Assessing and Proposing Countermeasures for Cyber-Security Attacks

Ali Al-Zahrani
College of Computer Sciences and Information Technology
King Faisal University Al-Ahsa 31982
Saudi Arabia

***Abstract*—Cyber-attacks on IT domain infrastructure directly affect the security of businesses' operational processes, potentially leading to system failure. Some industries have a high risk than others due to the sensitivity of their data, including the transportation industry, which has recently moved from traditional data management to digitalization. This study aims to identify the main cyber threats in the transportation sector by analyzing related works and highlighting the main countermeasures used to respond to such threats as well as enhance overall cybersecurity. This paper presents a comprehensive cybersecurity risk assessment for the transportation companies, identifying the most common attacks and proposing methods to minimize risk as much as possible. A risk assessment analysis was prepared by industry experts that included previous cyberattack scenarios. The results of our paper identified the most critical attacks on the transportation company's booking system and recommended suitable countermeasures to minimize the risk of those attacks.**

Keywords*—Cyber-attacks; cyber-security; risk assessment; countermeasures

I. Introduction

A. Background

Cyber-security attacks are considered one of the hot topics in the field of information security and can result in huge losses to organizations if not carefully handled. Cybersecurity attacks usually result from several factors related to threats, human errors or insufficient knowledge [1]. Cybersecurity relates to technologies, processes, practices, and information assets, aiming to protect against any damage or unauthorized access caused by cyberattacks [2]. Cyberattacks on information systems, in particular, directly affect the operational processes that support businesses, potentially leading to corporate paralysis. Some industries are at more risk than others due to their highly sensitive data, one of which is the transportation industry, which has recently moved from traditional data management to digitalization. This transition has raised concerns about cybersecurity and necessitated proper risk assessments due to their importance in protecting critical infrastructure; for instance, cyberattacks on aircraft, which are considered essential transportation, can impact safety-of-flight systems and/or the systems supporting the airlines' business [3]. Cyber threats often take advantage of the increased complexity of infrastructure systems, placing critical industries' security at risk [4]. A physical cyber threat not only harms the integrity of the IPs but may also disrupt production processes and cause serious damage to various systems [5]. To understand cyberattacks, it is important to dig deeply and identify their main causes. Spreading awareness and proper knowledge about cyberattacks and providing sufficient training can reduce the damage they cause. This is often difficult to accomplish because cybersecurity behaviors do not necessarily come naturally, and people need support and encouragement to develop and adopt them [1]. As technology becomes increasingly present in daily life, cybercrime, and cybersecurity tools and techniques require innovative solutions at all organizational levels [4].

Transportation systems, in particular, offer major services that can be put at risk by an absence of real awareness, and neglecting the proper assessment of vulnerabilities can lead to major damage [6]. Cyberattacks on transportation technologies are usually unexpected and require considerable effort to classify the threats, identify impacted assets, develop proper countermeasures, and engage IT teams throughout the process. However, transportation systems vary in their ability to handle threats and in the ways in which organizations prioritize their assets when a risk is identified. This paper discusses how risks to booking systems in the transportation industry are assessed at times of risk and presents a comprehensive cybersecurity risk assessment of information systems in a transportation company to identify the most common threats and recommend methods for minimizing risks as much as possible. A risk assessment report was prepared by industry experts that included previous cyberattack scenarios. This paper aims to answer the following questions:

What are the common types of cyberattacks on transportation systems?

What are the main techniques used to identify vulnerabilities in transportation systems?

What are the main risks and countermeasures used to mitigate these risks?

B. Motivation

Understanding the nature of cyberattacks and their main causes can enhance the overall cybersecurity of an organization. A cyber threat may disrupt production processes and cause serious damage to various systems [5]. Identifying the root cause of such problems can help organizations solve them at a deep level and avoid future attacks rather than relying on temporary prevention solutions. Information systems generally contain critical data that businesses place a high priority on protecting. Some industries, such as the

transportation industry, hold more sensitive data than others; hence, their risks from cyberattacks are huge and can directly impact operational processes. It is therefore vital for them to identify the main causes of cyberattacks and the main practices they should adopt to protect sensitive data from exposure. Cybersecurity for transportation systems has been affected by the dynamic nature of the technology used within the industry. Cybersecurity guidelines have been developed for transportation systems, especially in the past few years, to ensure cybersecurity and raise awareness of its importance [6].

