, the implementation of cybersecurity policies and rules, from government or authorized institutions, can impact the organisational cybersecurity culture. For example, banking and financial services companies are subject to very strict rules and regulations about managing their information and we expect those organisations to have different beliefs and attitudes towards cybersecurity than companies in other industries.

1.2. Peer Institutions

Peer institution refers to the pressure felt by managers in an organisation from actions their peer organisations have taken. Institutional theory seeks to explain organisational communication in terms of shared pre-existing rules, beliefs, and norms in the external environment of organisations. Institutional theory takes seriously the established aspects of organisations' external environments as important determinants of organisational communication and behaviour. Even as these external phenomena influence every organisation, they exist independently of particular organisations and together are generally referred to as the institutional environment of organisations. The institutional approach challenges interpersonal approaches to organisational communication studies by offering explanations of behaviour based on structural and environmental conditions.

It suggests that since cybersecurity is a relatively new threat with huge uncertainties for many organisations, managers often look to their institution peers for guidance and reference on

how to act. At the end, their customers begin to seek out vendors with strong cybersecurity practices that match their supply chain requirements, organisation are pressured to up their cybersecurity posture in order to win the business competitive. These important concerns would drive different attitudes about cybersecurity than those organisations with peers who are less concerned about these issues.

2. Organisational Mechanisms

Cybersecurity culture and the unwritten rules of the organisation are created by the actions of managers and leaders which we have labeled management controls or managerial/organisational mechanisms. We describes three controls that leaders can use organisational mechanisms to influence the cybersecurity culture; (1) Organisational Learning, (2) Cybersecurity Awareness Training and (3) Communication Channel.

2.1. Organisational Learning

Organisational learning (OL) enables organisations to transform individual knowledge into organisational knowledge. OL is “the process through which organisations change or modify their mental models, rules, processes or knowledge, maintaining or improving their performance” [4]. It aims to adapt organisational processes through targeted activities [5]. OL is crucial for organisations operating in unpredictable environments to respond to unforeseen circumstances more quickly than their competitors [6].

Two of the most noteworthy contributors to the field of OL theory are Chris Argrys and Donald Schon [8]. According to Argrys & Schon [7], OL is a product of organisational inquiry. This means that whenever expected outcome differs from actual outcome, an individual or a group will engage in inquiry to understand and solve the inconsistency. In the process of organisational inquiry, individual employee will interact with other employee members of the organisation and learning will take place.

OL refers to the ways the organisation builds and retains cybersecurity knowledge. OL has been defined as “*the intentional use of learning processes at the individual, group, and system level to continuously transform the organisation in a direction that is increasingly satisfying to its stakeholders*” [8].

OL helps manage continuous change which is also characteristic of cybersecurity. OL in cybersecurity can include mentors who work together with individuals to help them build skills and bring new knowledge to the team.

2.2. Cybersecurity Awareness Training

Cybersecurity awareness training refers to courses and exercises that develop cybersecurity skills and knowledge. Cyber security awareness term was defined by Shaw et al [8] as "*[The] degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organisation's data and networks*".

Human factor has already been shown to main cause of cyber breaches, making more cyber awareness training programs are offered by educational institutions, with the aim of increasing individual awareness of cybersecurity risks and crimes [9]. Providing cybersecurity education and training activities are important. With such practical activities can ensure that employees in the organisation will acquire the actual skills necessary to promptly deal with security incidents in real situations. Training fosters cybersecurity awareness, educates employees on the importance of cybersecurity, and trains them to take the right of cybersecurity roles. Many organisations make new hires complete a cybersecurity awareness training as part of the onboarding process. Some organisations make employees take on regular basis or at least once in year to update their knowledge of cybersecurity knowledges. For example, in Japan, the National Institute of Information and Communications Technology coordinates a program named CYDER (Cyber Defense Exercise with Recurrence) that provides regular cybersecurity awareness training to IT personnel of national and local government organisations and also to large companies.

Cybersecurity training programs can take many forms, to communicate the best practices in cybersecurity, to inspire employees to change their cyber-insecure behaviours, and to improve cybersecurity behaviour over the long term [10].

2.3. Communications Channel

Communication channel refers to messages about cybersecurity communicated using multiple methods, channels and networks. Communication is a continuous, dynamic process and requires not only the correct transmission of the message over the communication channel, but also the correct interpretation and understanding of its core message that want to deliver to employees. Phone calls and email were the medium most used by employees in their day-to-day activities [11]. Currently email and face-to-face communication being employees' preferred communication channels [11]. Enterprise social media allows each individual employee to share information with other employees in the entire organisation [12]. While they found that having several social media at the workplace had benefits, such as information sharing among them.

