The Asian Journal of Shipping and Logistics 37 2021 20–36

Contents lists available at ScienceDirect

The Asian Journal of Shipping and Logistics

journal homepage: www.elsevier.com/locate/ajsl

Original Article

Port cybersecurity and threat: A structural model for prevention and policy development☆

Chalermpong Senarak

Department of Nautical Science and Maritime Logistics, Faculty of International Maritime Studies, Kasetsart University, Sriracha Campus, 199 Moo 6, Sukhumvit Road, Tung Sukla, Sri Racha, Chon Buri 20230, Thailand

ARTICLE INFO

Article history:
Received 11 November 2019
Received in revised form 26 April 2020
Accepted 18 May 2020

Keywords:
Cyberthreat
Port cybersecurity hygiene
Cybertechnology
Prevention and policy development
Port digitalization
Structural equation modeling

ABSTRACT

Most port operators have increasingly integrated cybertechnology into port activities to increase their competitiveness; unfortunately, this digitalization becomes the major vulnerability for the emerging cyberthreat. To help port policymakers develop cybersecurity measures, this study conceptualized and developed three dimensions of port cybersecurity hygiene (i.e. human, infrastructure, and procedure factors) and investigated the relationships between port cybersecurity hygiene and cyberthreats (i.e. hacktivism, cyber criminality, cyber espionage, cyber terrorism, and cyber war). A questionnaire survey was used to collect data from all international container port operators and shipping lines with branches in Thailand, and the proposed relationships were tested by structural equation modeling. The results indicated that container ports tended to encounter hacktivism when their human, infrastructure, and procedure factors were vulnerable. The weakness of the human factor could also lead to cyber terrorism, while the deficiency of the infrastructure factor could lead to cyber criminality. Moreover, container ports were likely to be harmed by cyber espionage if their procedure factor was poorly implemented. Hence, the provision of training and education to all port workers, including top executives, managers, and supervisors, are necessary to ensure a cyberthreat-awareness culture at all organizational levels. Improving cybersecurity equipment could prevent unauthorized access to port business data and keep important information secure, while the ISPS Code-based procedures and other preventive measures should be strictly implemented by container ports to reduce the risk of cyberthreats.

1. Introduction

The maritime industry is becoming increasingly digitalized. Over decades, most maritime operators have adopted digital technologies to modify their business model and upgrade process efficiency to create value for customers (Shepherd, 2004), comply with legal requirements (Chao & Lin, 2009), and generate a competitive advantage (Barnes & Oloruntoba, 2005). Clear evidence is provided by the shipping segment. For example, over 90% of the global merchant fleet uses digital systems: to connect with digital navigation networks such as ECDIS, GNSS, AIS, VDR and radar (ICS, 2018); to support access control to ensure physical security, administration of the ship or the welfare of the crew, and communication among ships, shippers, and seaports (Tsai, 2006); to support the loading, management and control of cargo, make cargo manifests, loading lists, and other documents (ICS, 2018); and to replace manual systems for monitoring and controlling onboard machinery and the propulsion and steering of most modern vessels (Yeo, Pak, & Yang, 2013). As a logistics center and linkages with shipping lines becomes digitalized, container ports have the inevitable duty to integrate cybertechnologies into port activities, such as process design (Lee & Whang, 2005), cargo handling and navigation (Yeo et al., 2013), environment and pollution prevention, and risk management (ICS, 2018), and port safety and security (Tsai, 2006). In some cases, the container ports digitalize their operation in order to comply with international and national practices, such as the installation of AIS as required by the SOLAS Convention (IMO, 2019a, 2019b, 2019c), the use of hybrid-electric technologies to replace pure diesel engine vehicles and equipment in ports as required by the MARPOL Convention (IMO, 2019a, 2019b, 2019c), X-ray and gamma-ray imaging systems for safety and security purpose as required by the ISPS Code (Homeland Security, 2018), and the development of a digital network to support electronic transactions with government departments through the National Single Window System as encouraged by the national government (Pintong, 2010). Apart from external forces, the desire of port operators to

☆ Peer review under responsibility of the Korean Association of Shipping and Logistics, Inc.

https://doi.org/10.1016/j.ajsl.2020.05.001

improve port efficiency and competitiveness is another great force internally driving increased digitalization, such as the adoption of automated vehicles and stacking cranes, gate automation, optical characters recognition, license plate recognition, automated teller machines, e-tracking services, and wireless devices (Chao & Lin, 2009). Based on the digital transformation rate in the maritime industry, global hub ports will be completely digital in less than a decade.

Nevertheless, the vulnerabilities created by accessing, interconnecting, or networking with these cybertechnologies and digital systems can lead to cyberthreats (IMO, 2017). It was reported that many leading ports and shipping operators have encountered cyberthreats costing them huge amounts of money for the business outage and system recovery. Some of the biggest cases have been the cyberattacks on the system of the Greek Shipping Company in 2010, the Iranian Shipping Line in 2011, Australian Customs and Border Protection Service agency in 2012, Port of Antwerp in 2013, Danish Port Authority in 2014, the Mearsk Line in 2017, and the COSCO Shipping Lines in 2017 (Ahokas, Kiiski, Malmsten, & Ojala, 2017; Kapalidis, 2018). Based on the above cases, more than 80% of cyberthreats were due to the weakness of port cybersecurity (Kapalidis, 2018) and the lack of a port prevention policy (Tonn, Kesan, Zhang, & Czajkowski, 2019). This highlights the essential role of port cybersecurity and policy in preventing container ports and shipping firms from malicious cyber actions. Unfortunately, a review of the literature shows the deficiency of knowledge regarding cyberthreat and cybersecurity regarding container ports. More than 90% of the research papers discovered from the online databases of Scopus, Web of Science, and ScienceDirect, do not focus on port cybersecurity and threats, but rather concentrate on port physical security, such as the studies of Roach (2004), Tsai (2006), Orosz et al. (2009); Papa (2013), Janssens-Maenhout, Roo, and Janssens (2010), McLay and Dreiding (2012), Michel, Mendes, Ruiter, Koomen, and Schwaninger (2014), McNicholas (2016), and Pallis (2017). This review also demonstrated that most scholars focused on the development of risk assessment methods that were claimed as effective approaches enabling port operators to identify vulnerabilities in ports and to select suitable measures to reduce natural and man-made hazards, such as the studies of Orosz et al. (2009), Mansouri, Nilchiani, and Mostashari (2010), McLay and Dreiding (2012), Chang, Xu, and Song (2014), John et al. (2014), Loh and Thai (2014), Yang, Ng, and Wang (2014), Johnstone (2015), and Pallis (2017). Adopting advanced technologies to improve physical port security is another attractive area for most academics (Tsai, 2006; Mansouri et al., 2010; Janssens-Maenhout et al., 2010; Scholliers, Permala, Toivonen, & Salmela, 2016), while some studies have attempted to explore other approaches to improve physical port security, such as the international collaboration among governments (Papa, 2013), national laws and regulation to support the implementation of port security measure (Roach, 2004), and national policy to support investment in critical cybersecurity infrastructure (King, 2005). Some studies have analyzed cybersecurity in general, but most of the issues were not related to container ports. However, port cybersecurity is directly explored in the works of Ahokas et al. (2017), Homeland Security (2018), Bermejo (2010), and Moerel and Dezeure (2017). Even though the components of cybersecurity has already been documented by Kapalidis (2018) and the different types of cyberthreats encountered by maritime operators have been discussed by Ahokas et al. (2017), Moerel and Dezeure (2017) and Homeland Security (2018), the working process of each element in port cybersecurity is still unknown and the body of knowledge enabling port managers and policy makers to understand how port cybersecurity is threatened by different cyberthreats is still deficient.

Using Laem Chabang Port as a case study, the current study aimed to narrow the literature gap by creating a novel model demonstrating the integral elements of port cybersecurity hygiene and its relationship with five groups of cyberthreats. The author examined the relationships by using covariance based SEM. The rest of this paper is organized as follows. In Section 2, the author reviews the literature on port cyberthreat and cybersecurity hygiene to provide a theoretical background and considered concepts for developing the conceptual research model which was used as the reference for developing research hypotheses. Section 3 explains the research methodology of this study, while the result for the measurement model is explained in Section 4. This is followed by the explanation of results for the structural model in Section 5 and the discussions in Section 6. Section 7 is the last part containing the conclusions.

1.1. *Laem Chabang Port*

Leam Chabang Port (LCP) is the largest container port located on the east coast of Thailand (see Fig. 1). Located at the center of the region, LCP has played an important role in driving the economic growth of not only the country but also the ASEAN region. Its service is used by many global shipping lines, such as CMA CGM, CNC, ONE, Evergreen Marine, Maersk Line, KMTC, SITC, Mitsui OSK Lines, Wan Hai Lines, APL, Yang Ming, and Hapag-Lloyd Container Shipping. As a result, LCP is linked to more than 141 worldwide ports (Civil Engineering Division, 2015). Currently, there are two phases in LCP comprising 18 terminals. LCP Phase 1 consists of 11 terminals (Terminals A0-A5 and Terminals B1-B5), and LCP Phase 2 contains 7 terminals (Terminals C0-C3 and Terminals D1-D3). They provide services to containers vessels, general cargo vessels, roll-on/roll-off ships, bulk carriers, passenger ships, and flat-bottomed boats (Laem Chabang Port, 2019a, 2019b, 2019c). Over a decade, the container throughput of LCP has continuously increased, rising from 5.08 million of TUEs in 2010 to 8.01 million of TUEs in 2019 (Laem Chabang Port, 2019a, 2019b, 2019c), as illustrated in Fig. 2.

Due to the growing demand for domestic and regional container transportation, the LCP-Phase 3 project becomes one of the most important megaprojects contained in Thailand's Eastern Economic Corridor (EEC) development plan. LCP Phase 3 aims to increase container handling capacity from 7.7 million TEUs/year to 18.1 million TEUs/year by establishing Terminals E1, E2, F1, and F2 with investment value from public-private partnerships of THB 155.834 billion (EECO, 2018). The investment of LCP Phase 3 focuses on automation technologies, green equipment, and electronic systems in order to support the Sustainable Development Goals of the United Nations (Laem Chabang Port, 2019a, 2019b, 2019c). It is believed that the EEC development plan can be achieved by technology-driven innovation and collaboration among government agencies, private sectors, educational institutes, and communities in an innovation ecosystem. Hence, all areas in EEC (i.e. Chachoengsao, Chonburi, and Rayong provinces), including LCP, are full of the digital and innovative ecosystems, such as the Digital Park Thailand, eight digital clusters, the First S-Curve industry (e.g. automotive, smart electronics, affluent, medical and wellness tourism, agriculture and biotechnology, and food for the future), and the New S-Curve (e.g. robotics, aviation and logistics, biofuels and biochemicals, digital industry, and medical hub) (BOI, 2019). The investment of these targeted industries is supported by the financial incentives of the Board of Investment of Thailand (BOI, 2019).