C. Cybersecurity

The main reasons for cybersecurity failures are human error and insufficient knowledge [1]. According to [2], cybersecurity is central to all technologies, standards, and procedures developed to protect infrastructure elements against serious cyberattacks. Some cyberattacks cause major harm to system users, sometimes unintentionally [7]. In other words, cybersecurity protects property rights in an infrastructure context if an attack occurs. Furthermore, cybersecurity is concerned with related issues such as access, extraction, manipulation, or modification of property [8], protecting property against the harm that can be caused by an attack [7] To maintain a secure environment, effective cybersecurity behaviors must be identified and promoted to raise awareness among users from different backgrounds. Both human and technological aspects of information systems need to be clearly identified to maintain a strong cybersecurity environment [1].

1) Cybersecurity in information systems: Today's technology allows for easy, rapid communication across different systems, particularly in domains such as teleworking and m-commerce, which have grown rapidly [9]. Moreover, information and communication technology (ICT) applications have increased dramatically and cyberattacks have spread easily across such applications [10]. The more sensitive the data is, the greater attention needs to be paid. Sensitive data can be vital for businesses because they use it to make critical decisions; major problems can result from cyberattacks that place data at risk of exposure. Protecting infrastructure is a major priority for preventing unauthorized access that can lead to data misuse or corruption. Both individuals and organizations can suffer hugely from data exposure [11].

Recently, cyberattacks have increased due to advances in the technologies used in most information systems. Consequently, most organizations need to invest in cybersecurity and employee training to raise awareness of the importance of securing systems and their sensitive information [12]. One approach to protecting information systems was suggested by [13], which suggested that integrating information systems across organizational environments can improve cybersecurity. The researchers suggested and tested three hypotheses to investigate whether integration is positively related to cybersecurity countermeasures (see Table I).

Although [14] suggested considering all ICS features, the researchers proposed a targeted multilevel Bayesian network for identifying attacks, the functional level of attacks, and incident models. This dynamic cybersecurity risk assessment approach can help assess the risks caused by unknown attacks (see Fig. 1).

Study [10] evaluated power supply reliability using Stackelberg Security Game (SSG) strategies to assign defense resources to various cyber-threat targets. This paper discussed how to benefit from the intrusion tolerance capability of SCADA systems that provide buffer periods before the failure of substations. The overall goal was to improve network strength in the face of cyber threat events. Different cyber threat scenarios were tested to assess intrusion tolerance capabilities, and the authors designed an insurance premium principle to provide incentives for enhancing intrusion tolerance capability.

Study [5] conducted a literature review to identify the impact of cyberattacks on total productive maintenance in smart manufacturing systems. Cyberattacks can directly affect manufacturing equipment and, hence, the services provided, including maintenance services. This paper highlighted major physical cyberattacks and proposed countermeasures to reduce the negative impact of such attacks. The authors identified different challenges in enhancing equipment effectiveness in light of current cybersecurity threats in the manufacturing industry.

TABLE I. HYPOTHESES AND EVIDENCE SUMMARY [12]

Hypotheses	Findings	Evidence
H1. The greater the integration of IS, the greater the investment in countermeasures.	Supported	IS integration causes fewer weak points, reducing the possible impact of breaks.
H2. H1 will be more powerful when considering external IS integration rather than internal IS integration.	Supported	Weak points in external IS integration involve greater risk exposure because of greater uncertainty.
H3. Organizations tend to use self-protective controls more often in highly volatile environments than in less volatile environments.	Supported	Although the impact may not be strong, volatile environments can impact the three aspects of vulnerability. This means that the addressing of weak points must highlight these aspects.

