Modus Operandi, Factors, Implications and Governance of Ransomware Attacks on Transportation Systems

Ani Munirah Mohamad[1] Felicia Yong Yan Yan[2,] Nurhazman Abdul Aziz[3], Shuhairy Norhisham[4,] Grace Sharon[5]

[1] Universiti Utara Malaysia, Malaysia
[2]Universiti Tunku Abdul Rahman, Kuala Lumpur, Malaysia
[3] Republic Polytechnic, Singapore and
UNITAR International University, Malaysia
[4] Universiti Tenaga Nasional, Malaysia
[5] Universitas Krisnadwipayana, Indonesia
animunirah@uum.edu.my

Abstract. An efficient transportation system provides numerous benefits to people, businesses, and the larger community, including effective transportation of people and goods, enhanced economic growth, less congestion and travel time, improved access to education and healthcare and other benefits. The digital revolution has transformed the transportation sector, making it more efficient, sustainable, and customer centric. As public transit networks grow increasingly digital, so does the possibility of cyberattacks, one of the common attacks being ransomware, which could cause severe repercussions, leading to service disruptions and putting people at risk. Engaging in document review and paper analysis of past literature and government documents, this paper investigates the modus operandi, factors, implications, and governance of ransomware attacks on the transportation system. The study found various factors that motivate ransomware in transportation systems such as financial gain, service disruption, espionage, and political motivations. This further leads to various implications such as disruption of the normal operation of public transportation networks, financial losses, loss of vital data, harm to health and safety of users, degradation of the reputation of public transportation networks, as well as legal and regulatory repercussions. In Malaysia, ransomware is governed by Section 5 of Computer Crimes Act 1997 for unauthorised modification, Penal Code's Sections 378 for theft, 420 for deception, and 506 for criminal intimidation, as well as relevant provisions of the Personal Data Protection Act of 2010. The study is expected to contribute to the body of literature on ransomware and cybersecurity in the context of transportation systems.

R. Abdul Rahman et al. (eds.), *Proceedings of the 12th UUM International Legal Conference 2023 (UUMILC 2023)*, Atlantis Highlights in Social Sciences, Education and Humanities 15,
https://doi.org/10.2991/978-94-6463-352-8_4

Keywords: Computer crimes, Cybersecurity, Cyberattacks, Ransomware, Transportation systems.

1 Introduction

For a nation's economic and social development, a reliable transportation network is indispensable. It facilitates the movement of people and products, thereby promoting commerce, tourism, and business. An efficient transportation system reduces the cost of transporting products and services, which ultimately results in reduced consumer prices. Additionally, it helps reduce traffic congestion and air pollution. A dependable transportation system is essential for attracting investments and generating employment.

Nevertheless, the transportation systems are not immune to potentiality of problems [1]. One of the problems facing transportation systems is the significant risk from ransomware attacks. These attacks can disrupt the typical operation of transportation systems, resulting in enormous economic losses and public inconvenience [2]. Multiple ransomware attacks on transportation systems, including airports, seaports, and rail networks, have been reported in recent years. The assailants can seize control of vital systems, such as traffic control, communication systems, and ticketing systems, and demand a ransom in exchange for restoring the functionality of the system [3].

This paper is divided into several sections. The first sections provide the background of the study, comprising the problem statement, research question, purpose of study and the methodology engaged in the study. The following part conceptualises the transportation system in general and deliberates on the significance of having excellent transportation system. It is important to have a strong basis for the understanding of excellent transportation systems, and how they could be impacted by potential risks. The next section discusses the digitalisation of transportation systems and potentiality of ransomware attacks, particularly in the era of industrial revolution 4.0 (IR 4.0). Next, the paper highlights the modus operandi and selected ransomware attack incidences in Malaysia and few selected jurisdictions, followed by the factors and implications of ransomware attacks on transportation systems. The significant part of the paper on the governance of ransomware attacks on transportation systems is analysed in the following part of this paper. Finally, the paper provides some recommendations and concludes with potential directions for future research on the subject matters of ransomware attacks and transportation systems.

2 Problem Statement

It is undeniable that the transportation is essential to the operation of our society. However, the industry encounters numerous obstacles that impede its operation. One such difficulty is the escalating threat of cyberattacks, specifically ransomware. Due to its reliance on technology, the transportation industry is highly susceptible to cyber threats,

making it an attractive target for cybercriminals. While numerous studies have examined the issue of cybersecurity in the transportation industry, there is a need to focus on ransomware in particular. In the transportation industry, ransomware attacks have become widespread, resulting in significant financial losses and operational disruptions. These assaults can compromise the secrecy, availability, and integrity of vital information, resulting in severe consequences for the industry's stakeholders.

The problem is exacerbated by the fact that transportation organisations have difficult-to-secure complex and interconnected systems. In addition, transportation stakeholders lack awareness of the risks posed by ransomware and the need for cybersecurity measures to mitigate these risks.

Examining the mode of operation of ransomware attacks on transportation systems and their implications for the transportation industry is crucial. The dependence of the transportation industry on technology makes it susceptible to cyberattacks. With the increased use of Internet of Things (IoT) devices and connected systems, ransomware attacks are anticipated to become more prevalent. The transportation industry must invest in cybersecurity precautions to protect vital systems and data [4].

Moreover, ransomware attacks on transportation systems can have severe repercussions, including disruption of essential services, revenue loss, and reputational harm to transportation companies. These assaults can also result in safety risks, such as collisions and accidents [5]. Therefore, transportation companies must adopt a proactive approach to cybersecurity and implement measures to prevent ransomware attacks and mitigate their effects.

Within the broader context, it is undeniable that a country's economic and social development depends on its transportation system [6]. With the growing peril of ransomware attacks, however, transportation companies must invest in cybersecurity measures to protect vital systems and data. By analysing the modus operandi of ransomware attacks and their effects on the transportation industry, transportation companies can develop effective strategies to prevent and mitigate the effects of cyberattacks [7].

3 Research Question

The research question of the study is: What are the modus operandi, factors, implications, and governance of ransomware attacks on transportation systems within the context of Malaysia laws and regulations?

4 Purpose Of Study

Based on the above premises, this paper examines the modus operandi, factors, implications, and governance of ransomware attacks on transportation systems within the context of Malaysia laws and regulations. It is hereby submitted that it is crucial to understand the various aspects of ransomware attacks on transportation systems particularly on the regulatory aspect, so that proper and appropriate measures can be taken

against future potential attacks which could harm the entire nation and the people in the long run.

5 Methodology

The study engaged in document review and paper analysis of past literature and government documents. It is hereby submitted that this study approach is adequate for the purpose of answering the research question and meeting the purpose of the study.

6 Conceptualising Transportation Systems and the Significance of Having Excellent Transportation Systems

There are a number of transportation systems, being road, air, water, pipeline, and cable. The first of the available transportation systems is the road transportation system, which consists of roads, highways, streets, and bridges utilised by automobiles, buses, trucks, and motorcyclists, among others [8]. This sort of transportation is typically utilised for short to medium distances and is frequently employed for everyday commuting, delivery of commodities, and passenger transportation. The railways are a well-liked kind of transportation that consists of trains, rails, and terminals. They are frequently used for intercity and intercountry transportation of people and cargo across great distances. They are frequently more eco-friendly than road transit systems and are generally seen as safer [9].