Clear business communications require that the right information is heard by the right person at the right time over the right channel. But what works for one person may not be the same for another. Leaders must create multiple formal and informal channels for reporting cyber

incidents, sharing dynamic cyber information, and even identifying potential vulnerabilities. For example, some organisations create cybersecurity information with marketing-like campaigns, that make more attractive, to influence employee behaviours by keeping the cybersecurity issues for employees. Another example, leaders is using short communication moments at the beginning of every company meeting to share a cybersecurity message that need to address to meeting members.

3. Organisational Cybersecurity Culture

Cybersecurity culture has been defined as the behaviour of humans in an organisational context to protect information processed by the organisation through compliance with the information security policy and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives [13].

Cybersecurity culture emphasizes behaviours that comply with information security policy, but a cybersecurity culture includes not only compliance with policy, but also personal involvement in organisational cyber safety. There is consensus in the literature on the need for organisations to develop cybersecurity culture to protect their information assets [3]. The process of establishing cybersecurity culture has gained significant focus in cybersecurity literature with early work in the area aimed at establishing and understanding the concept [1].

4. Cybersecurity Protection Behaviour and Protection Motivation Theory (PMT)

Protection motivation theory (PMT) explains how individuals are motivated to respond to warnings about threats or other dangerous behaviours [14][15]. This theory is explaining an individual's intention to engage in cybersecurity protective actions [16]. PMT model focuses on developing protective behaviour to deal with threats and it has been applied to study cybersecurity problems when employees need incentives to protect their organisation's information assets [17].

Protection motivation deriving from the appraisal of the two processes of threat appraisal and coping appraisal is defined as 'an intervening variable that has the typical characteristics of a motive: it arouses, sustains and directs activity' [14]. Threat appraisal includes four subconstructs, which are perceived severity, perceived vulnerability, intrinsic reward and extrinsic reward when employees face the cyberattacks. Threat appraisal describes how individuals assess the level of danger posed by a threatening cyber-crime. Coping appraisal that consist three subconstructs, which are self-efficacy, response efficacy and response cost, refers to how individuals assess their abilities to deal with and avert the potential loss or damage arising from a threat [14].

The management in the organisations are likely to provide guidance and procedure to the employees to perform security protection actions and develop experience in fighting cyberattacks [18]. Aligning organisational environment with cybersecurity awareness will help employees to identify security threats.

Employees may have risky behaviours such sharing personal passwords, downloading illegal content, and ignoring required software updates/patches. Their findings associated these risky behaviours with employee self-feeling, defined as the feeling that cybersecurity is not a primary concern in their place of employment.

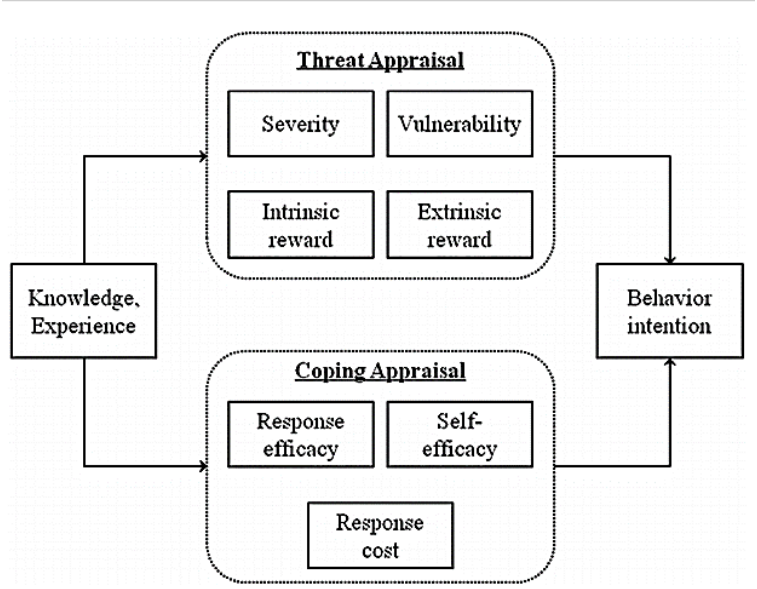

Figure 1. PMT framework with its seven subconstructs [14][15].