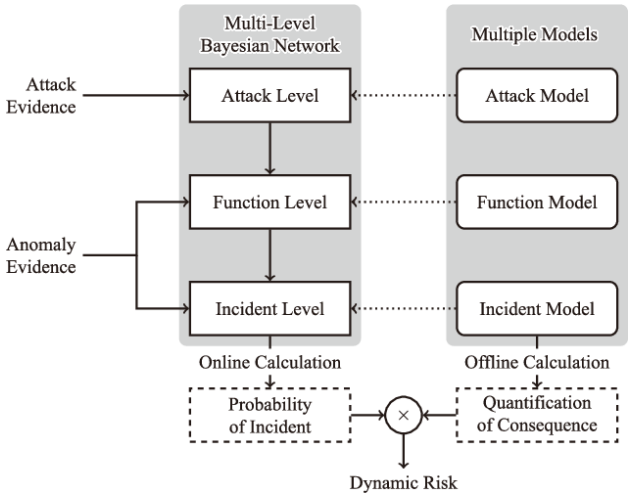

Fig. 1. Architecture of the Dynamic ICS Cybersecurity Approach.

According to study [15], attack graphs are essential for identifying the variables involved in an attack and reducing their impact on networks. This research introduced a cyberattack path method that used restrictions and an in-depth search to successfully produce attack graphs according to the interests of users. The researchers used real data from a maritime supply chain to ensure the validity of the proposed method.

In [16], the author identified the effects of cyberattacks on general systems. As cyberattacks continue to develop, it is becoming more difficult to identify the nature of the attacks; therefore, there is a great need for smart risk assessment. This research proposed the use of a fuzzy inference (FIS) model to produce risk assessment outputs, which relied on four risk factors—vulnerability, threat, likelihood, and impact—to identify risks targeting a system entity and suggest possible solutions for them. A summary of related work is provided in Table II.

2) Cybersecurity threats in the transportation industry: The transportation industry needs to distinguish between operations systems and business systems to provide the right protection for each [6] Over the years, the industry has shifted from traditional business to e-business, and this shift has expanded technologies and their features [2]. According to [11], 80 % of assets in transportation infrastructure are being digitalized. In recent years, many attacks have been made on transportation, which has increased the need for cybersecurity protection guidelines [6], and some factors are critical for ensuring the effectiveness of overall cybersecurity, such as PCS systems, knowledge about cyber threats, and communication between private corporations and public agencies [17]. In the air transportation domain, cybersecurity tends to focus greatly on protecting the operational and technical aspects of businesses; hence, fast adaption to a rapidly changing risk environment is vital, and the framework of technical and operational systems should be redesigned based on continuous risk analysis and simulations [18]. The rapidly changing nature of the transportation industry makes it important to focus on cybersecurity to protect valuable assets and protect the business from harmful threats.

Study [18] was conducted to address the increase in cyberattacks, the impact of which could critically affect civil aviation functions. The huge increase in technologies and integrated connectivity tools can expose air traffic management (ATM) to major risk, despite its high value as an asset. This study evaluated cybersecurity difficulties in ATM to develop a threat model that included likely risks. It also included an overall framework that required full collaboration between entities to identify threats and protect systems from attacks.

Study [19] asserted that the port industry is experiencing a transformation in connectivity between ports, where most functions are being digitalized. This necessitates focusing on cybersecurity to protect major infrastructure against advanced attacks and maximize the use of new technologies with minimum risk of affecting valuable business assets.

Study [11] highlighted the importance of data-driven functions that many business aspects depend on, such as operations, maintenance, planning, and decision-making. To ensure the smooth operation of all functions relating to railways, data should be strongly secured against cyberattacks and unauthorized access to avoid major losses. This paper identified possible challenges, impacts, threats, vulnerabilities, and methods for managing risks and protecting railway infrastructure data, particularly in an e-maintenance context.

Study [6] used a case study to raise awareness of the cybersecurity attacks that affect the transportation field. It developed an attack–fault tree for the mentioned case study as proof of concept for integrated risk analysis. The overall purpose was to help companies understand that no attacks targeting critical technological systems should be ignored, and potential risks should be analyzed.

The author in [3] proposed a new system for gathering, managing, and reporting aircraft failures. The motivation behind this paper was the great expansion in connectivity and communication infrastructure that is affecting aircraft. The increase in mobile computing device use among individuals has allowed for external connectivity increments as well as providing internet access for passengers, involving a greater risk of aircraft cyberattacks that can affect other critical systems supporting the business. The proposed system can help identify such attacks, hence reducing their impact. A summary of related work in the transportation domain is provided in Table III.