The air transportation systems are comprised of airports, aircraft, and air traffic control systems. They are frequently utilised for long distance travel and international travel [10]. They are often more expensive than other modes of transportation, but speedier [11]-[12]. In addition to air transportation, there are water transportation systems, which include ships, boats, and ferries [13]. They are frequently used to transport people and commodities across bodies of water such as oceans, seas, and rivers. They are frequently employed in international commerce and are typically regarded as a cost-effective form of transport for big cargo [14].

In addition, there are pipeline transportation systems which are comprised of pipelines used to carry fluids including oil, gas, and water [15]. They are frequently utilised to transfer these materials across great distances and are frequently regarded as the most efficient and cost-effective means of transport [16]. Lastly, there are the cable transportation systems, which include cable cars, funiculars, and gondolas. They are often used for tourism and the transfer of people and goods over mountainous terrain, such as mountains [17].

An efficient transportation system can provide numerous benefits to people, businesses, and the larger community. Unquestionably, a reliable transportation infrastructure could result in effective transportation of people and goods [18]. A good transportation infrastructure facilitates the efficient movement of people and goods, which is essential for the operation of a modern economy. It facilitates speedy and reliable travel

to work, education, and other key destinations. It also promotes the movement of commodities between regions and nations, which is crucial for international commerce. Moreover, it may result in enhanced economic growth [19]. By making it easier for firms to transfer goods and interact with customers, a strong transportation infrastructure can stimulate economic expansion.

Moreover, it can encourage investment and generate employment opportunities, particularly in the development, maintenance, and operation of transportation infrastructure. There may be less congestion and travel time when the transportation system is efficient. A good transportation system can assist reduce congestion on the roads and in public transit systems, saving time for individuals and businesses [20]. This can also aid in reducing pollution and enhancing air quality, thereby making cities and towns more habitable and sustainable.

In a broader perspective, a reliable transportation infrastructure could improve access to education and healthcare [21]. By making it easier for individuals to reach schools, universities, hospitals, and clinics, a robust transportation system can boost access to education and healthcare [22]. This can have a substantial influence on people's quality of life and help eliminate access disparities to these vital services. A reliable transportation infrastructure could also boost mobility and accessibility of people with impairments and those living in isolated or rural locations can be enhanced by a reliable transportation system [23]. This can improve their quality of life and provide them with access to possibilities they might not have otherwise.

Lastly, a reliable transportation system may help improve social connections [24]. By making it easier for people to travel and interact with their friends, family, and neighbours, an efficient transportation system can serve to establish social bonds. This can have a favourable effect on mental health and wellbeing, particularly for isolated or vulnerable individuals [25]. As can be seen, an efficient transportation infrastructure is crucial for the contemporary economy and society to function. It can bring a variety of benefits, including as enhanced economic growth, decreased congestion and travel time, improved access to education and healthcare, increased mobility and accessibility, and strengthened social relationships.

7 Digitalisation Of Transportation Systems and Potentiality Of Ransomware Attacks

In the period of IR4.0, the transportation sector is increasingly coordinated and managed digitally. The digital revolution has transformed the transportation sector, making it more efficient, sustainable, and customer centric. Digitalisation in the context of transportation systems refers to the incorporation of digital technologies into a variety of transportation operations and infrastructure components [26]. One of the most significant effects of digitalisation is the ability to gather, store, and analyse vast quantities of transportation-related data. This data can be utilised to better decision-making, optimise operations, and improve the customer experience. For instance, data from GPS systems and vehicle sensors can be used to track the location and status of vehicles in

real-time, enabling operators to make more informed decisions regarding routes, scheduling, and maintenance [27].

The development of new transportation modes and services, such as ride-sharing platforms and electric scooters, has also been assisted by digitalisation. Often, these services are offered via smartphone applications that let clients to book rides, pay for them, and follow their location in real time [28]. This has made transportation more accessible and easier for a great number of individuals, particularly in urban areas. In addition, digitalisation has enabled the creation of intelligent transportation systems, which employ cutting-edge technology such as artificial intelligence and the internet of things (IoT) to optimise traffic flow, alleviate congestion, and enhance safety [29].
For instance, traffic lights and road signs can be linked to a central network to enable real-time control based on traffic conditions. Additionally, digitalisation has permitted the development of sustainable transportation systems, such as electric and hybrid automobiles, which generate less pollution and greenhouse gases than conventional vehicles. Intelligent charging systems can be used to control the charging of electric vehicles, ensuring that they are charged when renewable energy sources are most readily accessible.

The danger of cyberattacks increases in tandem with the growing digitalisation of public transport networks. The number of cyberattacks launched against public transportation systems has surged in recent years. These attacks have the potential to cause serious disruptions to transportation networks, putting the safety and security of passengers in jeopardy. One of the worrying forms of cyberattacks is called ransomware, which is discussed in the following section [30].

8 Findings

This section presents the findings of the study on the modus operandi, factors, implications, and governance of ransomware attacks on transportation systems within the context of Malaysia laws and regulations.

8.1 Modus Operandi and Selected Ransomware Attack Incidences

In recent years, ransomware attacks have become an increasingly widespread form of cyberattack. In the context of public transportation systems, ransomware attacks can have severe repercussions, causing service disruptions and putting people at risk. Ransomware is a sort of malware that encrypts a victim's files and renders them inaccessible to the user [31]. The attackers demand a ransom in exchange for the decryption key, which may be used to decrypt the encrypted files. Ransomware attacks can be disastrous, as they can interrupt business significantly and lead to the loss of valuable data.

In the context of public transportation networks, ransomware attacks primarily target the supporting IT infrastructure [32]. This comprises the ticketing system, scheduling software, and other vital components necessary for the safe and effective functioning of the transportation system. Often, the first step in a ransomware assault is to acquire access to the target system. This can be accomplished by several methods, including

phishing emails, social engineering, and exploiting software and hardware flaws. After gaining access, the attackers will install ransomware on the system, which will encrypt files and limit access to vital systems and data.

After ransomware has been deployed, attackers often display a message alerting the victim that their files have been encrypted and that a ransom payment is necessary to receive the decryption key. Often, the communication will include instructions on how to make the payment as well as a payment date. The ransom is often sought in a cryptocurrency, such as Bitcoin, as this provides the attackers with a high level of anonymity [33]. The ransom payment price might vary depending on the size and complexity of the target system as well as the victim's estimated ability to pay. If the ransom is not paid within the allotted period, the attackers may threaten to erase the encrypted files or increase the ransom demand. In rare instances, the attackers may carry out their threats, leading in the loss of vital data and the disruption of operations.

After understanding the mode of operation of ransomware attacks, it is helpful to examine some selected ransomware attack incidences against transportation systems.
In June 2017, ransomware compromised the payment system of the Kiev Metro, in Ukraine. As a result of the attack, the ticket machines were disabled and only cash was accepted on the subway [34]. In exchange for the decryption key, the attackers requested 10 bitcoins (about $40,000 at the time). Instead of paying the ransom, the Kiev Metro attempted to restore its payment system.