5. Conceptual Framework

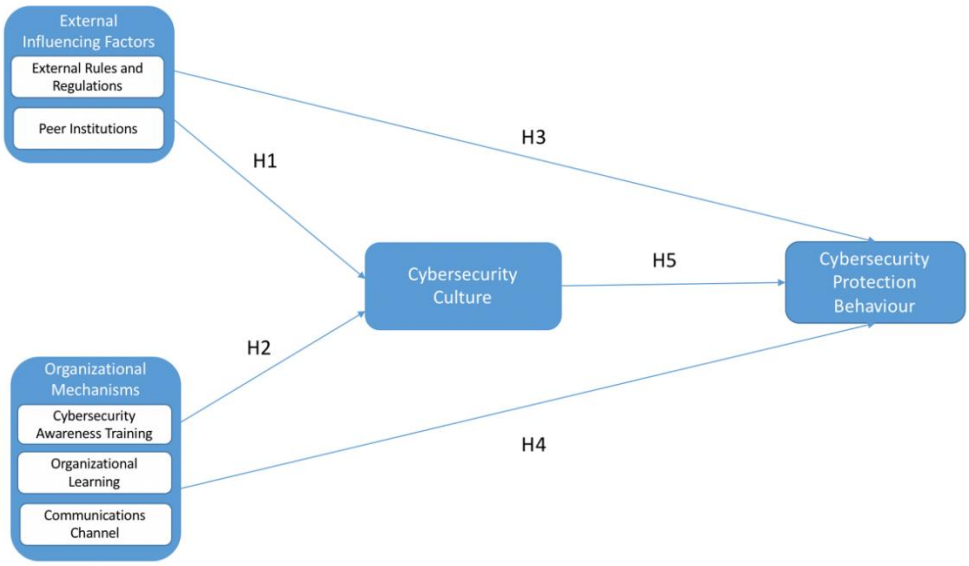

Figure 2. Research Framework on Cybersecurity Protection Behaviour.

3. DISCUSSION

Digital technology has enabled borderless connected world, digital innovation, economic growth and productivity, but in other hand it has also given rise to the risk and threat of cybercrime that possible to destroy business. Cybercrime actors now have access to a range of resources to support cyberattacks, many of these becoming more widely available, had serious cyberattacks, many as a consequence of social engineering attacks. Unfortunately, attackers seem to be more expert and understand about employee behaviour and exploit this knowledge via employees' gap with sophisticated social engineering attacks.

It's a common agreement that cybersecurity is important in all industries and organisations, and rules and regulations are factors influencing cybersecurity culture, that expecting all employees in the organisation to follow and act properly to those external influencing factors. Complying with the external industry rules and regulations, and learning from other peer institutions plays a key role in advancing cybersecurity culture. However, for employees the impact from regulations and peer institutions are important to improve individual employees' protection behaviour regarding cybersecurity.

To continually advance the cybersecurity culture maturity and engage the involvements to entire employees, the organisational learning and communications play an important role. Management in the organisation wanted to minimize employee behaviours from potential creating cybersecurity vulnerabilities and in other way they wanted to increase employee behaviours that

protect their organisation from cyberattacks. Management need to made strong decisions that influencing cybersecurity culture to employees, to keeping their technologies always up to date and using the latest cybersecurity software patches, i.e. using the latest updated antivirus software at their laptop or computer, aware for suspicious emails and websites with low or bad reputation. Communications channel focused on awareness, action and execution. The objective was for all employees to understand their individual responsibility for cybersecurity risks and threats.

Cybersecurity awareness training is a course designed to help employees understand the role they play in helping to combat information security vulnerabilities. This awareness training will help employees to understand risks and identify potential attacks such when they receive email or use the web. An employee who perceives high vulnerability to his organisation's information systems will be more willing to take protective actions. There are significant challenges, therefore, in ensuring that people are both aware of cybersecurity risks and can respond to those risks in a meaningful way. Simple policy campaigns or warning messages, intended to increase their awareness of the risks involved are not always effective, as they implicitly rely on users making very informed or rational decisions [19].

Becoming a cyber-resilient organisation is a combination of both technology and organisational investment. All the technology available to secure systems will not keep an organisation secure if the people in the organisation make bad or uninformed decisions that open up the system to threat actors. Management in the organisation continue to invest in upgraded technologies in organisational mechanisms that would increase resilience of their cybersecurity.

This paper suggests a number of ways leaders can help build a culture of cybersecurity, and how an organisation can evaluate if their culture drives cyber secure behaviours. Behaviours are driven by unwritten rules, which are difficult to see.

Management can strengthen the cybersecurity culture through decisions they make about performance, control, and governance systems. This work highlights three controls for leaders to use such as building cybersecurity expectations in creating strong communications plans, and providing ongoing training and updated opportunities for learning about increased cybersecurity activities. All are actions any leader in an organisation can take to strengthen cyber resiliency. Management can take initiative in creating a cybersecurity culture, they can expect to see results that increase resilience in the organisation. Increasing cyber-resilience is on every executive agenda will help leadership teams and all levels of management identify specific ways they can aid their organisation in achieving their main objectives; cybersecurity culture and protective behaviour.

4. CONCLUSION

Employees, as an important asset, also plays as essential part of any organisation, can contribute to organisation's cybersecurity in many ways. In order to improve individual employees' cybersecurity protective behaviour, organisations must develop relevant and engaging cybersecurity culture and awareness programs that can motivate their employees to really care about risks off cyberattacks to stay alert and behave aware.