TABLE II. SUMMARY OF RELATED WORK

Study	**A Cybersecurity Insurance Model for Power System Reliability Considering Optimal Defense Resource Allocation** [10]	**Multimodal-Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems** [14]	**Cybersecurity Concerns for Total Productive Maintenance in Smart Manufacturing Systems [**5]	**Improving Risk Assessment Models of Cyber Security Using a Fuzzy Logic Inference System [**16]	**Cyberattack Path Discovery in a Dynamic Supply Chain Maritime Risk Management System** [15]
Domain	Cyber physical systems (CPSs)	Industrial control systems (ICSs).	Manufacturing systems	General system	Dynamic supply chain maritime risk management system
System	Modern power grids	Simplified chemical reactor control system	Total productive maintenance (TPM)	Various system entities	Maritime supply chain

Purpose	To benefit from the intrusion tolerance capability of SCADA systems that provide buffer periods before the failure of substations. The overall goal was to improve network strength and counter cyber threats.	To develop a dynamic risk assessment approach that could identify risks due to unknown threats and enhance the accuracy of risk assessment processes.	To illustrate the impact of cyberattacks on total productive maintenance in smart manufacturing systems and to discuss countermeasures to reduce the negative impact of an attack.	To use a fuzzy inference (FIS) model to produce risk assessment outputs, which relied on four risk factors—vulnerability, threat, likelihood, and impact—to identify risks targeting a system entity and suggest possible solutions for such threats.	To introduce a cyberattack path method that used restrictions and an in depth search to successfully produce attack graphs according to the interests of users using real data from a maritime supply chain to ensure the validity of the proposed method.
Possible Threats	• a denial-of-service (DoS) attack • bypassing the VPN to gain access to the servers • changes in voltage and standard measurements	• malicious attacks • spoof attacks • breaches of an intrusion detection system (IDS)	• intellectual properties threats, including theft and data modification • cyberphysical threats that disrupt production processes • a Stuxnet worm infection • malicious void attacks	• website attacks • malware • hacking • denial of service (DoS) • name hijackings • dissemination of viruses. • phishing and spam e-mails	Attack paths within a network: • DoS attacks • distributed denial of service (DDoS) attacks
Risk assessment enhancement (previous approaches)	▪ Component burnout and exhaustion of processing power. ▪ Simulating and forecasting real-time load to ensure system frequency during an attack.	▪ IDS to observe network and system activities. ▪ An anomaly detection system (ADS) to gather data from a system and compare them with normal values (reports produced in cases of deviation)..	▪ Use of overall equipment effectiveness (OEE), which is considered a major KPI for measuring the effectiveness of TPM in a system. The OEE of a system is calculated using the input of three components: - breakdowns (availability) - small stops (performance) - defects (quality) ▪ Each component can be impacted by a cyberattack. ▪ OEE = availability * performance * quality	▪ To deal with the uncertainty factor when gathering data, the fuzzy set theory can help in making decisions about various alternatives. Despite its ability to deal with fuzziness, only a few studies have used fuzzy set theory to handle risk uncertainty, although it is highly recommended for improving the use of this theory for critical risk assessment. ▪ Existing models without human intervention.	▪ MulVal network security analyzer to target bugs within network configurations. ▪ TVA tool for topological network-based analysis. ▪ A graph model based on a specific language to simulate attack scenarios using various methods. ▪ An intrusion detection system to generate graphs for attacks. ▪ NuSMV model for allocating vulnerabilities and producing attack graphs.
Proposed Contribution/ Recommendation	A Stackelberg Security game model to allocate defense resources, unknown to the attacker. Encouraging investment in defense resource coverage to improve the intrusion tolerance capability of SCADA systems and protect them against failure.	The proposed solution is capable of measuring cybersecurity risks of ICSs in a A short-term multimodal-based cybersecurity risk assessment approach with the ability to produce cybersecurity risk values by calculating the probabilities of risks and quantifying the impacts of different possible incidents caused by cyberattacks.	Acquiring an agile maintenance system and considering both mean time between failures (MTBF) and mean time to repair (MTTR), relying on a short repair time. A proposed plan for system recovery, enabling repairs to be performed as quickly as possible.	The proposed solution senses a weak item and moves it to a risk assessment model, which then determines the items for the spatial computation methods and passes them to the next model for approval. Approval suggests the end of the process. However, if an item is not approved, it will be moved to other models for vulnerability estimation using fuzzy theory. Information will be displayed to interested parties, enabling them to decide mitigating actions. The process starts again, relying on human judgment to decrease uncertainty.	•. The proposed method identifies specific paths in a certain network to enhance risk assessment. These paths are unique, such as: o attacker capability o attacker location o propagation length o maximum length o entry points o target points