Many employees' email accounts were hijacked by a phishing attack in January 2016 against the Washington, D.C. Metro. The attackers gained access to the email accounts of multiple employees and stole critical data, including employee and customer information [35]. The attack had no effect on the running of the Metro, but it compromised the personal information of Metro staff and consumers. The January 2016 phishing assault on the Washington, D.C. Metro compromised employees' and consumers' sensitive personal information. The loss of such information could lead to identity theft and financial fraud, which could result in substantial financial losses for those impacted. In addition, it could lead to a loss of public confidence in the transportation provider, which could diminish ridership and income.
Later in August 2018, a ransomware attack compromised the Istanbul Metro's electronic display systems. In exchange for the decryption key, the attackers sought a ransom of 1 bitcoin (about $6,000 at the time). Instead of paying the ransom, the Istanbul Metro attempted to repair its display systems [36]. The August 2018 ransomware attack on the electronic display systems of the Istanbul Metro forced the transit operator to focus on restoring the systems rather than on its core operations. Even if the transportation operator declined to pay the ransom, it would have to expend costs to restore its systems, highlighting the financial effect of such attacks.

In May 2021, German Railways' IT systems were compromised by a cyberattack. The attack had little effect on the railroad's operations, but it did shut down several of its IT systems, notably its email and phone services [37]. The attackers gained access to critical data, including employee and customer information. While the cyberattack on German Railways in May 2021 had no effect on the company's operations, it did result in the suspension of mission-critical IT systems, including as email and phone services, which could lead to a loss of productivity. In addition, the breach of sensitive

data, such as employee and customer information, could have legal and regulatory consequences.

In November 2018, the payment systems of the San Francisco Muni Train System were compromised by a ransomware attack. In exchange for the decryption key, the attackers requested 100 bitcoins (about $700,00 at the time). Instead of paying the ransom, the Muni Rail System attempted to restore its payment mechanisms [38]. The November 2018 ransomware attack on the San Francisco Muni Rail System resulted in huge financial losses for the transportation operator, with the perpetrators demanding 100 bitcoins (about $700,000 at the time) in exchange for the decryption key. The transportation operator incurred additional costs to repair its payment systems because of its unwillingness to pay the ransom, underlining the financial impact of ransomware attacks.

In July of 2020, a cyberattack compromised the Chennai Metro's online ticketing system. The ticketing system was stopped down for several hours due to the hack. After a few hours, the Chennai Metro was able to restore its ticketing system. The hack on the Chennai Metro's online ticketing system in July 2020 led to the temporary suspension of the system, resulting in operational interruption and potential revenue loss. It also exposed the susceptibility of transportation operators' essential systems to cyberattacks, which might have substantial economic and safety consequences [39].

Within the context of Malaysia, in recent years, ransomware attacks against Malaysian public transportation networks have been recorded on multiple occasions [40]. The ticketing system of the Light Rail Transit (LRT) system in Kuala Lumpur was compromised by ransomware in August of 2019. In exchange for the decryption key, the attackers sought a ransom of 1 bitcoin (about $10,000 at the time). Instead of paying the ransom, the LRT system sought to restore its ticketing system and avoided heeding to the demands of the attackers.

The computer systems of the Penang Port in Malaysia were compromised by a cyberattack in December 2019. The attack brought down the port's Computer infrastructure, including its website and email servers. The port declined to pay the ransom sought by the attackers in exchange for the decryption key and instead worked to restore its IT infrastructure [41].

The information screens and flight information systems at Kuala Lumpur International Airport (KLIA) were compromised by ransomware in May 2020. The attack caused aircraft delays and cancellations, and travellers were encouraged to verify the status of their flight before travelling to the airport [42]. The attackers sought a ransom in exchange for the decryption key, but the airport declined to pay, instead focusing on restoring its information displays and flight information systems.

These attacks underscore the significance of deploying comprehensive cybersecurity safeguards in Malaysian and international public transportation systems. Systems of public transportation must maintain the security of their IT infrastructure and have a plan in place to respond to intrusions. To identify and avoid phishing attempts and other cyber dangers, it is essential that personnel receive regular cybersecurity training. By implementing these precautions, public transportation networks can safeguard themselves and their passengers against the threat of cyberattacks.

8.2 Motivating Factors of Ransomware Attacks on Transportation Systems

Increasingly frequent ransomware attacks on transportation systems can have devastating effects for both the firm and its customers. Many high-profile ransomware attacks against transportation networks, including airports, railways, and public transit services, have occurred in recent years. There are a variety of motives for these attacks, but four are frequently listed in the academic literature, being financial gain, interruptions in the service of the transport companies, espionage and political manoeuvre. Each of these factors are discussed below.

Financial Gain. Financial gain is one of the primary motivations behind ransomware attacks on transportation systems. Transportation systems are interesting targets because they frequently manage significant quantities of sensitive data and play a vital part in people's everyday lives [43]. Ransomware is used by attackers to encrypt crucial data and demand money in exchange for the decryption key; it may be a profitable source of cash for hackers. In addition, attackers may demand a ransom that is less than the cost of retrieving the data, which makes paying the ransom an attractive choice for the victim.

Interruptions in Service. The disruption of services is an additional motivation for ransomware attacks on transportation infrastructure. Transportation systems are essential infrastructure and play a crucial part in the society's seamless operation [44] [45]. With ransomware, attackers interrupt the operation of transportation networks, causing passengers to be inconvenienced. Such assaults can cause enormous economic losses to the transportation sector, its passengers, and the larger community because of delays, cancellations, and other disruptions.

Espionage. Espionage is another major motivation for ransomware attacks on transportation infrastructure. Attackers can employ ransomware to steal sensitive information, such as passenger data, financial information, and other secret data that can be sold on the dark web or utilised in other nefarious ways [46]. The data obtained by these assaults can be utilised for identity theft, fraud, and other cybercrimes, as well as to gain a competitive advantage in the transportation business.

Political manoeuvres. Lastly, ransomware attacks on transportation systems can be motivated by politics. State-sponsored actors may execute ransomware attacks on transportation systems to destroy their rivals' infrastructure or further their political ambitions [47]. These attacks may be part of a larger operation to destabilise or destroy the economy of the target nation. In some instances, attackers may employ ransomware attacks to steal sensitive data that can be used for espionage or to threaten the security of key infrastructure.

As is evident, ransomware attacks on transportation systems are driven by several objectives, including financial gain, service disruption, espionage, and political motivations. These attacks can have substantial effects for transportation networks, their

passengers, and the community. Transportation systems must employ robust cybersecurity safeguards, such as regular vulnerability assessments, multi-factor authentication, and endpoint protection, to prevent these assaults. Companies should also build incident response plans to ensure they are prepared to respond swiftly and effectively to a ransomware assault. In addition, transportation systems must interact with government agencies, industry groups, and other stakeholders to share information and develop solutions to avoid ransomware attacks and reduce their effects. By taking these measures, transportation systems may increase the safety and security of their operations, their customers, and the community at large.

8.3 Implications of Ransomware Attacks on Transportation Systems

The impact of ransomware attacks, which have become a significant threat to public transit networks, cannot be underestimated. These attacks have the potential to cause significant operational disruption, financial losses, data loss, safety concerns, reputational injury, legal and regulatory repercussions, and national security concerns. In the following paper, we will examine these consequences in greater detail.

Disruption to Operations. Ransomware attacks have the potential to interfere with the normal operation of public transportation networks, which could result in both delayed and cancelled services [48]. Because of this, passengers are likely to become frustrated, which could have ramifications for the economy. Because of holdups in the delivery of goods and services, customers might not make it to their appointments or flights, and companies might suffer financial losses as a result.

An example of a ransomware attack in the transportation industry that caused significant disruptions is the attack on the San Francisco Municipal Transportation Agency (SFMTA) in November 2016 [49]. The attack impacted the payment systems of the agency's light rail system, which prevented passengers from purchasing tickets and caused delays in the trains' schedules. As a result, the agency had to allow passengers to ride for free, leading to an estimated loss of revenue of around $50,000 per day [50]. The attack also affected the agency's email system and forced employees to resort to using personal email accounts to communicate with each other, causing further disruptions to operations.