To have more mature in cybersecurity culture, awareness and protection behaviour, management in the organisation must not only implement the latest technology but also invest in the organisational culture. The leaders are play as key role to increase the cybersecurity culture maturity level in the organisation, then it will be increased the employees' cybersecurity protection behaviour. Encouraging the attitude of cybersecurity is needed to do for everyone, so everyone can contribute to create more resiliency, at the center of cybersecurity culture, and everyone will behave protective to cybersecurity in day-to-day activities.

This paper is based on only theoretical conceptual aspects of cybersecurity culture and cybersecurity protection behaviours. This study has clear theoretical and only a conceptual paper, however, some limitations are noted. A set of qualitative/quantitative studies, survey-based, may be combined to exhaustively research upcoming and novel concepts. The future research should address this.

REFERENCES

[1] R. Van Niekerk, J. and Von Solms, "Information security culture: a management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, 2010.

[2] K. L. Thomson, R. von Solms, and L. Louw, "Cultivating an organisational information security culture," *Comput. Fraud Secur.*, vol. 2006, no. 10, pp. 7–11, 2006, doi: 10.1016/S1361-3723(06)70430-4.

[3] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, 2010, doi: 10.1016/j.cose.2009.09.002.

[4] R. Chiva, P. Ghauri, and J. Alegre, "Organisational Learning, Innovation and Internationalization: A Complex System Model," *Br. J. Manag.*, vol. 25, no. 4, pp. 687–705, 2014, doi: 10.1111/1467-8551.12026.

[5] G. F. Templeton, B. R. Lewis, and A. Charles, "Journal of Management Development of a Measure for the Organisational Learning Construct," no. July, 2012, doi: 10.1080/07421222.2002.11045727.

[6] F. Garvin, D. A., Edmondson, A. C., & Gino, “Is yours a learning organisation?,” *Harv. Bus. Rev.*, vol. 86, pp. 109–116, 2008.

[7] D. A. Argyris, C., & Schön, “Organisational learning II: Theory, method, and practice (2nd ed.),” *Reading, MA Addison-Wesley*, 1996.

[8] R. S. Shaw, C. C. Chen, A. L. Harris, and H. J. Huang, “The impact of information richness on information security awareness training effectiveness,” *Comput. Educ.*, vol. 52, no. 1, pp. 92–100, 2009, doi: 10.1016/j.compedu.2008.06.011.

[9] R. C. Dodge, C. Carver, and A. J. Ferguson, “Phishing for user security awareness,” *Comput. Secur.*, vol. 26, no. 1, pp. 73–80, 2007, doi: 10.1016/j.cose.2006.10.009.

[10] I. Katz, “Cybersecurity awareness training: How to improve employee security behaviour,” 2017.

[11] T. Turner, P. Qvarfordt, J. T. Biehl, G. Golovchinsky, and M. Back, “Exploring the workplace communication ecology,” *Conf. Hum. Factors Comput. Syst. - Proc.*, vol. 2, pp. 841–850, 2010, doi: 10.1145/1753326.1753449.

[12] P. M. Leonardi, M. Huysman, and C. Steinfield, “Enterprise social media: Definition, history, and prospects for the study of social technologies in organisations,” *J. Comput. Commun.*, vol. 19, no. 1, pp. 1–19, 2013, doi: 10.1111/jcc4.12029.

[13] A. da Veiga, L. V. Astakhova, A. Botha, and M. Herselman, “Defining organisational information security culture—Perspectives from academia and industry,” *Comput. Secur.*, vol. 92, p. 101713, 2020, doi: 10.1016/j.cose.2020.101713.

[14] R. W. Rogers, “A Protection Motivation Theory of Fear Appeals and Attitude Change1,” *J. Psychol.*, vol. 91, no. 1, pp. 93–114, 1975, doi: 10.1080/00223980.1975.9915803.

[15] J. E. Maddux and R. W. Rogers, “Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change,” *J. Exp. Soc. Psychol.*, vol. 19, no. 5, pp. 469–479, 1983, doi: 10.1016/0022-1031(83)90023-9.

[16] P. Ifinedo, “Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory,” *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, 2012, doi: 10.1016/j.cose.2011.10.007.

[17] P. Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, “What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviours in users,” *MIS Q.*, vol. 39, no. 4, pp. 837–864, 2015.

[18] A. Ahmad, S. B. Maynard, and G. Shanks, “A case analysis of information systems and security incident responses,” *Int. J. Inf. Manage.*, vol. 35, no. 6, pp. 717–723, 2015, doi: 10.1016/j.ijinfomgt.2015.08.001.

[19] G. L. ACQUISTI, ALESSANDRO, BRANDIMARTE, LAURA, “Privacy and human behaviour in the age,” *Science (80-.).*, vol. 347, no. 6221, pp. 509–514, 2015.