TABLE III. SUMMARY OF RELATED WORK IN THE TRANSPORTATION DOMAIN

Study	Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management [18]	Cybersecurity in Ports and the Maritime Industry: Reasons for Raising Awareness on This Issue [19]	Cybersecurity for eMaintenance in Railway Infrastructure: Risks and Consequences [11]	Cybersecurity and its Integration with Safety for Transport Systems: Not a Formal Fulfillment but an Actual Commitment [6]	A System for Real-time Monitoring of Cybersecurity Events on Aircraft [3]
Domain	Air transportation	Port industry	Railway industry	Railway industry	Air transportation
System	ATM	Port 4.0	E-maintenance in railway infrastructure	Subsystem for railway vehicles (wheel slide protection [WSP])	Aircraft
Purpose	To analyze potential targets and risks.	To maximize the benefits of using full technology while ensuring that major infrastructure elements are well protected against cyberattacks.	To identify possible difficulties, impacts, and risks of data security for railway infrastructure, and to highlight methodologies for attaining and securing data against possible breaches.	To enhance awareness of possible weaknesses that impact transport systems. Also, to install spotting lights on the embedded devices used by those systems and prevent major attacks that can target them if not well protected.	To track and monitor incidents/failures and protect aircraft and related systems from cyberattacks.
Possible Threats	• passive observers • activists and lobbyists • insiders • cyber crime • cyber terrorism • hostile nation-states	• organized criminal rings • drug traffickers • terrorists • hackers • industrial spies and competitors • disgruntled staff and insiders, enemy states, and foreign intelligence	• data theft • database breaches • targeting of application servers • stealing of authentication details from system administrators • data integrity being affected by modification actions • DDoS • directed denial of service attacks • physical annihilation attacks	• physical attacks: installing malicious devices • side-channel attacks to obtain encryption keys • logical attacks: malicious code injections	• delayed aircraft flight operations • compromised safety of flight systems • high recovery costs affecting business • theft of passengers' personal data. • malware deployed on multiple targets.
Current Security Measures	• physical security • (e.g., access control) • personnel security • (e.g., security clearances) • information security • (e.g., software updates and patches) • communication security • (e.g., network segregation) • intelligence support • (e.g., security alert level declarations) • security information exchanges • (e.g., incident identification and notification) • operational continuity • (e.g., emergency responses)	• Increase awareness among port ecosystem parties by: • publishing standards to address cybersecurity issues • issuing shipping company guidelines and recommendations • requesting the inclusion of cybersecurity in facility security assessments to address any vulnerabilities • publishing a Guide on Port Cybersecurity	• General examples: • inventory of devices/software • malware defenses • application software security • wireless device control • data recovery capability • security skill assessments and training • protection of network ports and services • boundary defense • security audit logs • account monitoring and control • data loss prevention • incident response capability • penetration	• Current strategy of risk assessment is based on single threats and compliance to specific practices, leading to neglect of the effects of combined hazardous events.	• Current systems include logging and monitoring of failures as maintenance data. This approach does not allow prompt tracking of security attacks on aircraft networks, which can allow successful attacks with no detectable trace.
Proposed Contribution/ Recommendation	This study proposed an interactive and model-based cyber risk analysis	Policymakers should work closely with industry to ensure full	• Enhancing confidentiality: ensuring data privacy (i.e.,	An integrated safety and cybersecurity analysis of all	All apps should send security event failure logs for security