Financial Losses. Second, there is the possibility that ransomware attacks could cause public transit networks to incur financial losses. They may be compelled to pay a ransom to regain access to their systems, or they may incur costs related to recovering both their systems and their data [51]. The ransomware attack may also result in financial loss because of service disruptions, reputational harm, and a decline in ridership. To illustrate, in March 2021, the Dutch public transport operator Keolis Nederland fell victim to a ransomware attack, providing a real-world example of ransomware attacks resulting in financial losses in public transit networks [52]. The company was forced to close its IT network, which included ticketing machines, disrupting bus and train service in multiple regions. Keolis Nederland was forced to pay the ransom demanded by

the assailants to regain access to its systems, resulting in a loss of millions of euros. In addition, the business was required to invest in additional security measures and employ external experts to assist in recovering their systems and data. Passengers were left stranded, and the company was unable to provide accurate information about when services would recommence, resulting in significant reputational damage. Consequently, some passengers opted for alternative modes of transport, resulting in a decline in ridership and additional financial losses for the company.

Data Loss. Thirdly, there is always a chance that a ransomware attack could result in the loss of vital data, such as itineraries, routes, and passenger information [53]-[54]. In addition to having potential legal and regulatory ramifications, this might cause severe operational interruptions. The loss of passenger data could potentially jeopardise the passengers' personal information and safety. The 2020 ransomware assault on the Irish public transportation operator Bus Éireann is a real-world example of a ransomware attack resulting in the loss of vital data in the transportation industry [55].

Because of the ransomware attack, the company was compelled to shut down its whole information technology infrastructure, including its servers and email, for several days. In addition to obtaining valuable information, such as payroll data and employee personal information, the attackers threatened the security as well as the privacy of both employees and passengers [56]. Because of the event, personnel were forced to rely on manual operations, which led to delays and cancellations of appointments and other commitments. This caused significant operational interruptions. The organisation was forced to rebuild its information technology systems, restore their data, and improve their security procedures, all of which resulted in additional costs on top of the financial losses that were incurred as a direct result of the attack.

Harm to Health and Safety. Fourthly, there is the potential for ransomware attacks to pose a harm to the health and safety of public transit system users and employees [57]. When important computer systems are compromised, it can lead to service outages, accidents, and other situations where people's safety is at danger. This may potentially result in the loss of life and material damage. The 2019 ransomware attack on Baltimore's public transit system is a real-world example of a ransomware attack endangering the health and safety of public transit system passengers and employees. Consequently, the city's emergency medical services (EMS) and the capacity of the transport system to issue bus and rail tickets were compromised [58]. The city's computer-aided dispatch (CAD) system, which is used to receive and respond to emergency communications, was inaccessible to the emergency medical services (EMS). This delayed response times and posed a threat to the health and welfare of the city's residents. The ransomware attack impeded the city's transportation department's ability to respond to traffic accidents and emergencies and access vital systems such as traffic signals, CCTV cameras, and vehicle monitoring systems. This further demonstrates that a ransomware attack on public transit systems can have potentially devastating effects on people's health and safety, in addition to financial losses and service disruptions.

Degradation of Reputation. Fifthly, a ransomware attack can degrade the reputation of public transportation networks, causing passengers to lose faith in their ability to provide safe and dependable services [59]. This may have a long-term impact on both the number of passengers and the revenue. People may lose faith in both the public transportation system and the government's capacity to accomplish its job effectively if its reputation is compromised. The 2021 assault on the Metropolitan Transportation Authority (MTA) in New York City is a real-world example of a ransomware attack that damaged the reputation of a public transportation network. The ransomware attack severely disrupted the MTA's computer systems, resulting in service interruptions, train delays, and a loss of consumer confidence [60]. Personal information of MTA employees and consumers was also compromised, raising concerns about data privacy and security. Criticisms of the MTA's cybersecurity practises and preparedness for such an attack harmed its reputation. The incident illustrates the significant impact a ransomware attack can have on a public transport network's reputation and its capacity to serve its consumers.

Legal and Regulatory Risks. If ransomware is employed in attacks against public transportation networks, there may be legal and regulatory repercussions. Failure to comply with data protection rules may result in fines and other consequences for public transportation networks [61]. The severity of these repercussions will depend on the nature of the attack and the information that was stolen or otherwise exposed. This can exacerbate the financial losses already sustained by the business. One example of a ransomware attack on public transit networks in Asia occurred in the Philippines in October of 2020 [62]. The Land Transportation Franchising and Regulatory Board (LTFRB) announced that its online payment system had been compromised by ransomware, causing delays and disruptions in the processing of permit and franchise applications. The attack also exposed the names and addresses of approximately 200,000 individuals who had applied for transportation-related permits and franchises, which may have violated the country's data privacy laws. Later, the LTFRB reported that it did not comply with the ransom demand and had taken steps to strengthen its cybersecurity measures to prevent future attacks.

National Security Concerns. Lastly, there is the possibility that ransomware attacks on public transit networks could raise national security concerns. If essential systems are compromised, this can pose a threat to the general population's health and safety, prompting the involvement of relevant government agencies and possibly even law enforcement [63]. The incident that occurred in July 2021 in Kaohsiung, Taiwan, is an example of a ransomware attack on public transport networks in Asia. The ticketing and access control systems of the Kaohsiung Rapid Transit Corporation (KRTC), which operates the city's public transportation system, were shut down due to a ransomware attack [64]. The assault affected over 40 stations, and until the systems were restored, KRTC was forced to use manual ticketing and entry systems for several days. The attack not only caused significant disruptions to the public transit system, but also raised concerns about the security of Taiwan's essential infrastructure, prompting the National Security Bureau and other government agencies to become involved.

As demonstrated, ransomware-based assaults pose a substantial threat to the nation's public transportation system, and the consequences of such attacks can be disastrous. Thus, it is imperative that public transportation networks implement comprehensive cybersecurity measures to protect themselves against ransomware attacks and mitigate the damage they do.

8.4 Governance of Ransomware Attacks in the Context of Malaysia

In Malaysia, ransomware attacks are crimes that are punishable under a variety of laws. Malaysia's major ransomware-related statute is the Computer Crimes Act of 1997 (CCA). The CCA is the primary law that criminalises illegal access to computer systems, data, and networks. It also includes charges associated with ransomware, such as unauthorised modification of computer systems, intentional disruption of computer systems, and unauthorised disclosure of confidential information.

Unauthorized access to computer systems, including the use of ransomware to gain unauthorised access to a computer system or network, is criminalised by Section 3 of the CCA. The clause states that anybody who knowingly enters or induces access to any computer system or network without authorisation is guilty of an offence punishable by a fine of up to RM50,000 or imprisonment for up to five years, or both. In addition, Section 4 of the CCA encompasses the purposeful disruption of computer systems, which includes the use of ransomware to disrupt the operation of a computer system or network. Any individual who wilfully disrupts or causes the disturbance of a computer system or network is subject to a fine of up to RM150,000, imprisonment for up to 10 years, or both.