1.2. *Cybersecurity and threat in Thailand and Laem Chabang Port*

The Global Cybersecurity Index in 2018 indicated that the Thai government has put a great effort into improving cyber competency in terms of data protection laws (ITU, 2018). Despite being

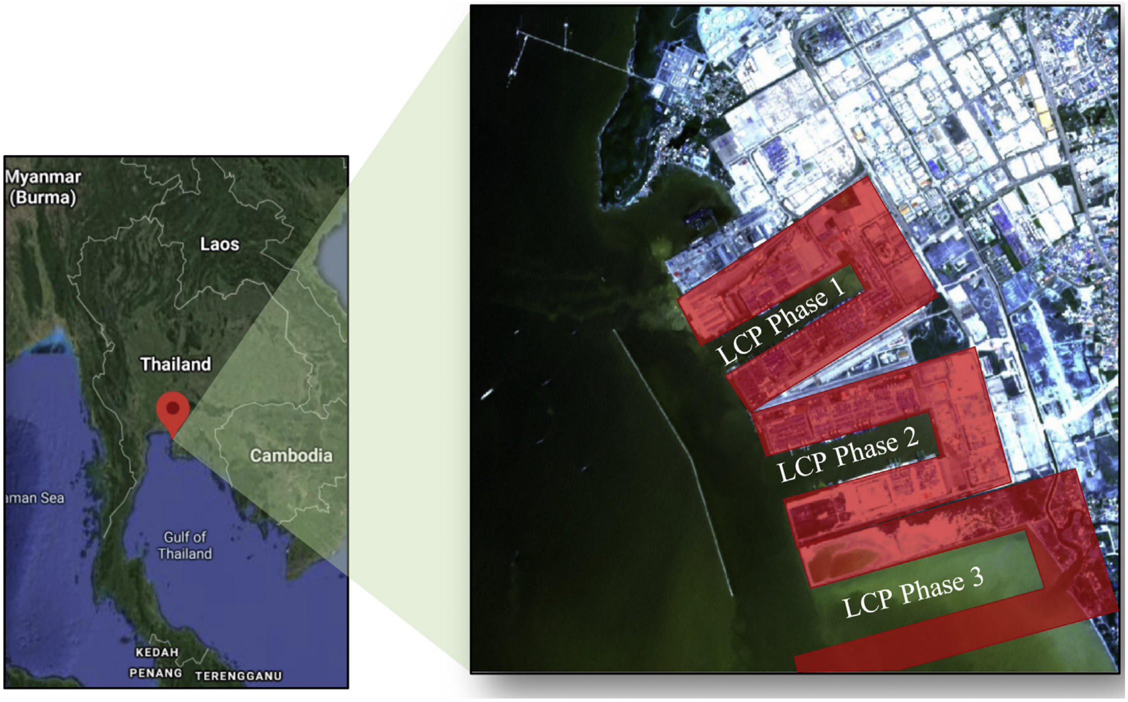

Fig. 1. The satellite view of LCP in Chonburi Province, Thailand.
Source: Google Maps (2020) and United States Geological Survey (2020).
Remark: The left picture was drawn from Google Mapes by Google and the right picture was drawn from EarthExplorer by the United States Geological Survey and modified in QGIS version 3.0.

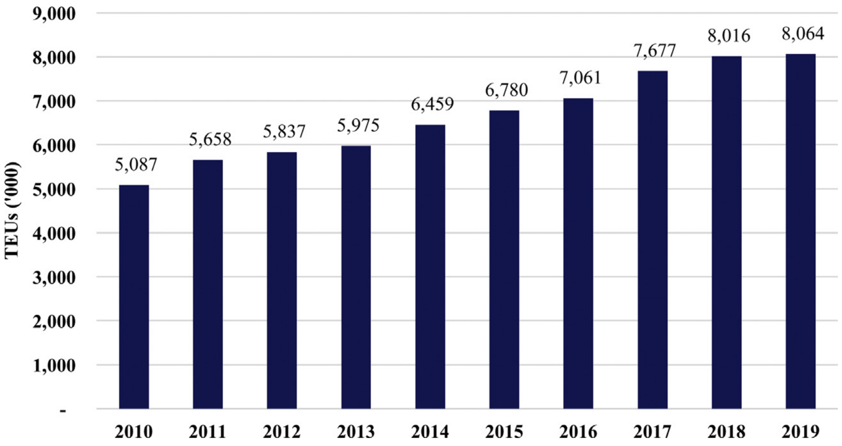

Fig. 2. Container port throughput at LCP. *Source*: Port Authority of Thailand, based on data from performance reports 2010–2019.

ranked in the top 10 best-prepared countries for cyberattacks in the Asia-Pacific region, Thailand is one of the countries that is experiencing a huge amount of cyberattacks each year. Table 1 shows that the number of cyber incidents in both the private and public sectors in Thailand has continuously increased since 2011 and reached the highest point in 2016 (4371 reports of the cyber incident). It was reported that fraud, intrusion attempts, and malicious code are the top three most frequently reported types of cyber incidents (TCERT, 2019). For the public and governmental sectors, the abusive content was the most common threat used to attack the office of the prime minister. The intrusion attempt was the threat usually encountered by the independent public agencies and the court of Thailand, while the Denial of Service (DDoS), including Open DNS Resolver, Flood, and Sabotage, was frequently used to attack the computer network of public organizations, professional qualification institutes, state enterprises, and state universities (TCERT, 2016). For the private sector, the financial sector was repeatedly threatened by the act of fraud (e.g. web phishing, masquerade, and unauthorized use of resources and copyright). The energy business was frequently attacked by the abusive content, whereas the securities company was frequently attacked by the intrusion attempt (TCERT, 2016). Unlike other sectors, 107 firms in the transportation, logistics, and port sectors reported that they were mainly attacked by two types of cyberthreats. The first one was the malicious code using malware, virus, worm, trojan, and ransomware to control the firms' system and steal secret information. The second one was the DDoS used to disrupt the regular operation of the firm (TCERT, 2016). They explained that the use of digital technologies becomes more common in port and transportation industry in Thailand, this modern environment will pose a greater risk of cyberthreats and the need to maximize protection.

Table 1
Cyber incidents in public and private sectors in Thailand (number of reports).

Incident type/year	2011	2012	2013	2014	2015	2016	2017	2018	2019
Abusive content	77	3	13	8	8	0	0	1	124
Availability	6	2	10	8	6	29	540	0	79
Fraud	309	534	694	1007	1141	1002	841	929	912
Information gathering	93	62	8	29	0	0	8	0	60
Information security	0	2	0	4	1	20	68	18	165
Intrusion Attempts	94	75	316	504	664	706	939	1102	467
Intrusions	0	13	631	709	1005	1020	570	335	218
Malicious code	63	82	73	1738	1546	1020	271	127	436
Other	4	19	0	0	0	0	0	8	9
Total	646	792	1745	4007	4371	3797	3237	2520	2470

Remark: Statistics are based on the ThaiCERT's incident reports from 2011 to 2019.

To minimize the cyber risk in the port industry, Port Authority of Thailand (PAT) has taken measures and policies to prevent upcoming cyber threats in LCP and other state-owned ports. The initial measure focuses on the information security management system (ISMS) of the port. As PAT holds the ISO 27001 certification, the regulation of ISO 27001 is strictly used as a reference to develop the internal policies and procedures for systematically managing the security of assets, such as financial information, intellectual property, employee details, and information entrusted by third parties (PAT, 2018a, 2018b). To comply with the ISO 27001, PAT obliges to ensure that the ISMS is based on the information risk management process that includes all legal, physical, and technical perspectives. Additionally, the maritime cyber risk management suggested by the International Maritime Organization is also used to improve a port risk assessment process to recognize the full range of the cyber risk from digitization, integration, automation, and network-based systems that the port and data might encounter. By doing this, PAT can develop the appropriate emergency preparedness plan, mitigation measure, safety management system, cybersecurity, and strategy for reducing the cyber risk or increasing awareness of cyber risks at all levels of an organization (PAT, 2018a, 2018b; IMO, 2019a, 2019b, 2019c). Another port cybersecurity measure concentrates on the improvement of knowledge and competency of the port staff (Office of the Official Information, 2020). PAT and LCP regularly provide training courses to address the dangerous behavior and increase cybersecurity awareness of employees, managers, and directors of the port organization, such as data and IT security training, IT systems operations and maintenance, network security, regulatory and standards compliance, and security risk management (TCERT, 2018). Apart from these measures, PAT and LCP heavily attempt to link the port facility security with port cybersecurity by adopting the regulation of the International Ship and Port Facility Security (ISPS) Code to design the internal port operation to support their cybersecurity (PAT, 2018a, 2018b). For instance, only persons and vehicles with an admission card issued by the security center are allowed to enter for port business contacts. This could prevent malicious outsiders from passing into the port and accessing the secret information (PAT, 2018a, 2018b). Likewise, only authorized officers could access into and out of specific areas; and the personal information of port staffs, including port transaction data, could not be accessed by any unauthorized officers to prevent the information from any unauthorized use and to comply with the Personal Data Protection Act, B.E. 2562 (2019) (PAT, 2018a, 2018b).

The Cyber Security Act, B.E. 2562 (2019) is another important law in the port industry of Thailand. This act was enforced in 2019 to prevent and combat any unlawful actions done using a computer, etc., to cause damage or harm to a computer system, computer data, or other relevant data (TSPM, 2019). The regulation of this act empowers the related governmental authority to determine the response measure for handling the cyberthreat and offender, such as examining computers, computer systems, and cyber data, seizing computers, computer systems, any other equipment, and penalizing the offender by fines or other punishments. Another related law is the Official Information Act, B.E. 2540 (1997). This act enables LCP to enhance port cybersecurity by concealing important information from the public (Office of the Official Information, 1997). LCP may issue an order prohibiting the disclosure of official information if the disclosure will (1) jeopardize the national security, international relations, national economic, or financial security, (2) result in the decline in the efficiency of law enforcement or failure to achieve its objectives, (3) endanger the life or safety of any person, and (4) unreasonably encroach upon the right of privacy, etc. In addition to law enforcement, the Thailand Computer Emergency Response Team (ThaiCERT) was specifically established by National Electronics and Computer Technology Center to monitor and handle computer security incidents in all cyber communities in Thailand (TCERT, 2000). ThaiCERT also provides other necessary supports to ports and other institutes in order to enhance the national cybersecurity, such as a digital forensic examination by certified examiners, reporting service in compliance with current international standards, and cyber incident handling.

2. Literature review and hypothesis development

2.1. *Cyberthreats*

Research papers regarding port security and threat have been published since the terrorist attacks on the World Trade Center and the Pentagon in the United States (McNicholas, 2016). Many scholars revealed that the important infrastructure, especially transportation sector, was the target of the terrorist, such as hijacking and migrant smuggling (Roach, 2004), information risk of transit containers in Taiwanese ports (Tsai, 2006), maritime terrorist attacks (Orosz et al., 2009; Papa, 2013), illicit trafficking of fissionable material in container cargoes (Janssens-Maenhout et al., 2010), smuggling nuclear material into the USA for nuclear terrorism (McLay & Dreiding, 2012), transportation of dangerous weapons of terrorist organizations (Michel et al., 2014), cargo thieves, stowaways, pirates, and drug smugglers (McNicholas, 2016), and vandalism, illegal immigration, and blockade (Pallis, 2017). Due to the increasing number of terrorist attacks in maritime transport chain, the safety of container cargo and security measure of seaport became the attractive issue in the global arena. Since automated technology has been adopted in the maritime industry, port operators and sea carriers become the target of cybercrime (Choong-Hee, Soon-Tai, & Sang-Joon, 2019). Table 2 summarizes the cyberattacks exposed by leading shipping lines, shipbrokers, logistics companies, and large container ports. The literature review demonstrated that the approach and motivation for conducting cyberthreat differed from case to case. Among these, the ransomware was the most frequently used threat for

Table 2
Cyberattacks in maritime transport industry.