	that could produce non-stop cyber flexibility in the air transportation domain.	protection of multiple port systems because they have a major impact on the global economy. Also, they should continuously review current policies and regulations and adopt new industrial technologies. Moreover, they should invest in alert systems to detect cyber incidents.	targeted data accessed/viewed only by authorized individuals). • Enhancing integrity: 1. Supporting data authenticity by using digital signatures or other trusted identifiers. 2. Avoiding data errors when transferring/storing data and making sure that data are original. • Enhancing availability: ensuring that data access is granted to authorized parties.	related control systems could reduce the impact of major threats, as suggested by this study.	monitoring and assessment and: 1. comprise similar applications 2. capture security event failure logs from applications and services on aircraft 3. manage the logs for essential security event failures 4. alert crew for fast recovery and communication with ground system in case of major failures 6. maintain the logs for future maintenance usage.

II. Case Study: Risk Assessment

A. Scenario

Daily DDoS attacks against company systems are a great concern for IT managers; however, the previous severe DDoS attack, which was repeated twice, resulted in approximately four hours of total downtime, was extremely intense, and aimed to fully disrupt the company's booking services, which could have had a significant financial impact. IT leaders directed the cybersecurity team to immediately conduct a risk assessment of these cyberattacks and provide feedback for decision-making. A risk analysis report was prepared using various cybersecurity risk management methodologies to overcome the above-mentioned issues, and the general scenario related to "the risk associated with cyberattacks against the availability of the booking system." [22-26].

B. Risk Assessment

The company follows a combined approach to risk assessment, which is managed by the Cybersecurity Department and the IT Governance, Risk, & Audit (GRA) Department. Their goal is to ensure the management of information technology and security risks [27-32].

1) Asset identification: To identify the assets related to the system, system functions were first had identified [32-38]. The scope of the risk assessment was the company's booking system, represented by an application that provides reservation and ticketing services to various transport sectors through the company's digital channels (see Table IV). List of the most common risks and their corresponding controls targeting booking systems is shown in Table V.

2) Threat and vulnerability identification: Table VI contains the most common threat types targeting web-based systems and their threat communities. Due to the high level of data sensitivity, vulnerabilities were derived from study [20], which highlighted the most common vulnerabilities of Web-based systems but did not necessarily reflect the actual company's data [39-40].

Vulnerabilities can be divided into two classes. The first class includes vulnerabilities that affect a host or only a service running on it:

- host crash.
- performance fault.
- host infection.

The second class includes vulnerabilities that affect only a single service:

- inaccessible service.
- corrupted service.

3) Techniques to identify vulnerabilities: Companies use various techniques to identify vulnerabilities in their systems, and this paper identifies the set of techniques used by transportation companies; for instance, the network security team scans the system a number of times daily, and firewalls and scanners are in place to detect spikes in incoming traffic. Additionally, a DDoS protection service is in place to protect the system. The IT Security team conducts regular exercises to identify vulnerabilities using various technologies, including system vulnerability scans, penetration testing, Web application assessments, and network mapping. Furthermore, the IT team conducts special system scans for indicators of compromise upon requests from the NCA. The company also has monitoring, incident response, and forensics teams working closely with security business partners to cover various areas, such as system logs and audit reports.

C. Minimizing Risks

The chosen risk was based on the two previous high-DDoS incidents that affected the transportation company's system. Management direction played a critical role in selecting what type of risk to manage (see Table VII).

1) Threat community profile: Each threat was known to have its own community profile and could have different initiating factors or triggers. Below are common factors relating to cybersecurity attacks (particularly regarding DDoS; see Table VIII).