Section 5 of the CCA criminalises illegal computer system modifications. This clause renders unauthorised modification or alteration of computer data, computer programmes, or computer systems a crime. This offence is punishable by a fine not exceeding RM150,000 or imprisonment for not more than ten years, or both. The clause is intended to deter and punish those who participate in acts that jeopardise the integrity and security of computer systems, which can result in substantial harm to organisations and individuals. Illegal modification of computer systems can take many forms, including hacking, introducing malware or viruses, modifying data, and stealing information. The rule applies to anybody who modifies or alters a computer system, whether the modification or alteration is temporary or permanent. This implies that even momentary alterations to a computer system, such as altering the background image or font, might result in criminal culpability.

The same Section 5 of the CCA includes acts of unauthorised alteration performed using another user ID or password. This is significant because it recognises that illegal alteration of a computer system does not necessarily require physical access. Using another person's login credentials to gain access to a system and make illegal changes is likewise a violation of this rule. Unauthorized modification of computer systems is a serious violation since it can result in substantial harm to individuals and corporations. For instance, an illegal alteration of a computer system may lead to the loss of important data, the theft of secret information, or the interruption of essential activities. This can result in financial losses, reputational harm, and legal liabilities.

This section is very relevant in the context of ransomware attacks, as ransomware is a sort of virus meant to modify computer systems without consent. Typically, ransomware attacks encrypt files on a victim's computer system, rendering them inaccessible to the user. The attackers then demand payment, typically in cryptocurrency, for a decryption key that may be used to restore access to encrypted information. This type of assault is a blatant breach of Section 5 of the CCA, as the attackers make unauthorised changes to the victim's computer system. The statute defines "modification" as any change, deletion, or addition to a computer programme or computer-held data. In a ransomware attack, the attackers modify the victim's data by encrypting it and then demand money to regain access.

In terms of legal sanctions, Section 5 of the CCA stipulates that a person convicted of violating this section is subject to imprisonment for a term not to exceed 10 years or a fine not to exceed RM500,000, or both. This means that ransomware attackers in Malaysia could face severe penalties if they are apprehended and convicted. By virtue of the Section, individuals who commit ransomware attacks in Malaysia could suffer severe legal repercussions if apprehended and convicted under this clause and other provisions of the legislation. Organisations must be aware of the legal framework around ransomware attacks in Malaysia and take the necessary precautions to safeguard their computer systems and data from this type of threat.

In addition to the CCA, the Penal Code also criminalises ransomware attacks under Sections 378 for theft, 420 for deception, and 506 for criminal intimidation. The provisions of the Criminal Code can be utilised to prosecute ransomware culprits. The Malaysian Criminal Code is a comprehensive statute that covers a wide range of illegal behaviours, including ransomware attacks.

First and foremost, Section 378 of the Penal Code criminalises theft, which is the dishonest taking or removal of another person's property without their permission. Theft can occur in the context of ransomware crimes when a criminal employs ransomware to steal data or information from the computer system or network of a victim. A hacker might, for instance, employ ransomware to obtain illegal access to the computer system of a public transportation system and steal sensitive data, such as client information or financial data. The hacker may then demand a ransom in exchange for the return of the stolen data or to prevent its publication or sale on the dark web. If apprehended, the culprit may be prosecuted with theft under Section 378 of the Criminal Code, and if convicted, he or she faces up to seven years in jail and a fine.

Section 420 of the Penal Code criminalises cheating, which is the act of deceiving someone with the goal of gaining an advantage or causing the victim to suffer a loss. Cheating can occur within the context of ransomware crime when a criminal employs ransomware to trick a victim into paying a ransom in exchange for access to their computer system or data. With ransomware, a hacker may encrypt the data of a public transportation system and demand payment in exchange for the decryption key. The hacker may fool the victim by promising to give the decryption key once the ransom has been paid but failing to do so after receiving the cash. If caught, the culprit may be prosecuted with cheating under Section 420 of the Criminal Code, and if convicted, he or she may face up to ten years in prison and a fine.

In addition, Section 506 of the Penal Code criminalises criminal intimidation, which is the act of threatening another person with the goal of compelling them to do or stop from doing something. Criminal intimidation can occur in the context of ransomware crime when a perpetrator uses ransomware to threaten a victim with the publishing or sale of their sensitive data or information. For instance, a hacker may employ ransomware to obtain unauthorised access to the computer system of a public transportation system and threaten to sell or publish critical customer data unless the victim pays a ransom. If apprehended, the perpetrator may be prosecuted with criminal intimidation under Section 506 of the Criminal Code, and if convicted, they may face up to seven years in prison, a fine, or both.

In addition, ransomware attacks are covered by the Personal Data Protection Act of 2010 (PDPA), which guarantees the security of personal data against illegal access, use, and disclosure. The PDPA stipulates that anybody who accesses, uses, or discloses personal information without authorisation is guilty of an offence punishable by a fine of up to RM500,000 or imprisonment for up to three years, or both. In Malaysia, the PDPA regulates the collecting, processing, and storage of personal data by organisations. The PDPA applies to ransomware attacks because they frequently entail the illegal access and theft of personal data, which can subsequently be exploited for malevolent purposes such as identity theft, financial fraud, or phishing scams.

Under the PDPA, companies are required to prevent unauthorised access, use, and disclosure of the personal information they collect and process. In the event of a ransomware attack, firms subject to the PDPA could be held accountable for data breaches if they fail to deploy proper security measures. Before collecting and processing an individual's personal information, organisations are required by the PDPA to get the individual's consent. This means that businesses must inform individuals of the purpose for which their personal data is being collected, the types of personal data that will be gathered, and the way the data will be used and secured.

In the context of ransomware attacks, enterprises that collect and process personal data must verify that suitable security measures have been taken to prevent unauthorised access or disclosure. To prevent illegal access to systems and data, this may involve regular data backups, encryption of critical data, and the adoption of multi-factor authentication. In the event of a ransomware attack, enterprises subject to the PDPA may be obligated to report the breach to the necessary authorities and impacted persons, as well as take measures to minimise the breach's damage and avoid future attacks.

Ultimately, the PDPA is very relevant to ransomware attacks because it requires enterprises to secure personal data from illegal access, use, and disclosure. By establishing comprehensive security measures and adhering to the PDPA's criteria, enterprises can assist in preventing ransomware attacks and mitigating their effects if they do occur.

Thus, ransomware attacks are governed by multiple laws in Malaysia, such as CCA, the Penal Code, and the PDPA. These rules impose heavy penalties on those who conduct ransomware attacks. Transportation systems and other companies must ensure compliance with these regulations and take the necessary precautions to prevent ransomware attacks. In addition, they should build incident response strategies to effectively respond to such attacks and reduce their effects on operations and consumers.

Yet, the pieces of legislation analysed above may not be adequate to expressly handle ransomware attacks. Ransomware attacks are an emerging threat that necessitates specific knowledge and technologies for detection, prevention, and response. To counter ransomware attacks effectively, further precautions may be required. This could involve amending the law to specifically handle ransomware attacks and other cyber risks. This may require identifying criminal charges associated with ransomware attacks and implementing punishments for anyone found guilty of perpetrating such offences.

In addition, law enforcement organisations may require training and resources to effectively investigate and prosecute ransomware attacks. This could involve forming cybercrime divisions inside law enforcement agencies and equipping them with the necessary tools and resources to battle ransomware attacks successfully. In addition to legal and law enforcement procedures, enterprises must deploy effective cybersecurity safeguards to prevent ransomware attacks and respond to them. This includes creating access controls to prevent unwanted access to important systems, routinely backing up critical data, and educating personnel on best practises for cybersecurity. In addition, it is crucial for firms to establish a plan for responding to ransomware attacks. This should include protocols for identifying and containing the assault, engaging with law enforcement and other stakeholders, and restoring vital data and systems.