Firm	Type of operator	Type of cyberattack	Year	Source
Islamic Republic of Iran Shipping Lines	Shipping line	Cyberattack	2011	Torbati and Saul, (2012); Hayes (2016)
Japanese and Korean shipbuilding	Ship builder	Advanced phishing attacks Persistent threat	2013	Hayes (2016); Shaikh (2017); ICS (2018)
Maritime industry in South Korea	Shipping line Port operator	Cyberattack	2016	Shaikh (2017); Nichols (2016)
Maersk line and Maersk group's APM Terminals	Shipping line Port operator	Malware Cyber extortion	2017	Jensen (2017); Fosen (2019)
BW Group	Shipping operator Floating gas infrastructure	Hacktivism	2017	Fosen (2019)
FedEx	Logistics company	Wiper virus for deleting data	2017	McKevitt (2017)
Clarkson Plc	Shipbroker	Hacktivism	2017	Kennard (2019)
Port of Barcelona	Port operator	Ransomware attack	2018	Aharoni (2018)
COSCO terminal in Long Beach Port	Port operator	Ransomware attack	2018	Aharoni (2018); Fosen (2019)
US Port of San Diego	Port operator	Cybersecurity incident Ransomware attacks	2018	The Institute of Marine Engineering, Science and Technology (2018)
Total Quality Logistics (TQL)	Logistics company Freight broker	Data phishing attempt	2020	TQL (2020); Forde (2020)
Toll Group	Freight forwarder	Ransomware attack	2020	Otago Daily Times (2020)

disrupting the computer networks and servers, such as the attacks in Port of Barcelona (Aharoni, 2018), Port of San Diego (The Institute of Marine Engineering, Science and Technology, 2018), COSCO terminal in Long Beach Port (Fosen, 2019), COSCO Shipping Lines (Homeland Security, 2018), and Toll Group (Otago Daily Times, 2020). This was followed by the phishing attempt, malware, and virus for data destruction and cyber extortion. For example, in 2017 Maersk line and 76 terminals of A.P. Moller Maersk were attacked by malware for cyber extortion, costing the firm approximately USD 300 million and causing disrupted operations for many weeks (Ahokas et al., 2017; Jensen, 2017; Fosen, 2019).

Based on the work of Ahokas et al. (2017), shipping and port operators might be targeted by five categories of cyberthreats, namely, hacktivism, cybercrime, cyber espionage, cyber terrorism, and cyber war. Each has a different definition and characteristics. For example, the hacktivism means the operation in cyberspace using different hacking techniques (e.g. malware) to invade into web pages and on computers, and create pressure on a certain object. The aim for conducting hacktivism varies from gaining attention with his/her actions to disrupting business through the vulnerable gaps in the cyberspace (Ahokas et al., 2017). The cyber criminality refers to criminal activities that are deemed injurious to the public welfare and are legally prohibited. The motivation to conduct cyber criminality is normally to exploit human or security vulnerabilities in order to steal passwords, data, or money directly, such as using bogus emails to ask for security information and personal details (National Crime Agency, 2017). Sometimes, it aims to (1) gain financial benefits, (2) inflict personally motivated harm, (3) endanger confidentiality and availability of data and systems, or (4) violating a firm's reputation and brand (Christou, 2016). Like hacktivism, the cyber espionage is the illegal access to secret and delicate information (e.g. company strategy, private information, or intellectual capital). However, the cyber espionage aims to gain competitive advantages rather than create pressure and business disruption (Ahokas et al., 2017). Thus, the consequences might be the loss of intellectual property, business profits and efficiency, and customer information, additional costs thanks to the interrupted business plan, and damage to company reputation (Platt, 2011). In contrast, cyber terrorism is a politically-motivated attack of by cyberterrorist (e.g. international groups or secret agents) using various tools (e.g. computer viruses, computer worms, phishing, and other malicious software) to violate the information, computer systems, computer software, and databases of important organizations or global networks in order to accomplish the political or ideological gain (Ahokas et al., 2017). Thus, the cyber terrorism normally causes serious consequences, such as massive damage to government systems and national security programs, or loss of life or significant bodily harm (Limnéll, Majewski, Salminen, & Samani, 2015). The last category of cyberthreats is the cyber war which is a part of the modern information war between nations. In general, it is relevant to the military affair aiming to disable the military target by using malicious software, viruses, and other technologies (Lewis, 2002). Apart from the military, the cyber war might be done by the state-sponsored actor (e.g. terrorist groups, companies, political, or ideological extremist groups) to attack the opponent's computer networks (Green, 2015). Over decades, the hacktivism, espionage, denial-of-service attack, and disruption of electrical power grid have been found as the popular attack in cyber war (Homeland Security, 2018), but these actions could present a multitude of threats toward a nation (Weinberger, 2007). In cyber war, the computers and satellites might be used to disturb the critical water, power, fuel, communications, and transportation infrastructure that leads to disastrous consequences (Lewis, 2002). This infrastructure includes port infrastructure that is the key node of global trade holding substantial amounts of data and monetary transactions among stakeholders. This makes ports attractive for cyberattacks, especially the leading ports with a high degree of interconnection and lacking adequate cybersecurity (Ahokas et al., 2017; Lewis, 2002; Moerel & Dezeure, 2017). This argument is consistent with that of Tonn et al. (2019) who explored that the transportation infrastructure of most countries was the target of hackers, criminal organizations and thieves, state-sponsored attackers and spies, other companies or organizations, terrorists, malicious insiders, and contractors, resulting in customer data breaches, property damage or theft (e.g. accidents caused by compromising signaling systems), data damage (e.g. hacking maritime cargo management systems), loss of income due to outages and failure, website defacement, and cyber extortion. Based on the above explanation, this study gathered all cyberthreats exposed by port and other industries and classified them into five categories based on the approach of Ahokas et al. (2017), as presented in Table 3.

2.2. Port cybersecurity

Port cybersecurity is an important issue for port authority who takes responsibility for ensuring port safety and security. Basically, the port authority has powers and duties to issue general and specific regulations for regulating and controlling the

Table 3
Characteristics of cyberthreat.

Cyberthreat category	Objective	Cyberthreat	Sources
Hacktivism	■ To invade web pages and computers to create pressure	■ Hack by malware ■ Hack by ransomware ■ Credential theft ■ Privacy violation	Moerel and Dezeure (2017) Homeland Security (2018)
Cyber criminality	■ To gain financial benefits ■ To inflict personally motivated harm	■ Revenge or bullying ■ Criminal damage ■ Robbery of cargo ■ Identity theft ■ Data breach ■ Data damage ■ Illicit gambling or spreading false information ■ Copyright or brand violation	Ahokas et al. (2017) Tonn et al. (2019)
Cyber espionage	■ To gain competitive advantage and intellectual property of other business ■ To interrupt business operations ■ To damage company reputation	■ Illegal access to secret and delicate information such as company strategy, private information or intellectual capital ■ Cyber extortion ■ Information stealing ■ Insiders gaining unauthorized access to information systems ■ Intruder having direct physical access to systems and the network ■ Cross contamination ■ Cyber fraud	Ahokas et al. (2017) Homeland Security (2018)
Cyber terrorism	■ To politically attack information, computer systems, computer software and databases	■ Outage and information system failure ■ Website defacement ■ Subversion of security control Sabotage	Moerel and Dezeure (2017) Tonn et al. (2019)
Cyber war	■ To fight against opponent countries by damaging or disabling their rivals' computer networks, especially relevant to military affairs	■ Sabotage at national level ■ Disruptive attacks by state actors	Ahokas et al. (2017) Moerel and Dezeure (2017)

information exchange, communication, and digital transaction between terminal operators and their users within the framework of the ISPS Code (ESCAP, 2019; IMO, 2019a, 2019b, 2019c). To make sure that the relevant regulations are disseminated to all involved parties, the terminal operator will act in the interest of the port authority by issuing the effective security procedures and communicating them to the shipping line and other relevant operators (The World Bank, 2007). Based on this practice, one of the most important causes making port operators vulnerable to cyberthreats was the insufficient cybersecurity and policy to protect their digital assets and infrastructure (Ahokas et al., 2017; Homeland Security, 2018; Moerel & Dezeure, 2017). To maintain port cybersecurity, cooperation with the major partnerships is the first step to accomplish (Silgado, 2018), while standardizing the concept for regulating port and vessel cybersecurity is another key for cyberthreat protection. For this reason, ISPS Code plays the most important role in port cybersecurity.

ISPS code was launched in 2004 by the International Maritime Organization (IMO) for enforcing its regulation on all vessels over 500 GRT sailing the international trade routes and cargo transportation in ports (IMO, 2019a, 2019b, 2019c). As it is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988), ISPS Code heavily focuses on the minimum-security arrangements for ships, ports, and government agencies. To regulate all relevant operators, the special measures of the ISPS Code is implemented through the security regulation in chapter XI-2/3, XI-2/6, and XI-2/8 (IMO, 2014). The regulation in chapter XI-2/3 focuses on the procedure onboard the vessel and in port. It determines all ships that are prior to docking in port must immediately comply with all requirements for security levels that are determined by that contracting government (IMO, 2014). The regulation in chapter XI-2/6 concentrates on the security facility and equipment onboard the vessel. All firms must make sure that all ships are equipped with a security alarm system efficiently communicating from the ship to the onshore administration via satellite system. The regulation in chapter XI-2/8 focuses on humans. It establishes the main role of the ship master, allowing him to maintain order and conduct decisions for the sake of the personnel and security of the ship (IMO, 2014). Every port must designate a port facility security officer to take care of the development, implementation, revision, and maintenance of the port facility security plan and for liaison with the ship security officer and company security officer (IMO, 2014). Additionally, the PFSO is authorized to enter port facilities and to board ships to make inquiries, examinations, inspections, searches, seizures, and to apprehend in accordance with the ISPS Code; exercise control measures over ships within the port; and implement all security measures and exercise the Port Facility Security Plan as required by the ISPS Code.

The ISPS Code highlights the importance of human working onboard the vessel and in port, security equipment and infrastructure, and procedure for cybersecurity protection. This implies that port cybersecurity hygiene depends heavily on three main factors, namely human, infrastructure, and procedure, which enable firms to prevent cyber infrastructure and asset loss from cyberthreats (Moerel & Dezeure, 2017; Kapalidis, 2018). Regarding the human factor, a firm employing workers who have IT skill and cybersecurity knowledge could reduce the cyber risk. To ensure this, training courses should be provided to improve the knowledge, skill, awareness of IT staff and other employees, including executives of the firms; this was critical for the success of cybersecurity measures (Kapalidis, 2018). Additionally, a response team comprising IT staff, designated port security officers and top executives, should be specifically formed to deal with malicious acts (Ahokas et al., 2017) and to ensure a cyberthreat-awareness culture at all organizational levels (Moerel & Dezeure, 2017). The argument of Ahokas et al. (2017), Moerel and Dezeure (2017), and Kapalidis (2018) revealed that providing the training courses to all workers and setting up port cybersecurity team would ensure a cyberthreat-awareness culture at all organizational levels and reduce the cyber risk, while the studies of Lewis (2002), Ahokas et al. (2017), Moerel and Dezeure (2017), and Tonn et al. (2019) pointed out that ports hold substantial amounts of data and a number of financial transactions making them attractive for cyberattacks. Thus, port operators with a high degree of interconnection and lacking adequate cybersecurity could encounter with hacktivism (Ahokas et al., 2017), cyber criminality (Christou, 2016), cyber espionage (Platt, 2011), cyber terrorism (Limnéll et al., 2015), and cyber war (Green, 2015; Lewis, 2002). Hence, it is reasonable to believe that a higher capability regarding the human factor will reduce the opportunity for cyberthreats in container ports. In contrast, container ports tend to encounter cyberthreats when their human factor is vulnerable. Thus, it was hypothesized that:

H1a. The lower the human factor, the higher the hacktivism.

H1b. The lower the human factor, the higher the cyber criminality.

H1c. The lower the human factor, the higher the cyber espionage.

H1d. The lower the human factor, the higher the cyber terrorism.

H1e. The lower the human factor, the higher the cyber war.