9 Discussion and Recommendations

Ransomware attacks can have devastating effects, including monetary losses, data breaches, operational disruptions, and reputational harm. Strengthening ransomware governance is critical for preventing and mitigating the effects of these attacks. Outlined below are some methods for enhancing the management of ransomware attacks.

Awareness and education are vital for enhancing the ransomware governance system. It is crucial to educate employees on the hazards of ransomware attacks and the best cybersecurity policies [65]. Employees can be educated on the newest cyber risks and solutions to prevent ransomware attacks through frequent training and awareness initiatives provided by their employers. For example, businesses can run regular phishing simulations to assess their employees' awareness of ransomware attacks.

To combat ransomware attacks, businesses should implement more strict cybersecurity safeguards. This includes creating access controls to prevent unauthorised access to important systems, performing routine backups of vital data, and implementing multi-factor authentication for remote access [66]-[67]. In addition, businesses should conduct frequent vulnerability assessments to identify any security flaws and close them prior to an attack.

Additionally, businesses should develop ransomware response procedures to lessen the effects of an attack. This includes establishing rules for identifying and containing the assault, coordinating with law enforcement and other stakeholders, and restoring vital data and systems [68]. Frequent tabletop drills can assist assure the effectiveness of these reaction methods in the event of an actual attack.

Regular risk assessments can help businesses identify cybersecurity infrastructure weaknesses and vulnerabilities. Businesses can evaluate the risk of ransomware attacks and develop mitigating strategies [69]. This can aid in identifying potential security flaws and vulnerabilities in the system, allowing businesses to apply preventative measures.

Further, enhancing the governance of ransomware attacks necessitates collaboration with both private and public partners. Businesses should collaborate on response strategies, share information about threats and attacks, and follow best practises for avoiding and mitigating ransomware attacks [70]. Cooperation with government partners can aid businesses in comprehending the legal and regulatory implications of ransomware attacks, as well as in notifying law enforcement agencies of incidents and assisting with investigations.

Investing in technology can help organisations detect and avoid ransomware threats [71]. Endpoint protection, intrusion detection and prevention systems, and security information and event management (SIEM) systems can be implemented by businesses. These technologies can aid in detecting and preventing attacks before they do severe damage.

Improving governance of ransomware attacks is vital for preventing and mitigating the effects of these attacks, which is a truism. This includes improving awareness and education, instituting tighter cybersecurity rules, devising response plans, doing regular risk assessments, partnering with industry and government partners, investing in technology, and involving law enforcement. By proactively addressing the potential of ransomware attacks, organisations may secure the safety and security of their data and operations, as well as mitigate the reputational and financial consequences of these attacks.

10 Conclusion

Attacks using ransomware on transport systems are becoming an increasing source of concern due to the potential damage and disruption they can cause. The individuals responsible for these attacks may have a variety of goals in mind, ranging from the pursuit of monetary gain to political goals. To create successful measures to avoid and reduce the effects of ransomware attacks on transportation systems, it is vital to have a solid understanding of the variables listed above.

Education and raising people's consciousness are two ways that can help address this problem. Employees in transportation systems should receive training to spot possible ransomware threats, and they should also be supplied with the knowledge and skills necessary to avoid assaults of this nature. Enhancing the cyber resiliency of transport systems and reducing the likelihood of ransomware attacks can be accomplished through the implementation of ongoing training programmes and awareness campaigns.

The necessity for stricter cybersecurity measures is another essential part of tackling the repercussions of ransomware attacks on transportation systems. These attacks hold data hostage and demand money in exchange for releasing it. This includes developing

access controls to prevent unauthorised access to important systems, maintaining frequent backups of vital data, and implementing multi-factor authentication for remote access. In addition, this includes implementing multi-factor authentication for remote access. Conducting vulnerability assessments on a regular basis can also help identify any security flaws or vulnerabilities in the system, which enables businesses to take preventative measures.

In addition to these precautions, it is essential for transport systems to build reaction strategies, as this is the most effective way to reduce the disruption caused by ransomware attacks. This includes cooperating with law enforcement and other stakeholders, recovering critical data and systems, and setting guidelines for identifying and containing the assault. The effectiveness of these response plans can be tested through regular tabletop exercises, which can assist ensure their readiness in the case of a real assault. In Malaysia, ransomware attacks are covered by multiple laws, including the Computer Crimes Act 1997 for unauthorised modification, the Penal Code's Sections 378 for theft, 420 for fraud, and 506 for criminal intimidation, as well as related parts of the Personal Data Protection Act of 2010. These laws were passed in Malaysia. These rules establish a foundation for prosecuting those who attack computers using ransomware and holding them accountable for their crimes.

To address the overall effects of ransomware attacks on transport systems, a multi-pronged approach is required. This approach should include education and awareness campaigns, strong cybersecurity protections, and efficient response strategies. If transportation systems take preventative measures against the possibility of ransomware attacks, they will be able to ensure the safety and security of their operations, minimise their financial losses, and protect their customers from harm.

It is possible that in the future, the focus of research will shift to examining the effects that frequent employee training and awareness programmes have on ransomware attacks. It is uncertain how beneficial such training initiatives are in preventing or mitigating ransomware attacks in the transportation industry, even though staff education and awareness are regarded crucial for improving the governance of ransomware attacks. In the transportation industry, more research may investigate the influence that frequent employee training and awareness programmes have on the frequency of ransomware attacks and the severity of those attacks.

Evaluating the efficacy of different cybersecurity protections in warding off ransomware attacks is another avenue that should be explored during future study. A further essential way for increasing the governance of ransomware attacks is the adoption of more effective cybersecurity protections. On the other hand, it is not apparent how effective these safety measures are in preventing ransomware attacks from taking place. When it comes to the prevention of ransomware attacks in the transportation business, additional research might investigate the efficacy of various cybersecurity safeguards, such as access controls, backups, and multi-factor authentication.

Finally, an investigation into the legal and regulatory repercussions that ransomware attacks may have in the transportation sector may also be investigated. When it comes to ransomware attacks, the legal and regulatory problems that businesses in the transportation industry may encounter are likely to be one of a kind. This is especially true

about data protection and aviation security requirements. Additional research could investigate the legal and regulatory implications of ransomware attacks in the transportation industry and identify best practises for complying with applicable laws and regulations while responding to ransomware incidents. Additionally, this line of inquiry could investigate the implications of ransomware attacks in the financial sector.

11 Authors' Contributions

Authors 1 and 2 contributed to the data collection for the study. All authors contributed to the technical and academic writeup of the paper.