Regarding the infrastructure factor, Kapalidis (2018) considered that managers and policy makers should take into account the investment of infrastructure to maintain cybersecurity of the internet-based technologies that have been adopted by most modern companies. This includes the modern container ports which have increasingly integrated into port activities automatic and digital technologies (e.g. automated cargo handling equipment and vehicles (Boyes, Isbell, & Luck, 2016), smart office building, Internet of Things devices (Boiko, Shendryk, & Boiko, 2019), automated cargo container tracking system (Moerel & Dezeure, 2017), traffic control system (Vorakulpipat, 2013), and intelligent warehouse control system (Ahokas et al., 2017)). Without security infrastructure (e.g. firewalls, software encryption, virus detection, and system compartmentalization), a container port could easily be harmed by cyberthreats because the infrastructure factor dominates the capability of container ports in protecting cyberthreat. Therefore, the investment in security infrastructure, such as firewalls, software encryption, virus detection, and system compartmentalization, could help reduce cyber risk in modern container ports. Contrarily, the deficiency of port cybersecurity infrastructure could increase the opportunity of hacktivism (Ahokas et al., 2017), cyber criminality (Christou, 2016), cyber espionage (Platt, 2011), cyber terrorism (Limnéll et al., 2015), and cyber war (Lewis, 2002; Green, 2015) in ports. Thus, it is reasonable to believe that the container port with higher infrastructure factors could reduce the risk for cyberthreats, while those with lower infrastructure factors would increase the likelihood of cyberthreats. Based on this argument, it was hypothesized that:

H2a. The lower the infrastructure factor, the higher the hacktivism.

H2b. The lower the infrastructure factor, the higher the cyber criminality.

H2c. The lower the infrastructure factor, the higher the cyber espionage.

H2d. The lower the infrastructure factor, the higher the cyber terrorism.

H2e. The lower the infrastructure factor, the higher the cyber war.

The procedure factor is the last element of cybersecurity hygiene. It comprises the responsive measures enabling firms to prevent, reduce or eliminate a cyberthreat from their business activities. Some responsive measures that port managers could implement have been well documented, such as system design and operations improvements (Tonn et al., 2019), disaster response and damage management after an incident is detected (Chang et al., 2014), determination of buying objectives and concomitance between supply chain members (Windelberg, 2016), risk assessment and management (Boiko et al., 2019; Polatidis, Pavlidis, & Mouratidis, 2018; Ralston, Graham, & Hieb, 2007), improvement of transaction design and system by applying ISO regulations, and cyber insurance (Majuca, Yurcik, & Kesan, 2006). Among these measures, risk management seems to be the most preferable tool for port security enhancement as it helps port managers identify all possible risks and to then select suitable measures for addressing them effectively, while other measures that cannot provide these benefits are supportive tools that help port managers implement risk management more efficiently. Apart from these, the process of data sharing with other partners (e.g. port users) was claimed as another vital part of the procedure factor (Cho, Lee, & Moon, 2018). They argued that the vulnerable architecture of port information exchange could also lead to cyberthreats (Cho et al., 2018). This highlighted the importance of the data exchange methods and types of security program adopted to prevent threats in container ports. The previous studies revealed that the procedure factor could help ports to prevent, reduce, or eliminate a cyberthreat from their business activities. In contrast, the failure in implementing measures will lead ports to cyberthreats because the cyber risk was rarely identified and poorly understood due to the deficient procedure factor. This would disable ports to prepare the appropriate measures for mitigating cyber risks of hacktivism (Ahokas et al., 2017), cyber criminality (Christou, 2016), cyber espionage (Platt, 2011), cyber terrorism (Limnéll et al., 2015), and cyber war (Green, 2015; Lewis, 2002) in ports. Based on this argument, it was reasonable to hypothesize that:

H3a. The lower the procedure factor, the higher the hacktivism.

H3b. The lower the procedure factor, the higher the cyber criminality.

H3c. The lower the procedure factor, the higher the cyber espionage.

H3d. The lower the procedure factor, the higher the cyber terrorism.

H3e. The lower the procedure factor, the higher the cyber war.

Table 4
Cyber security hygiene.

Attribute	Sources
Human	
Training of workforce	Ahokas et al. (2017)
Security awareness of workforce	Moerel and Dezeure (2017)
Training of executives	Kanalidis (2018)
Security awareness of executives	IMO (2019a, 2019b)
IT security staff and response team	
Security culture of workers	
Infrastructure	
Physical infrastructure and commodity	
■ Office building	Nykodym and Taylor (2004)
■ Terminal operating center	IMO (2019a, 2019b)
■ Cargo	
Vehicle and equipment	Vorakulpipat (2013)
■ Vessels and long-haul trucks	Boyes et al. (2016)
■ Cargo handling equipment	Ahokas et al. (2017)
■ Automated cargo handling equipment and vehicles	IMO (2019a, 2019b)
■ Navigational support equipment	
■ Empty depot tools	Moerel and Dezeure (2017)
■ e-Desk tools	Kanalidis (2018)
■ Internet of Things devices (e.g. sensors and camera)	Boiko et al. (2019)
■ Other machinery and equipment	IMO (2019a, 2019b)
Port operation and control system	Tonn et al. (2019)
■ Port access control system	
■ Shore-based system for vessel operation and navigation	IMO (2017)
■ Automated cargo container tracking system	IMO (2019a, 2019b)
■ Internet-use control system	Tonn et al. (2019)
■ Handling control system	
■ Traffic control system	
■ Building control system	
■ Warehouse access control system	
■ Internal working network	
■ External business collaboration network	
■ Customs information technology	
Information infrastructure to support port cyber security	
■ Information security	
■ Application security	
■ Cyber threat protection	
■ Internet security	
■ Network security	
Procedure	
■ Risk management	Lee and Whang (2005)
■ Port risk governance	Majuca et al. (2006)
■ Change management	Ralston et al. (2007)
■ Information sharing	Boyes et al. (2016)
■ Threat and vulnerability management	Cherdantseva et al. (2016)
■ Event and incident response	Kanalidis (2018)
■ Cyber and program management	Polatidis et al. (2018)
■ Resilience measure and system redundancy	Boiko et al. (2019)
■ Damage management	IMO (2019a, 2019b)
■ ISO 31000:2009 and ISO/IEC 27005:2011	

Table 4 summarizes all factors influencing port cybersecurity hygiene, while Fig. 3 demonstrates the research model comprising cyberthreats grouped into five latent factors and port cybersecurity hygiene grouped into three latent factors. The causal relationships among the eight latent factors were based on research hypotheses H1a-H3e.

3. Research methodology

3.1. Measurement and questionnaire development

The items for survey measurement were drawn from the based on two groups. The first group comprised 25 items involving five categories of cyberthreat (i.e. four items for hacktivism, eight items for cyber criminality, seven items for cyber espionage, four items for cyber terrorism, and two items for cyber war) (see Table 3). The second group consisted of 43 items involving three factors representing three elements of cybersecurity hygiene (i.e. six items for the human factor, 27 items for the infrastructure factor, and ten items for the procedure factor) (see Table 4). The questionnaire was designed in three parts. The first part collected general information regarding the respondents and firms. The second and the third parts measured the 68 items mentioned above for the first and second groups, respectively. All measures were scored using a five-point Likert scale (1 = strongly disagree, 2 = disagree, 3 = neither agree or disagree, 4 = agree, and 5 = strongly agree). In questionnaire part two, the respondents were asked to identify the possible cyberthreats violating the cybersecurity of a container port, not specifically their branches in Thailand, but in other countries. In questionnaire part three, they were asked to rate the capability level of each measure sufficiently implemented to prevent a cyberthreat.

The first draft of the questionnaire was reviewed by five logistics experts from educational institutes, three port managers, three IT supervisors, three managers of shipping lines, and two customer service supervisors of freight forwarders to ensure the validity of the questionnaire and to make sure that the words or sentences used in the questionnaire were understood by the respondents. Minor revisions were made to replace ambiguous terms with better

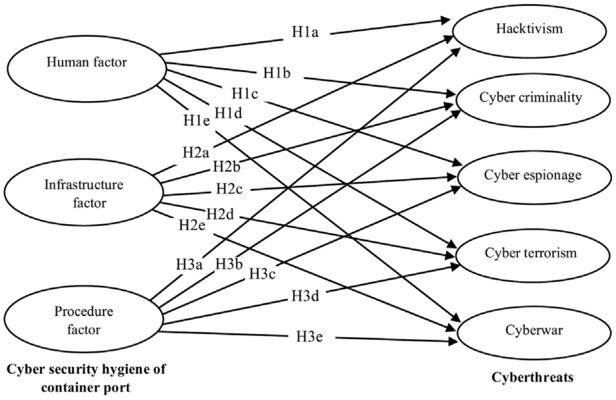

Fig. 3. Research conceptual model.

words and some redundancy of items was suggested resulting in some merging under the same structure. Thus, the items for measuring the factors were reduced: (1) infrastructure factor from 27 to 19 items; (2) hacktivism from four to three items; (3) cyber criminality from eight to seven items; and (4) cyber espionage from seven to five items. The remaining items were unchanged. Then, the pilot study was conducted by asking the same 16 experts to complete the revised questionnaire. The results showed that no revision was required by the experts and so the completed questionnaire was distributed to the respondents.

3.2. Sample and data collection

The current study avoided self-evaluation bias and incomprehensive information by collecting data from both international container port operators and port users (shipping lines and shipping agents) with established branches in Thailand. The titles and contact addresses of the 243 companies were obtained from: (1) the websites of Laem Chabang Port Authority and the Port Authority of Thailand; (2) the directories of Lloyd's List; and (3) from personal contact with the authors and colleagues, comprising 18 terminals in Laem Chabang Port, 5 private seaports in Chonburi Province, 10 terminals in Bangkok Port, and 210 shipping lines and ship agents. The author purposively selected the respondents who worked in the managerial levels of each company and had responsibility for information technology and cybersecurity in the firm. Where the respondents were at the operational level, they were required to at least five years' experience in the relevant fields. To ensure the respondents were suitably qualified to participate, the author and survey team provided the aims of study, the survey objective, and directions on how to answer the questionnaire to respondents or to the coordinators who would select the respondents via a telephone call before delivering a copy of the questionnaire at the office or sending the online questionnaire to the respondents. Respondents could choose the more convenient way for them to submit their questionnaire responses. Most of the firms expressed great concern at providing this critical information; thus, the company name and title of each respondent, including position, were kept confidential to avoid any conflict of interest or damage to a company's reputation. Furthermore, non-response bias was also reduced by providing a long data collection period (one month) to each of the respondents to allow completion of the questionnaire.

The first wave of questionnaires was sent out in April 2019 to all potential respondents. Each respondent was asked to complete the questionnaire within one month; subsequently, those who had not return by then were reminded by the author via a telephone call every month in order to ensure the response rate of the survey. Overall, the survey lasted from April to July 2019 and 147 completed questionnaires were returned to the author, accounting for 60.49% of the total respondents. These were made up of 129 shipping lines and agents (61.42% response rate) and 18 port operators (54.54% response rate). Table 5 describes the profile of respondents. It can be seen that more than half of the respondents are the senior supervisor. Almost 5% of the respondents are the senior manager or higher and about 30% of the respondents are the manager responsible for information technology, cybersecurity, ship operation security, port safety and security, and cargo operation. The majority of the respondents identified that they have working experience in cybersecurity and related areas of expertise. Almost 60% of the respondents have experienced more than 10 years and about 20% of the respondents have experienced at least 5 years, while the rest of the respondents have experienced less than 5 years. The areas of their duty are 9.52% port and cybersecurity, 14.29% IT and computer network, and 76.19% ship security, indicating that the respondents have covered the function in port and ship cybersecurity.

The author used SPSS Statistics version 22 by IBM to test the non-response bias and the difference between two respondent groups. The non-response bias was examined between the scores from the early and late respondents using a *t*-test and the result indicated that there was no statistically significant difference at $p < 0.05$ indicating that the survey data was free from non-response bias. Thereafter, the difference between the mean scores obtained from two groups of respondents were also investigated using *t*-test. These results implied that there were no statistically significant differences among mean at $p < 0.05$ meaning that shipping lines and port operators had similar attitudes toward possible cyberthreats and port cybersecurity hygiene. The mean and standard deviation of all items are presented in Table 6.

4. Results for the measurement model

Eight latent constructs, as shown in Fig. 3, were developed based on the existing literature (i.e. three constructs for cybersecurity hygiene and five constructs for cyberthreats). The author initiated the factor analysis by using SPSS Statistics version 22 by IBM to conduct exploratory factor analysis (EFA) and then AMOS version 21 by IBM to conduct confirmatory factor analysis (CFA) in order to evaluate the measurement model.

Cybersecurity hygiene comprises human, infrastructure, and procedure factors. Six items were used to measure the human factor, 27 items were used to measure the infrastructure factor, and 10 items were used to measure the procedure factor. After factor analysis was conducted, the result revealed that 26 items had loading factors less than 0.6 which should be deleted from the construct to maintain convergent validity (Hair, Black, Babin, & Anderson, 2010). Thus, the author removed one item from the human factor construct, 21 items from the infrastructure factor construct, and four items from the procedure factor construct because they will not adequately represent a specific construct and only items with loading factors greater than 0.6 were maintained and considered for further analysis. After removing these 26 items, the remaining items were factor analyzed and the results are presented in Table 7.

Cyberthreats contains five constructs; namely, hacktivism, cyber criminality, cyber espionage, cyber terrorism, and cyber war. Each construct was measured by different items: four items for measuring hacktivism; eight items for measuring cyber criminality; seven items for measuring cyber espionage; four items for measuring cyber terrorism; and two items for measuring cyber war. The result of factor analysis demonstrated that nine items had loading factors greater than 0.6 while the rest items had loading factors less than 0.6. To maintain convergent validity as suggested by Hair et al. (2010), the author removed one item from hacktivism

Table 5
Profile of survey respondents ($n = 147$).

Profile of respondents		Shipping lines and agents		Terminal operators		Total	
		n	%	*n*	%	*n*	%
Position	Senior supervisor	85	57.82	10	6.80	95	64.63
	Manager	39	26.53	6	4.08	45	30.61
	Senior manager or higher	5	3.40	2	1.36	7	4.76
Years of working experience (years)	1–4	31	21.09	5	3.40	36	24.49
	5–9	23	15.65	4	2.72	27	18.37
	>=10	75	51.02	9	6.12	84	57.14
Security-related duty	Port and cybersecurity	0	0	14	9.52	14	9.52
	IT and computer network	17	11.56	4	2.72	21	14.29
	Ship security	112	76.19	0	0.00	112	76.19
Nationality of firm ownership	Other	103	70.07	15	10.20	118	80.27
	Thai	26	17.69	3	2.04	29	19.73

Table 6
Mean and standard deviation of survey data.

Attribute	Shipping lines ($n = 129$)		Port operators ($n = 18$)	
	Mean	SD	Mean	SD
Human factor				
Training of workforce	3.403	1.0271	3.322	1.0178
Security awareness of workforce	3.581	.8988	3.433	.7859
Training of executive	3.403	1.0271	3.389	1.1448
Security awareness of executive	3.581	.8988	3.611	.9164
IT security staff and response team	3.055	.9799	2.967	.9701
Procedure factor				
Risk management	3.667	1.0704	3.578	1.0741
Port risk governance	3.155	.9799	3.189	1.0226
Information sharing	2.713	1.1263	2.622	.7321
Threat and vulnerability management	2.674	1.1330	2.533	.6860
Cyber and program management	3.264	1.1286	3.111	1.0226
Resilience measure and system redundancy	2.395	.9305	2.278	.8264
Infrastructure factor				
Cargo container tracking and traffic control system	2.798	.8041	2.611	.6077
Internet-use control system	2.674	.7823	2.578	.5745
External collaboration network	3.736	.8972	3.644	.7838
Information security	2.946	.8954	2.833	.7071
Communication and collaboration security	2.860	.8546	2.689	.6077
Internet and network security, including cyber threat protection	2.854	.8034	2.722	.8264
Hacktivism				
Hack by malware and ransomware	4.512	.6139	4.433	.6860
Credential theft	4.341	.7015	4.256	.7254
Privacy violation	4.318	.9099	4.233	1.0981
Cyber criminality				
Criminal and data damage	2.444	1.1338	2.389	.6978
Data breach	3.775	1.1541	3.822	.6468
Cyber espionage				
Insiders gaining unauthorized access to information systems	4.140	.5961	4.200	.5145
Intruder has direct physical access to systems and the network	3.333	.7840	3.467	.6860
Cyber terrorism				
Outages and information system failure	3.047	.8183	3.000	.7670
Subverting security control	2.736	.9145	2.778	.8085

construct, six items from cyber criminality construct, five items from cyber espionage construct, two items from cyber terrorism construct, and two items from cyber war construct. By doing this, only seven constructs of cyberthreats were maintained and the cyber war was excluded from further analysis because there was no significant item under its construct. After removing these 16 items, the remaining items were factor analyzed and the results are shown in Table 7.

The results of CFA illustrated that the measurement model was acceptable due to the fit indices of the model. As demonstrated at the bottom of Table 7, the value of relative chi-square (CMIN/DF = 1.722) which is less than 2 and not significant at $\alpha = 0.05$. The values of incremental fit index (IFI = 0.928), Tucker-Lewis index (TLI = 0.904), and comparative fit index (CFI = 0.926) were greater than 0.9, while the value of root mean square error of approximation (RMSEA = 0.05) was not significant at $\alpha = 0.05$. These indices were within the threshold recommended by Hu and Bentler (2009), indicating an adequate model fit. Furthermore, all items had loading factors greater than 0.6 (ranging between 0.621 and 0.909), indicating the good correlation between the item and its construct (Hair et al., 2010). The reliability and internal consistency of the measured items representing each construct were evaluated by composite reliability instead of Cronbach's alpha because the composite reliability is normally used to measure scale reliability overall in CFA (Bacon, Sauer, & Young, 1995), while the Cronbach's alpha is used in EFA (Nunnally, 1978). Hence, the composite reliability (ranging between 0.660 and 0.877) was greater than 0.6 which was within the recommended range in the literature (Bacon et al., 1995), indicating the internal consistency. The average variance extracted (AVE) was also used to assess the convergence among a set of items representing a latent construct. It was found that the AVE value of three constructs (i.e. human, infrastructure, and procedure factors) was higher than 0.5 indicating the convergence validity, while the AVE value of the other four constructs (i.e.

Table 7
Factor analysis of cybersecurity hygiene and cyberthreats.

Item	Component			
Cybersecurity hygiene	Human factor	Infrastructure factor		Procedure factor
Training of workforce	.751			
Security awareness of workforce	.904			
Training of executive	.734			
Security awareness of executive	.909			
IT security staff and response team	.638			
Cargo container tracking and traffic control system		.709		
Internet-use control system		.676		
External collaboration network		.785		
Information security		.661		
Communication and collaboration security		.666		
Internet and network security		.686		
Risk management				.844
Port risk governance				.621
Information sharing				.800
Threat and vulnerability management				.823
Cyber and program management				.776
Resilience measure and system redundancy				.778
Composite reliability	0.849	0.807		0.877
Average variance extracted	0.533	0.511		0.545
Cyberthreats	Hacktivism	Cyber criminality	Cyber espionage	Cyber terrorism
Hack by malware and ransom ware	.772			
Credential theft	.676			
Privacy violation	.738			
Criminal and data damage		.780		
Data breach		.717		
Insiders gaining unauthorized access to information systems			.666	
Intruder has direct physical access to systems and the network			.648	
Outages and information system failure				.817
Subverting security control				.970
Composite reliability	0.745	0.660	0.667	0.669
Average variance extracted	0.494	0.493	0.496	0.487

Remark: Model fit statistics: CMIN/DF = 1.722, IFI = 0.928, TLI = 0.904, CFI = 0.926, and RMSEA = 0.05.

Table 8
Convergent and discriminant validity analysis.

Construct	Human factor	Infrastructure factor	Procedure factor	Hacktivism	Cyber criminality	Cyber espionage	Cyber terrorism
Human factor	**0.533**						
Infrastructure factor	0.015	**0.511**					
Procedure factor	0.175	0.265	**0.545**				
Hacktivism	0.009	0.050	0.066	**0.494**			
Cyber criminality	0.003	0.337	0.299	0.000	**0.493**		
Cyber espionage	0.014	0.000	0.274	0.223	0.038	**0.496**	
Cyber terrorism	0.082	0.001	0.013	0.046	0.001	0.072	**0.487**

Remark: Values in bold text are AVE and values in regular text are squared correlations.

hacktivism, cyber criminality, cyber espionage, and cyber terrorism) was slightly less than 0.5. However, their composite reliability values were still within the recommended range in the literature (Bacon et al., 1995); hence, their convergent validity was still maintained. Finally, the discriminant validity was tested by comparing the AVE value with the square of the correlation estimate. Table 8 indicates the good evidence of discriminant validity because the AVE values for any of the two constructs are greater than the square of their correlation estimates. Therefore, each measurement item is unidimensional and only represents its loaded construct.

5. Results for the structural model

The author used a covariance based SEM to investigate the causal relationships between the cyberthreats and the port cybersecurity hygiene. Fig. 4a displays the path diagram resulting from the structural modeling analysis using AMOS version 21 by IBM. The result shows that the model was valid because all goodness-of-fit measures satisfy all criteria with RMSEA = 0.039, NFI = 0.932, RFI = 0.896, IFI = 0.978, TLI = 0.965, CFI = 0.977, and HOELTER = 251.

To investigate whether the model in Fig. 4a has the best fit, two alternative models were developed to compare their goodness-of-fit. Fig. 4b exhibits the first alternative model developed by dropping six paths which were not significant in the previous model. This includes the paths between (1) the human factor and hacktivism, (2) the human factor and cyber espionage, (3) the infrastructure factor and cyber espionage, (4) the infrastructure factor and cyber terrorism, (5) the procedure factor and cyber criminality, and (6) the procedure factor and cyber espionage. To do this, the coefficients of six insignificant paths were set to zero in AMOS. The result demonstrated that the model was still valid, and most of the goodness-of-fit measures improved. Overall, the model has a satisfactory fit with RMSEA = 0.038, NFI = 0.931, IFI = 0.978, TLI = 0.966, CFI = 0.977, HOELTER = 254. Only the value of RFI (0.897) was slightly lower than 0.9.

Further to the model in Fig. 4b, the author developed the model in Fig. 4c by adding two new paths based on two criteria. First, these two paths were reasonably supported by the previous literature. Second, the modification indices in AMOS suggested that adding them would improve the goodness of fit of the model.