References

1. Sabaliauskaite G, Cui J, Liew LS, Zhou F. Integrated safety and cybersecurity risk analysis of cooperative intelligent transport systems. In *2018 Joint 10th International Conference on Soft Computing and Intelligent Systems (SCIS) and 19th International Symposium on Advanced Intelligent Systems (ISIS)* 2018 Dec 5 (pp. 723-728). IEEE. Author, F.: Article title. Journal 2(5), 99–110 (2016).
2. Pizzi G. Cybersecurity And Its Integration With Safety For Transport Systems: Not A Formal Fulfillment But An Actual Commitment. Transportation Research Procedia. 2020 Jan 1;45:250-7.
3. Galego NM, Pascoal RM. Cybersecurity in smart cities: Technology and data security in intelligent transport systems. In Perspectives and Trends in Education and Technology: Selected Papers from ICITED 2021 2022 (pp. 17-33). Springer Singapore.
4. Chiappetta A, Cuozzo G. Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport. In 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS) 2017 Jun 26 (pp. 206-211). IEEE.
5. Adadurov SE, Diasamidze SV, Kornienko AA, Sidak AA. International Cybersecurity on Railway Transport: Methodological Approaches and Normal Procedural Framework. Russian Railway Science Journal. 2015 Dec 28(6):9-15.
6. Ivanova Y. Modelling the impact of cyber attacks on the traffic control centre of an urban automobile transport system by means of enhanced cybersecurity. In MATEC Web of Conferences 2017 (Vol. 133, p. 07001). EDP Sciences.
7. Schmittner C, Chlup S, Bonitz A, Latzenhofer M, Hofer M, Kloibhofer C, Raab T, Spahovic E, Doms T. Preliminary Considerations for a Cooperative Intelligent Transport System Cybersecurity Reference Architecture. In 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE) 2019 Nov 4 (pp. 1-6). IEEE.
8. Arnold P, Peeters D, Thomas I. Modelling a rail/road intermodal transportation system. Transportation Research Part E: Logistics and Transportation Review. 2004 May 1;40(3):255-70.
9. Sendek-Matysiak E. The role and importance of electric cars in shaping a sustainable road transportation system. In Research Methods and Solutions to Current Transport Problems: Proceedings of the International Scientific Conference Transport of the 21st Century, 9–12th of June 2019, Ryn, Poland 15 2020 (pp. 381-390). Springer International Publishing.

10. McCallie D, Butts J, Mills R. Security analysis of the ADS-B implementation in the next generation air transportation system. International Journal of Critical Infrastructure Protection. 2011 Aug 1;4(2):78-87.
11. Sun X, Wandelt S, Linke F. Temporal evolution analysis of the European air transportation system: air navigation route network and airport network. Transportmetrica B: Transport Dynamics. 2015 May 4;3(2):153-68.
12. Chu Z, Zhou Y. The Effect of Adopting the Next Generation Air Transportation System on Air Travel Performance. Available at SSRN 4108332. 2022 May 12.
13. Baten CA. Internal water transportation system: safety of inland Passenger vessels. NDC E-Journal. 2005 Jun 30;4(1):131-57.
14. Karademir C, Alves Beirigo B, Negenborn RR, Atasoy B. Two-echelon Multi-trip Vehicle Routing Problem with Synchronization for An Integrated Water-and Land-based Transportation System. In hEART 2022: 10th Symposium of the European Association for Research in Transportation 2022.
15. Xu Q, Zhou H, Zhu Y, Cao Y, Huang B, Li W, Guo L. Study of Identification Of Global Flow Regime In A Long Pipeline Transportation System. Powder Technology. 2020 Feb 15;362:507-16.
16. Priyanka EB, Thangavel S, Madhuvishal V, Tharun S, Raagul KV, Shiv Krishnan CS. Application of integrated IoT framework to water pipeline transportation system in smart cities. In Intelligence in Big Data Technologies—Beyond the Hype: Proceedings of ICBDCC 2019 2021 (pp. 571-579). Springer Singapore.
17. Saguin-Sprynski N, Jouanet L, Billeres M. Monitoring System for Cable Transportation. International Journal of Condition Monitoring. 2019 Jul 1;9(2):46-9.
18. Deveci M, Mishra AR, Gokasar I, Rani P, Pamucar D, Ozcan E. A decision support system for assessing and prioritizing sustainable urban transportation in metaverse. IEEE Transactions on Fuzzy Systems. 2022 Jul 13.
19. Pamucar D, Deveci M, Gokasar I, Martínez L, Köppen M. Prioritizing Transport Planning Strategies For Freight Companies Towards Zero Carbon Emission Using Ordinal Priority Approach. Computers & Industrial Engineering. 2022 Jul 1;169:108259.
20. Kouridis C, Vlachokostas C. Towards decarbonizing road transport: Environmental and social benefit of vehicle fleet electrification in urban areas of Greece. Renewable and Sustainable Energy Reviews. 2022 Jan 1;153:111775.
21. Kamruzzaman MM, Alrashdi I, Alqazzaz A. New opportunities, challenges, and applications of edge-AI for connected healthcare in internet of medical things for smart cities. Journal of Healthcare Engineering. 2022 Feb 23;2022.
22. Herath, H.M.K.K.M.B. and Mittal, M., 2022. Adoption of artificial intelligence in smart cities: A comprehensive review. International Journal of Information Management Data Insights, 2(1), p.100076.
23. Park, K., Esfahani, H.N., Novack, V.L., Sheen, J., Hadayeghi, H., Song, Z. and Christensen, K., 2023. Impacts of disability on daily travel behaviour: a systematic review. Transport Reviews, 43(2), pp.178-203.
24. Ipsen C, Repke M. Reaching people with disabilities to learn about their experiences of social connection and loneliness. Disability and Health Journal. 2022 Jan 1;15(1):101220.
25. Bailey M, Farrell P, Kuchler T, Stroebel J. Social Connectedness In Urban Areas. Journal of Urban Economics. 2020 Jul 1;118:103264.
26. Tomić Rotim S. Implementing Cybersecurity Measures in Transport Organisation. Annals of Disaster Risk Sciences: ADRS. 2020 Nov 17;3(1):0-.
27. Pawlik M. Rail Transport Systems Safety, Security and Cybersecurity Functional Integrity Levels. In Research Methods and Solutions to Current Transport Problems: Proceedings of

the International Scientific Conference Transport of the 21st Century, 9–12th of June 2019, Ryn, Poland 15 2020 (pp. 317-329). Springer International Publishing.
28. Lv Z, Li Y, Feng H, Lv H. Deep learning for security in digital twins of cooperative intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems. 2021 Oct 6;23(9):16666-75.
29. Gao Y, Qian S, Li Z, Wang P, Wang F, He Q. Digital twin and its application in transportation infrastructure. In 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI) 2021 Jul 15 (pp. 298-301). IEEE.
30. Rotim ST. Implementing Cybersecurity Measures in Transport Organisation. Annals of Disaster Risk Sciences. 2020 Nov 17;3(1).
31. Markusik S, Bułkowski A. Cybersecurity in Electric Bus Public Transport Systems. In Electric Mobility in Public Transport—Driving Towards Cleaner Air 2021 Apr 23 (pp. 169-188). Cham: Springer International Publishing.
32. Vogel B, Cross B, Charlaff J. Cyber Challenge Demands Attention: To Manage The Risk To Critical Systems, And Mitigate The Impact Of A Cyber Attack, The Air Transport Community Must Come Together As Never Before. IHS Jane's Airport Review. 2016 Feb.
33. Norhisham S, Samsudin NS, Ismail N, Mardi NH, Abu Bakar MF, Azlan NN, Ron Buking RA. Evaluating mass rapid transit (MRT) service quality according to customers' age group of varying travel pattern. In Sustainable Development Approaches: Selected Papers of AUA and ICSGS 2021 2022 Jun 17 (pp. 49-57). Cham: Springer International Publishing.
34. Petrenko AS, Petrenko SA, Makoveichuk KA, Chetyrbok PV. Protection model of PCS of subway from attacks type «wanna cry»,«petya» and «bad rabbit» IoT. In 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) 2018 Jan 29 (pp. 945-949). IEEE.
35. Tin D, Barten DG, De Cauwer H, Ciottone GR. Transport Terrorism: A Counter-Terrorism Medicine Analysis. Prehospital And Disaster Medicine. 2022 Apr;37(2):217-22.
36. Bešinović N. Resilience In Railway Transport Systems: A Literature Review And Research Agenda. Transport Reviews. 2020 Jul 3;40(4):457-78.
37. Dorbritz R, Weidmann U. Stability of public transportation systems in case of random failures and intended attacks-a case study from Switzerland. In 4th IET International Conference on Systems Safety 2009. Incorporating the SaRS Annual Conference 2009 Oct 26 (pp. 1-6). IET.
38. Lin W. The Third Rail of San Francisco Politics: Transportation, Race, and the Central Subway. Hastings LJ. 2018;70:919.
39. Demertzi V, Demertzis S, Demertzis K. An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. Applied Sciences. 2023 Jan 6;13(2):790.
40. Chapman RJ. The Rules Of Project Risk Management: Implementation Guidelines For Major Projects. Routledge; 2019 Sep 10.
41. Singh MM, Frank R, Zainon WM. Cyber-Criminology Defense In Pervasive Environment: A Study Of Cybercrimes In Malaysia. Bulletin of Electrical Engineering and Informatics. 2021 Jun 1;10(3):1658-68.
42. Hassan NH, Fauzee ZM, Ismail N, Maidin SS. Artificial intelligence of things (AIoT) ransomware detection conceptual framework. Proceedings of Mechanical Engineering Research Day. 2022 Aug;2022:205-6.
43. Almeida F, Imran M, Raik J, Pagliarini S. Ransomware Attack as Hardware Trojan: A Feasibility and Demonstration Study. IEEE Access. 2022 Apr 20;10:44827-39.