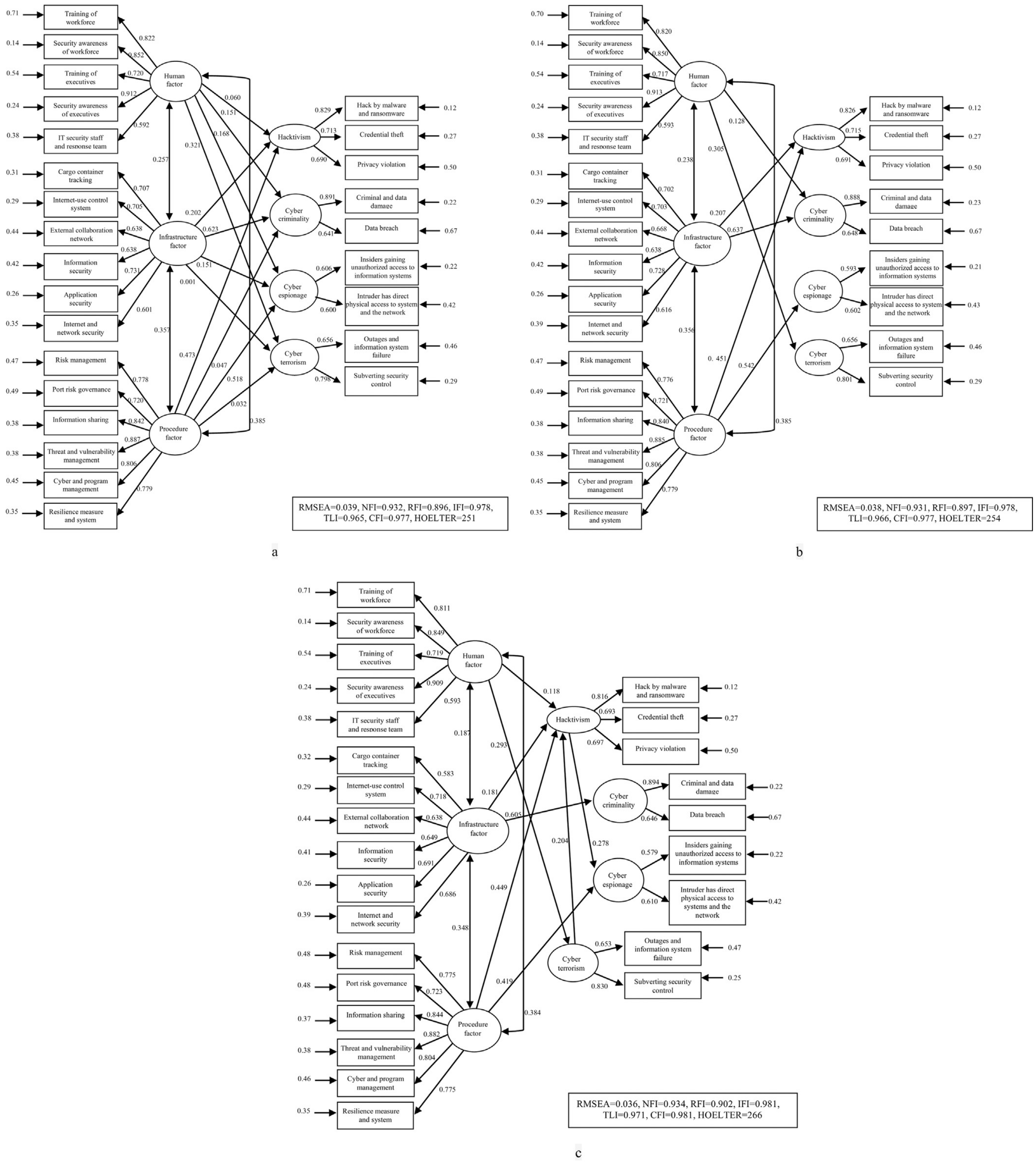
Training of workforce
Security awareness of workforce
Training of executives
Security awareness of executives
IT security staff and response team
Cargo container tracking
Internet-use control system
External collaboration network
Information security
Application security
Internet and network security
Risk management
Port risk governance
Information sharing
Threat and vulnerability management
Cyber and program management
Resilience measure and system
Human factor
Infrastructure factor
Procedure factor
Hacktivism
Cyber criminality
Cyber espionage
Cyber terrorism
Hack by malware and ransomware
Credential theft
Privacy violation
Criminal and data damage
Data breach
Insiders gaining unauthorized access to information systems
Intruder has direct physical access to system and the network
Outages and information system failure
Subverting security control
RMSEA=0.039, NFI=0.932, RFI=0.896, IFI=0.978, TLI=0.965, CFI=0.977, HOELTER=251
a
RMSEA=0.038, NFI=0.931, RFI=0.897, IFI=0.978, TLI=0.966, CFI=0.977, HOELTER=254
b
RMSEA=0.036, NFI=0.934, RFI=0.902, IFI=0.981, TLI=0.971, CFI=0.981, HOELTER=266
c

Fig. 4. Structural model of cyber security hygiene and threat of container port industry.

Logically, the cyber terrorism was the politically-motivated attack using malicious software to violate the digital asset of important organizations (Limnéll et al., 2015). To achieve this, the cyber-terrorist must use the malware (i.e. the hacking technique) to invade into the computer networks through the vulnerable gaps in the cyberspace (Ahokas et al., 2017) and then illegally access to the secret information (i.e. the cyber espionage) (Platt, 2011) before they use computer viruses or worms, etc., to violate the information, computer systems, computer software, and databases. Based on this process, it is reasonable to believe that the spiteful intention to conduct the cyber terrorism will initiate the motivation to conduct the hacktivism and cyber espionage respectively. Therefore, the first path assumed that cyber terrorism had a direct effect on hacktivism, and the second path assumed that hacktivism had a direct effect on cyber espionage. All in all, the model has a fit with RMSEA = 0.036, NFI = 0.934, RFI = 0.902, IFI = 0.981, TLI = 0.971,

Table 9
Comparison of alternative models.

Model	Chi-square	DF	Chi-square difference	DF difference	SCDTs ($\alpha = .05$)
Fig. 4c *Remove the paths*: Human factor → Hacktivism Human factor → Cyber espionage Infrastructure factor → Cyber espionage Infrastructure factor → Cyber terrorism Procedure factor → Cyber criminality Procedure factor → Cyber espionage *Add the paths*: Cyber terrorism → Hacktivism Hacktivism → Cyber espionage	299.410	218			
Fig. 4b *Remove the paths*: Human factor → Hacktivism Human factor → Cyber espionage Infrastructure factor → Cyber espionage Infrastructure factor → Cyber terrorism Procedure factor → Cyber criminality Procedure factor → Cyber espionage	316.054	220	16.644	2	Significant
Fig. 4a: Proposed model	311.613	214	12.203	4	Significant

Table 10
Results for the best model and hypothesis testing.

Hypothesis	Relationships between variables	Path coefficient	Supported or not
H1a	Human factor → Hacktivism	0.118*	Supported
H1b	Human factor → Cyber criminality	–	Not supported
H1c	Human factor → Cyber espionage	–	Not supported
H1d	Human factor → Cyber terrorism	0.293**	Supported
H1e	Human factor → Cyber war	–	Not supported
H2a	Infrastructure factor → Hacktivism	0.181*	Supported
H2b	Infrastructure factor → Cyber criminality	0.605**	Supported
H2c	Infrastructure factor → Cyber espionage	–	Not supported
H2d	Infrastructure factor → Cyber terrorism	–	Not supported
H2e	Infrastructure factor → Cyber war	–	Not supported
H3a	Procedure factor → Hacktivism	0.449**	Supported
H3b	Procedure factor → Cyber criminality	–	Not supported
H3c	Procedure factor → Cyber espionage	0.419**	Supported
H3d	Procedure factor → Cyber terrorism	–	Not supported
H3e	Procedure factor → Cyber war	–	Not supported
Novel relationships			
	Cyber terrorism → Hacktivism	0.204*	
	Hacktivism → Cyber espionage	0.278*	
RMSEA = 0.036, NFI = 0.934, RFI = 0.902, IFI = 0.981, TLI = 0.971, CFI = 0.981, HOELTER = 266			

Remark: *Significant at $\alpha < .05$, ** significant at $\alpha < .01$ (one-tailed test).

CFI = 0.981, and HOELTER = 266. The fit statistics for the models in Fig. 4a and b were not as good as the fit statistics for the model in Fig. 4c.

To further investigate whether the model in Fig. 4c should be considered the best model and accepted compared to the models in Fig. 4a and 4, sequential Chi-square difference tests (SCDTs) were conducted by calculating the difference between Chi-square statistic values for the model (Fig. 4c) and each of the models (Fig. 4a and b), with degrees of freedom equal to the difference in degrees of freedom for the two selected models (Anderson & Gerbing, 1998). A significant result in Table 9 indicates that the model in Fig. 4c which was added two additional paths and removed six insignificant paths incrementally help the explanation compared to the models in Fig. 4a and b at a significant level of .05, indicating that this model will be accepted.

Table 10 demonstrates the result of the model in Fig. 4c and hypothesis testing was summarized based on its result. It can be seen that the path coefficient between the human factor and hacktivism had a significant positive value of 0.118, indicating that the weakness of the human factor is positively related to hacktivism. In other words, the container port is likely to be threatened by hacktivism if the human factor is weak. This finding was in line with the study of Ahokas et al. (2017) and Homeland Security (2018). Hence, Hypothesis H1a was supported. The path coefficient between the human factor and cyber terrorism was also positive and significant at $p < 0.01$. This implies that the weakness of the human factor can lead to cyber terrorism. This result was consistent with the study of Moerel and Dezeure (2017). Thus, Hypothesis H1d was supported. However, the analysis showed that the coefficients of the paths between the human factor and the other two factors (cyber criminality and cyber espionage) were not significant at $p < 0.05$. This implies that the weakness of the human factor will not increase the likelihood of cyber criminality and cyber espionage in a container port. Hence, these results did not support Hypotheses H1b and H1c. For cyber war, the result of factor analysis indicated no significant item classified under the cyber war construct, implying the nonexistence of cyber war in the container port industry. In other words, container ports seem not the be the target of cyber war as this is generally more common in the subversion of military computer networks (Moerel & Dezeure, 2017). Thus, Hypotheses H1e, H2e and H3e were not supported.

The path analysis showed a positive relationship between the weakness of the infrastructure factor and cyber criminality due to the significant positive path coefficient, indicating that a container port is likely to be affected by cyber criminality if the infrastructure factor is vulnerable. This finding supported Hypothesis H2b and agreed with the studies of Nykodym and Taylor (2004) and Vorakulpipat (2013). Positive relationships were also found between the infrastructure factor and hacktivism as indicated by the significant positive coefficient of 0.181. These results imply that container ports tend to encounter hacktivism if the infrastructure has poor defenses. This finding was supported by the works of Kanalidis (2018) and Tonn et al. (2019) who argued that the deficiency of infrastructure made the firm's information system defenseless and hacktivist groups could easily find their way into computer systems. Hence, these results supported both Hypotheses H2a. Nevertheless, the path coefficients between the infrastructure factor and two threats (cyber espionage and cyber terrorism) were not significant at $p < 0.05$, meaning that the vulnerability of infrastructure factor does not lead to cyber espionage and cyber terrorism. Thus, Hypotheses H2c and H2d were not supported.

The model showed that the procedure factor of port cybersecurity hygiene is affected by hacktivism and cyber espionage because the coefficients of paths between the procedure factor and these two factors had significant values of 0.449 and 0.419 respectively. This implies that deficiencies in the procedure factor will increase the possibility of hacktivism and cyber espionage in the container port. These findings were consistent with the arguments of Cherdantseva et al. (2016) and Kanalidis (2018) and supported Hypotheses H3a, and H3c. Nevertheless, the path coefficients between the procedure factor and the other two cyberthreats (cyber criminality and cyber terrorism) were not significant at $p < 0.05$, meaning that vulnerability of the procedure factor of container port does not lead to cyber criminality and cyber terrorism. Thus, Hypotheses H3b and H3d were not supported.

The model in Fig. 4c also revealed some theoretical discoveries from the two additional paths. The path coefficient between cyber terrorism and hacktivism had a significant positive value of 0.204, indicating that a container port encountering cyber terrorism is more likely to encounter hacktivism. The positive path coefficient of 0.278 between hacktivism and cyber espionage implied that a container port that is being threatened by hacktivism is more likely to be harmed by cyber espionage. The weak correlation coefficient among human, infrastructure, and procedure factors (ranging from 0.187 to 0.384) revealed that elements of port cybersecurity hygiene were slightly correlated. In other words, the weakness in the human factor (e.g. insufficiency of workforce training and lack of security awareness of the workforce) slightly weakens the procedure and infrastructure factors. Likewise, the vulnerable port infrastructure (e.g. deficiency of cargo container tracking and traffic control system, internet-use control system, and information security) slightly leads to the vulnerability of human and procedure factors. A poor cybersecurity procedure (e.g. insufficient implementation of risk management, information sharing, and threat and vulnerability management) slightly harms the human and infrastructure factors.

6. Discussions

The findings revealed that three factors (human, infrastructure and procedure) constitute port cybersecurity hygiene but they slightly depend on each other. This means that the failure of one factor will slightly weaken the other factors. This result was consistent with its original philosophy which highlighted the dependency among three factors (Kapalidis, 2018). To initiate good cybersecurity hygiene, port managers and policymakers should prepare the cultivated and skillful manpower (the human factor) who will implement the preventive measures (the procedure factor) to secure port digital assets, technology and facilities (the infrastructure factor) against cyberthreats.

For human factor, provision of training and education to port workers is required, particularly those who have a direct responsibility in managing port information technology and networks, cybersecurity management, and policy development. A shortfall in the knowledge and skills of top executives and employees to enforce cybersecurity measures would possibly cause failure in developing successful port cybersecurity hygiene. In such a case, a container port is highly likely to be exposed to cyberthreats, especially hacktivism and cyber terrorism. Training should not be limited to the operational workers, but rather top executives, including port managers and supervisors, should also be trained to raise their awareness so that effective cybersecurity measures are implemented and emphasized at all organizational levels. By using both top-down and bottom-up approaches, a container port can gradually establish an active environment for continuously scaling up the awareness of all workers in monitoring cyberthreats. Setting up the team responsible for performing cyber risk assessment and other aspects could not only help the container port identify possible cyberthreats and their impacts on port digital infrastructure and security, but assist in the selection of suitable preventive measures to reduce cyber risk or address the impact of malicious actions. Port cybersecurity procedures should be synchronized with other procedures (such as onboard security) as suggested by the International Ship and Port Facility Security Code and the International Safety Management Code (IMO, 2017). These codes suggest that the cybersecurity systems and policies and their implementation at ports and on cargo ships should be officially developed by the firms and linked with the work instructions of the cybersecurity team and officers. All details might also be included in ship security plans, port safety management manuals or cybersecurity manuals so that all team members can understand and implement the procedures as well as monitor and review the results for further improvement (IMO, 2017). This highlighted the importance of port users in setting up port cybersecurity because their information system is directly linked with that of the container port. However, the stakeholder is not limited to port users, other private and government agency, including community, are also the key success factor of port cybersecurity. Thus, all stakeholders are suggested to involve in port cybersecurity development and good collaboration should be continuously ensured.

For infrastructure factor, investment in port infrastructure and facility is also essential for container ports to strengthen their cybersecurity hygiene. Any weakness in the port infrastructure will be critical regarding hacktivism and cyber criminality; thus, using a secured container tracking and traffic control system is the first step that the port managers should take. Monitoring internet use by internal employees is another effective way to reduce the risk of cyberthreats. The port manager should have a record of the computer equipment and software used in the business in order to keep important information secure, prevent unauthorized access, and encourage employees to be mindful of where and how they keep their devices. This highlights the essence of regular training of employees concerning using a USB stick or portable hard drive because unknown cyberthreats can be accidentally transferred from a portable device from home directly into the container port system. The findings also showed that deploying a cybersecurity infrastructure is also important for a container port to secure its computer network from intruders (network security), keep software and devices free of threats (application security) and protect the privacy of data, both in storage and in transit (information security). This sheds light on the vital role of the installation of security software on the computers and devices used in the port operation and administration systems to prevent infection by malware and viruses, while setting up firewall security also helps to defend port communication networks from unauthorized internet users accessing port networks (Tonn et al., 2019).

For procedure factor, preventive measures and other security procedures should be strictly implemented by a container port. Basically, exposure of a container port to cyberthreats, particularly hacktivism and cyber espionage depends on how the information is shared between port operators and other stakeholders, especially port users. Ensuring security in the data exchange process and storage throughout the infrastructure should be considered when the process and system are designed so that any data breaches can be contained. The port manager should control all digital networks and systems by changing default passwords and disabling all administrative access and communication channels in order to avoid external attackers gaining access to a computer or network in the container port. Applying a digital signature to authenticate a person's identity is another approach to reduce the risk of access by unauthorized employees. Cybersecurity measures (control of internet use and the communication network by employees, checklists for cyber hazard identification, provision of training, and regular testing to ensure adequate levels of knowledge and skills of port employees) should be enforced strictly without compromise. This includes risk management and governance which require collaboration by the container port with government authorities, business partners, academic and civil society in performing risk identification, assessment, management and communication of cyber risks. To ensure the effectiveness of cyber risk management, it is obligatory for the senior management level to embed a culture of cyber risk awareness into all organizational levels and to ensure a holistic and flexible risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms (Pallis, 2017). Apart from port cybersecurity hygiene, the findings also confirmed that the container port industry tends to be the target of four cyberthreats as explored by Ahokas et al. (2017). As the most critical infrastructure in every country become increasingly digitalized, it is suggested that government agencies in collaboration with all operators in every industry and other international partners: (1) invest in national and regional cybersecurity; (2) develop a holistic strategy and policy; and (3) update the national regulations in order to sustainably reduce the risk of cyber malicious acts in not only the port industry, but also other critical industries associated with chemicals, commercial activities, communications, manufacturing, dams, energy financial services, and food and agriculture.

7. Conclusions

In conclusion, the SEM highlighted the positive relationship between cyberthreats and port cybersecurity hygiene. Each factor in port cybersecurity hygiene is subject to different cyberthreats depending on its vulnerability; thus, it is necessary for LCP and other container ports to maintain the fitness of human, procedure, and infrastructure factors. Even though each factor is slightly dependent on each other, this study encourages all container ports to ensure the seamless connection among human, procedure, and infrastructure factors in order to maintain good cybersecurity hygiene. Furthermore, a container port is an attractive target for the hacktivist, snooper, criminal, and terrorist. Attempts by the individual container port to address these malicious acts are essential, but not sustainable over the long term because this issue has a large-scale impact on not only the port industry but on the entire national economy. Therefore, the port industry is encouraged to coordinate with relevant government organizations not only to determine the direction of cybersecurity prevention in the industry but also to promote international government coordination. The government should scale up national cybersecurity through collaboration with neighboring countries or international institutes because global collaboration would allow all countries to share and gain experience from each other. This includes accessibility to state-of-the-art technologies and innovative policies that potentially help increase government capability to secure the critical infrastructure of the country, including the port industry (Pounder, 2003). To further help increase the cybersecurity performance of container ports, the current study developed a structural model illustrating the association between port cybersecurity hygiene and cyberthreats; hence, some theoretical findings can be used by port practitioners in the early stage of port risk assessment in the identification of the hazards. Additionally, this model can be used as a reference for developing multi-hazard matrices, hazard models, and risk assessment for future study. Nevertheless, the current study surveyed only port operators, shipping lines, and ship agents who are the key players in maritime transportation in Thailand and the ASEAN region, where most national ports have become integral parts of digitized supply chains, innovation districts, and smart cities projects. The seamless boundary between these ports and other entities increases the variety and risk of cyberthreats. Thus, future research is suggested to extend the scope of the study and to consider the impact of external factors from other organizations on port security performance and competitiveness. Developing new risk assessment methods to quantify the risk of each cyberthreat is also recommended because this would substantially support port managers and policymakers in making better decisions. The author also plans to continue studying the above-recommended topics.

Declaration of interest

I confirm that I have given due consideration to the protection of intellectual property associated with this work and that there are no impediments to publication, including the timing of publication, with respect to intellectual property. In so doing we confirm that we have followed the regulations of our institutions concerning intellectual property.

I understand that the Corresponding Author is the sole contact for the Editorial process (including Editorial Manager and direct communications with the office). The Corresponding Author is responsible for communicating with the other authors about progress, submissions of revisions and final approval of proofs. I confirm that I have provided a current, correct email address which is accessible by the Corresponding Author and which has been configured to accept email from chalermpong.s@ku.th.

Funding source

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. There is no financial and personal interest influencing the validity of research.

Permission note

I confirm that all figures and tables in the manuscript are the original content.

Acknowledgement

The author thanks all the experts who reviewed and evaluated the attributes of cybersecurity and threat and thanks all the respondents to the survey. This research did not receive any specific grant from any funding agencies in the public, commercial, or not-for-profit. There's no financial and personal interest influencing the validity of research.

References

Aharoni, E. (2018). *Cybercriminals are industrious when hacking industries.*. Retrieved from https://blog.cymulate.com/cybercriminals-are-industrious-when-hacking-industries

Ahokas, J., Kiiski, T., Malmsten, J., & Ojala, L. (2017). Cybersecurity in ports: A conceptual approach. *Hamburg International Conference of Logistics*, 23.

Anderson, J., & Gerbing, D. (1998). Structural equation modeling in practice: A review and recommendation two-step approach. *Psychological Bulletin*, *103*(3), 411–423.

Bacon, D. R., Sauer, P. L., & Young, M. (1995). *Composite reliability in structural equations modeling*. California: SAGE.

Barnes, P., & Oloruntoba, R. (2005). Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management. *Journal of International Management*, *11*(4), 519–540.

Bermejo, A. G. (2010). *Maritime cybersecurity using ISPS and ISM codes.*. Retrieved from https://www.he-alert.org/filemanager/root/site_assets/standalone_article_pdfs_1220-/he01335.pdf

BOI. (2019). *Digital Park Thailand.*. Retrieved from https://www.boi.go.th/upload/04_Digital_Park_Thailand&EEC_13589.pdf

Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: Uncertainties, risks and cyber security. *Procedia Computer Science*, *149*, 65–70.

Boyes, H., Isbell, R., & Luck, A. (2016). *Code of practice cyber security for ports*. London: Institution of Engineering and Technology.

Chang, C.-H., Xu, J., & Song, D.-P. (2014). An analysis of safety and security risks in container shipping operations: A case study of Taiwan. *Safety Science*, *63*, 168–178.

Chao, S.-L., & Lin, P.-S. (2009). Critical factors affecting the adoption of container security service: The shippers' perspective. *International Journal of Production Economics*, *122*(1), 67–77.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27.

Cho, H. S., Lee, J. S., & Moon, H. C. (2018). Maritime risk in seaport operation: A cross-country empirical analysis with theoretical foundations. *The Asian Journal of Shipping and Logistics*, *34*(3), 240–247.

Choong-Hee, H., Soon-Tai, P., & Sang-Joon, L. (2019). The Enhanced Security Control model for critical infrastructures with the blocking prioritization process to cyber threats in power system. *International Journal of Critical Infrastructure Protection*, *26*, 103–112.

Christou, G. (2016). *Cybersecurity in the European Union*. London: Palgrave Macmillan.

Civil Engineering Division. (2015, January 15). *Management of hazardous waste in Laem Chabang Port*. (C. Senarak, Interviewer).