44. Ruggiero AF, Owusu TD, Staley JJ. Ransomware In Local Government: Risk Factors, Vulnerabilities, And Exploitation During A Global Pandemic. Issues in Information Systems. 2022 Oct 1;23(4).
45. Dullah H, Khai WJ, Ismail N, Norhisham S, Ramli MZ, Mohamad AM, Bakar MF. Advances of Mass Rapid Transit's Facilities in ASEAN Cities: A Review. In Advances in Civil Engineering Materials: Selected Articles from the 6th International Conference on Architecture and Civil Engineering (ICACE 2022), August 2022, Kuala Lumpur, Malaysia 2023 Jan 1 (pp. 481-490). Singapore: Springer Nature Singapore.
46. Al-rimy BA, Maarof MA, Shaid SZ. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security. 2018 May 1;74:144-66.
47. Gazzan M, Alqahtani A, Sheldon FT. Key Factors Influencing the Rise of Current Ransomware Attacks on Industrial Control Systems. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) 2021 Jan 27 (pp. 1417-1422). IEEE.
48. Roberts FS, Egan D, Nelson C, Whytlaw R. Combined Cyber and Physical Attacks On The Maritime Transportation System. NMIOTC Maritime Interdiction Operations Journal. 2019 Jan;18.
49. Liska, A., 2019. Early findings: Review of state and local government ransomware attacks. Recorded Future, 10.
50. Mitchell, R., 2017. Recent Cyber Security Events and Future Research Directions (No. SAND2017-0030C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
51. Weaver GA, Feddersen B, Marla L, Wei D, Rose A, Van Moer M. Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach. Transportation Research Part C: Emerging Technologies. 2022 Apr 1;137:103423.
52. NL Times, 2021, July. Dutch companies also targeted in large ransomware attack. https://nltimes.nl/ accessed 1 April 2023.
53. Brierley C, Arief B, Barnes D, Hernandez-Castro J. Industrialising blackmail: Privacy invasion based IOT ransomware. In Secure IT Systems: 26th Nordic Conference, NordSec 2021, Virtual Event, November 29–30, 2021, Proceedings 26 2021 (pp. 72-92). Springer International Publishing.
54. Brewczyńska M, Dunn S, Elijahu A. Data privacy laws response to ransomware attacks: A multi-jurisdictional analysis. Regulating New Technologies in Uncertain Times. 2019:281-305.
55. Vasudevan, M., Townsend, H., Dang, T.N., O'Hara, A., Burnier, C. and Ozbay, K., 2020. Identifying Real-World Transportation Applications Using Artificial Intelligence (AI): Summary of Potential Application of AI in Transportation.
56. Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., Kantarci, B. and Soyata, T., 2019. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, 50, p.101660.
57. Zhao JY, Kessler EG, Yu J, Jalal K, Cooper CA, Brewer JJ, Schwaitzberg SD, Guo WA. Impact Of Trauma Hospital Ransomware Attack On Surgical Residency Training. Journal of Surgical Research. 2018 Dec 1;232:389-97.
58. Preis, B. and Susskind, L., 2022. Municipal Cybersecurity: More Work Needs To Be Done. Urban Affairs Review, 58(2), pp.614-629.
59. Corbet S, Goodell JW. The reputational contagion effects of ransomware attacks. Finance Research Letters. 2022 Jun 1;47:102715.
60. Akilal, A. and Kechadi, M.T., 2022, June. A Forensic-Ready Intelligent Transportation System. In Science and Technologies for Smart Cities: 7th EAI International Conference,

SmartCity360°, Virtual Event, December 2-4, 2021, Proceedings (pp. 617-630). Cham: Springer International Publishing.
61. Watney M. Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: a Legal Perspective. In European Conference on Cyber Warfare and Security 2022 Jun 8 (Vol. 21, No. 1, pp. 319-327).
62. Kroll, 2020. 2020 Ransomware Attack Trends in Asia Pacific – Beyond the Ransom. https://www.kroll.com/ accessed 1 April 2023.
63. Reshmi TR. Information Security Breaches Due To Ransomware Attacks-A Systematic Literature Review. International Journal of Information Management Data Insights. 2021 Nov 1;1(2):100013.
64. Kuo, H.M., Chen, T.L. and Yang, C.S., 2022. The effects of institutional pressures on shipping digital transformation in Taiwan. Maritime Business Review, 7(2), pp.175-191.
65. Luo X, Liao Q. Awareness education as the key to ransomware prevention. Information Systems Security. 2007 Sep 4;16(4):195-202.
66. Richardson R, North MM. Ransomware: Evolution, Mitigation and Prevention. International Management Review. 2017;13(1):10.
67. Norhisham S, Sidek LM, Beddu S, Usman F, Basri H, Katman H. Awareness and Level of Usage for Park and Ride Facilities in Putrajaya, Malaysia. In Proceedings of the 5th Engineering Conference, Engineering Towards Change—Empowering Green Solutions, Kuching Sarawak, Malaysia 2012 Jul (pp. 10-12).
68. Lee K, Yim K, Seo JT. Ransomware prevention technique using key backup. Concurrency and Computation: Practice and Experience. 2018 Feb 10;30(3):e4337.
69. Thomas J, Galligher G. Improving Backup System Evaluations In Information Security Risk Assessments To Combat Ransomware. Computer and Information Science. 2018;11(1).
70. Barker WC, Scarfone K, Fisher W, Souppaya M. Risk Management. *National Institute of Standards and Technology*. 2021 Sep 8.
71. Alazab M, Venkatraman S, Watters P, Alazab M. Information security governance: the art of detecting hidden malware. In *IT Security Governance Innovations: Theory And Research* 2013 (pp. 293-315). IGI Global.