Eastern Economic Corridor Office. (2018). *Government Initiative.*. Retrieved from https://eng.eeco.or.th/en/government-initiative

Forde, M. (2020, February). *TQL cyber breach is latest example of the industry's vulnerability to hacking.*. Retrieved from https://www.supplychaindive.com/news/tql-cyber-breach-industry-vulnerability-hacking/573174/

Fosen, J. (2019). *Cyber security awareness in the maritime industry.*. Retrieved from http://www.gard.no/Content/25634225/Cyber%20Security_Presentation%20(ID%201418279).pdf

Google Maps. (2020). *Thailand*. Retrieved from https://www.google.co.th/maps/@14.0682723,124.6694005,7090772m/data=!3m1!1e3?hl=en

Green, J. A. (2015). *Cyber warfare: A multidisciplinary analysis*. Abington: Routledge.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis*. New Jersey: Upper Saddle River.

Homeland Security. (2018). *Examining physical security and cybersecurity at our nation's ports*. Washington: U.S. Government Publishing Office.

Hu, L.-T., & Bentler, P. M. (2009). *Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives*. pp. 1–55.

International Chamber of Shipping. (2018). *The Guidelines on Cyber Security Onboard Ships.*. Retrieved from https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20

International Maritime Organization (IMO). (2014). *Maritime (ISPS Code) Regulations 2014.*. Retrieved from http://extwprlegs1.fao.org/docs/pdf/fij152587.pdf

International Maritime Organization (IMO). (2014). *Guidelines on maritime cyber risk management*. Retrieved from http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

International Maritime Organization (IMO). (2019a). *Air pollution, energy efficiency and greenhouse gas emissions.*. Retrieved from http://www.imo.org/en/OurWork/Environment/PollutionPrevention/AirPollution/Pages/Default.aspx

International Maritime Organization (IMO). (2019b). *AIS transponders.*. Retrieved from http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx

International Maritime Organization (IMO). (2019c). *SOLAS XI-2 and the ISPS code.*. Retrieved from The International Ship and Port Facility (ISPS) Code: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

International Telecommunication Union (ITU). (2018). *Global Cybersecurity Index 2018.*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Janssens-Maenhout, G., Roo, F., & Janssens, W. (2010). Contributing to shipping container security: Can passive sensors bring a solution? *Journal of Environmental Radioactivity*, *101*(2), 95–105.

John, A., Paraskevadakis, D., Bury, A., Yang, Z., Riahi, R., & Wang, J. (2014). An integrated fuzzy risk assessment for seaport operations. *Safety Science*, *68*, 180–194.

Johnstone, R. W. (2015). Transportation security policymaking. *Protecting Transportation*, 143–177.

Kapalidis, C. (2018, November 27). *Port Cyber Security: Maersk, Cosco, Barcelona, San Diego. Who is next?* Retrieved from http://www.boussiasconferences.gr/files/_boussias_conferences_content/presentations/portdevelopment/2018/chronis_kapalidis_portdevelopment_18.pdf

Kennard, D. (2019, July 1). *Cyber security and cyber risk in the shipping industry.*. Retrieved from https://www.penningtonslaw.com/news-publications/latest-news/2019/cyber-security-and-cyber-risks-in-the-shipping-industry

King, J. (2005). The security of merchant shipping. *Marine Policy*, *29*(3), 235–245.

Laem Chabang Port. (2019a). *Laem Chabang Port phase 3 – Project scope.*. Retrieved from http://www.laemchabangportphase3.com/files/MarketSounding2/Documentation2.pdf

Laem Chabang Port. (2019b). *Statistics 2016–2019.*. Retrieved from http://lcp.port.co.th/cs/Satellite?blobcol=urldata&blobheadername1=Content-Disposition&blobheadername2=filename&blobheadervalue1=inline%3B+filename%3D%22st2562.pdf%22&blobheadervalue2=filename%3D%22st2562.pdf%22&blobkey=id&blobnocache=false&blobtable=Mung

Laem Chabang Port. (2019, January 25). *Translation of the invitation to tender. Chonburi, Thailand.*. Retrieved from http://www.laemchabangportnew.com/attachments/article/1959/LCP%20Ph3%20Invitation%20toTender_EN%2020190125.pdf

Lee, H. L., & Whang, S. (2005). Higher supply chain security with lower cost: Lessons from total quality management. *International Journal of Production Economics*, *96*(3), 289–300.

Lewis, J. A. (2002, November 1). *Assessing the risks of cyber terrorism, cyber war and other cyber threats.*. Retrieved from https://www.csis.org/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats

Limnéll, J., Majewski, K., Salminen, M., & Samani, R. (2015). *Cyber security for decision makers*. Aalborg: Docendo.

Loh, H. S., & Thai, V. V. (2014). Managing port-related supply chain disruptions: A conceptual paper. *The Asian Journal of Shipping and Logistics*, *30*(1), 97–116.

Majuca, R. P., Yurcik, W., & Kesan, J. P. (2006, January 6). *The evolution of cyberinsurance*. (Cornell University). Retrieved from https://arxiv.org/abs/cs/0601020

Mansouri, M., Nilchiani, R., & Mostashari, A. (2010). A policy making framework for resilient port infrastructure systems. *Marine Policy*, *34*(6), 1125–1134.

McKevitt, J. (2017, June 29). *Maersk, FedEx cases show how cyberattacks can roil global logistics.*. Retrieved from https://www.supplychaindive.com/news/FedEx-TNT-Express-cybersecurity-attack-ransomware/446078/

McLay, L. A., & Dreiding, R. (2012). Multilevel, threshold-based policies for cargo container security screening systems. *European Journal of Operational Research*, *220*(2), 522–529.

McNicholas, M. A. (2016). Vulnerabilities in the cargo supply chain. *Maritime Security*, 137–168.

Michel, S., Mendes, M., Ruiter, J. C., Koomen, G. C., & Schwaninger, A. (2014). Increasing X-ray image interpretation competency of cargo security screeners. *International Journal of Industrial Ergonomics*, (44), 551–560.

Moerel, L., & Dezeure, F. (2017). *Cyber security in port: Business as usual?* Retrieved from http://www.vndelta.eu/files/3215/1125/0649/Cyber_Security_in_Ports_Whitepaper_VND_vonference_november_2017.pdf

National Crime Agency. (2017). *Cyber crime.*. Retrieved from https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

Nunnally, J. C. (1978). *Psychometric theory*. New York: McGraw-Hill.

Nykodym, N., & Taylor, R. (2004). The world's current legislative efforts against cyber crime. *Computer Law & Security Review*, *20*(5), 390–395.

Office of the Official Information. (1997). *Official Information Act 1997.*. Retrieved from www.oic.go.th/FILEWEB/CABINFOCENTER0/DRAWER002/GENERAL/DATA0000/00000008.PDF+&cd=3&hl=en&ct=clnk&gl=th

Office of the Official Information. (2020). *Training in Official Information Act, B.E. 2540 1997*. Retrieved from http://www.oic.go.th/infocenter6/602/

Otago Daily Times. (2020, February 20). *Courier and freight firm Toll Group targeted in cyber attack*. Retrieved from https://www.odt.co.nz/star-news/star-national/courier-and-freight-firm-toll-group-targeted-cyber-attack

Pallis, P. L. (2017). Port risk management in container terminals. *Transportation Research Procedia*, *25*, 4411–4421.

Papa, P. (2013). US and EU strategies for maritime transport security: A comparative perspective. *Transport Policy*, *28*, 75–85.

Pintong, W. (2010). *GMS trade facilitation enhancement thailands contributions.*. Retrieved from https://www.nesdb.go.th/ewt_dl_link.php?nid=3358

Platt, V. (2011). Still the fire-proof house? An analysis of Canada's cyber security strategy. *International Journal: Canada's Journal of Global Policy Analysis*, *67*(1), 155–167.

Polatidis, N., Pavlidis, M., & Mouratidis, H. (2018). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces*, *56*, 74–82.

Port Authority of Thailand. (2018a). *Information Security*.. Retrieved from http://www.port.co.th/cs/internet/internet/ISO27001.html

Port Authority of Thailand. (2018b). *Safety*.. Retrieved from http://www.port.co.th/cs/internet/internet/Safety.html

Pounder, C. (2003). Governments act to improve security. *Computers & Security*, *22*(3), 207–211.

Ralston, P., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions*, *46*(4), 583–594.

Roach, J. A. (2004). Initiatives to enhance maritime security at sea. *Marine Policy*, *28*(1), 41–66.

Scholliers, J., Permala, A., Toivonen, S., & Salmela, H. (2016). Improving the security of containers in port related supply chains. *Transportation Research Procedia*, *14*, 1374–1383.

Shaikh, S. A. (2017). *Future of the sea: Cyber security*. London: Government Office for Science.

Shepherd, J. (2004). What is the digital era? *Social and Economic Transformation in the Digital Era*, 18.

Silgado, D. M. (2018). *Cyber-attacks: A digital threat reality affecting the maritime industry*. Malmö: World Maritime University.

Thailand Computer Emergency Response Team (TCERT). (2000). *About us*.. Retrieved from https://www.thaicert.or.th/about-en.html

Thailand Computer Emergency Response Team (TCERT). (2000). *Cybersecurity Survey 2016*.. Retrieved from https://www.thaicert.or.th/downloads/files/Cybersecurity_Survey_2016.pdf

Thailand Computer Emergency Response Team (TCERT). (2018). *ThaiCERT annual report 2017–2018 (Thai version)*.. Retrieved from https://www.thaicert.or.th/downloads/downloads.html

Thailand Computer Emergency Response Team. (2019). *Statistics*.. Retrieved from https://www.thaicert.or.th/statistics/statistics-en.html

The Secretariat of the Prime Minister (TSPM). (2019). *Thailand's Cyber Security Act B.E.2562 (2019)*. Retrieved from www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF+&cd=1&hl=en&ct=clnk&gl=th

The United States Geological Survey (TUSGS). (2020, March 1). *Laem Chabang Port*.. Retrieved from https://earthexplorer.usgs.gov/

The World Bank. (2007). *Port reform*.. Retrieved from https://ppiaf.org/sites/ppiaf.org/files/documents/toolkits/Portoolkit/Toolkit/pdf/modules/04_TOOLKIT_Module4.pdf

Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. *Transport Policy*, *79*, 103–114.

TQL. (2020, February 28). *Notice of carrier data breach*.. Retrieved from https://www.tql.com/carrierhotline

Tsai, M.-C. (2006). Constructing a logistics tracking system for preventing smuggling risk of transit containers. *Transportation Research Part A: Policy and Practice*, *40*(6), 526–536.

Vorakulpipat, C. (2013). *Good practices and challenges in Cyber Security Thailand*.. Retrieved from www.connect2sea.eu/news-and-events/news/details/EU-SEA-Workshop-International-Cooperation-on-Cyber-Security-Towards-the-New-Avenues-organised-in-Hanoi-Vietnam.html%3Ffile%3Dfiles/connect2sea/files/Workshops/Good%2520Practices%2520and%2520Challenges%2520in

Weinberger, S. (2007, October 4). *How Israel Spoofed Syria's Air Defense System*. Retrieved from https://www.wired.com/2007/10/how-israel-spoo/

Windelberg, M. (2016). Objectives for managing cyber supply chain risk. *International Journal of Critical Infrastructure Protection*, *12*, 4–11.

Yang, Z., Ng, A. K., & Wang, J. (2014). A new risk quantification approach in port facility security assessment. *Transportation Research Part A: Policy and Practice*, *59*, 72–90.

Yeo, G.-T., Pak, J.-Y., & Yang, Z. (2013). Analysis of dynamic effects on seaports adopting port security policy. *Transportation Research Part A: Policy and Practice*, *49*, 285–301.