TABLE IV. ASSET IDENTIFICATION AND CORRESPONDING VALUES

System functions	System elements	Related department	Number of employees	Assets	Value
1. booking of tickets for trips, cars, trains, hotels, etc. **2.** lounge access **3.** requests for trip upgrades **4.** loyalty programs **5.** online payments **6.** online check-ins **7.** service refunds **8.** real-time trip information and schedules	A. **Input**: 1. trip schedule 2. locations 3. customer information B. **Processing**: 1. booking of trips 2. payment 3. checking in C. **Output**: 1. scheduled trips 2. booking reservations 3. ticket passes 4. marketing campaigns D. **Interface**: 1. website 2. mobile application	1. **Business**: marketing and ticketing services 2. **IT**: digital products and services 3. **Others:** vendor and IT business partners	20 employees	• servers • firewalls • databases • micro services • application gateway • VPN gateway • API gateway	**Information:** customers' data, such as national IDs and credit-cards, are considered the mostvaluable asset in this system. **Internal HW/SW: s**upport that helps with various functions of the system. **Vendor Services:** security services that protect against availability attacks).

TABLE V. A LIST OF THE MOST COMMON RISKS AND THEIR CORRESPONDING CONTROLS TARGETING BOOKING SYSTEMS

Risk	Counter Measures
Suspected phishing domain similar to the company website.	• block the domain. • request to take down the domain
A copy of a company application.	• request to remove the app
Employee login credentials on the dark Web.	• check the accounts • reset passwords • enable MFA
Company internal environment exposed.	• hide the internal environment • restrict access to authorized personnel only
Malware detected internally.	• remove the malware
User logon from a risky IP address.	• check with the user • block the IP
Activity from a Tor IP address.	• check with the user • block the IP
Files shared with unauthorized domain.	• check with the user • block the domain

TABLE VI. COMMON THREATS TARGETING WEB-BASED SYSTEMS AND THEIR COMMUNITIES

Type	**Threat Community (source)**	**Asset at Risk**	**Effect**
DDoS	Cyber criminals	Booking system	Availability
SQL injection	Cyber criminals	Booking system	Confidentiality
SQL injection	Cyber criminals	Booking system	Integrity
Cross site scripting	Cyber criminals	Booking system	Confidentiality
Cross site scripting	Cyber criminals	Booking system	Integrity
SQL injection	Script kiddies	Booking system	Confidentiality
SQL injection	Script kiddies	Booking system	Integrity
Privilege escalation	Privileged insiders and employees	Booking system	Confidentiality
Privilege escalation	Privileged insiders and employees	Booking system	Availability
Privilege escalation	Privileged insiders and employees	Booking system	Integrity
Bad bots	Cyber criminals	Booking system	Confidentiality
Illegal resource access	Cyber criminals	Booking system	Confidentiality
Phishing	Social engineer	Booking system	Confidentiality

TABLE VII. THE SELECTED RISK

Asset at Risk	Threat Community	Type	Effect
Booking system	Cyber criminals	DDoS	Availability

TABLE VIII. DDOS COMMUNITY PROFILE

Factor	Value
Motive	Financial disruption.
Primary intent	Illegal activities to maximize profit.
Sponsorship	Non-state or illegal gangs.
Preferred general target characteristics	Easy financial gains via remote means.
Preferred targets	Financial services and retail organizations.
Capability	Professional, skilled, and well-funded hackers.
Personal risk tolerance	Relatively high, without being exposed.
Concern for collateral damage	Prefer to keep their identities hidden.

D. Likelihood Estimation

Threat event frequency (TEF) was used to estimate the likelihood of a threat, indicating the probable frequency within a given timeframe that a threat would result in loss (see Table IX).

TABLE IX. THREAT EVENT FREQUENCY (TEF) FOR A DDOS ATTACK

TCom	Threat Type	TEF Min	TEF ML	TEF Max
Cyber criminals	DDoS	365 (per year) 1 (daily)	1,825 (per year) 5 (daily)	10,220 (per year) 28 (daily)

TCom: Threat community (source)
TEF Min: Minimum threat event frequency (attack frequency)
TEF ML: Most likely threat event frequency (attack frequency)
TEF Max: Maximum threat event frequency (attack frequency)

Similarly, loss-even frequency (LEF) was calculated to indicate the probable frequency within a given timeframe of a loss being expected to occur (see Table X).

TABLE X. LOSS EVENT FREQUENCY (LEF) FOR A DDOS ATTACK

TCom	Threat Type	LEF Min	LEF ML	LEF Max
Cyber criminals	DDoS	1 per year	2 (per year)	4 (per year)

1) Likelihood scale for the identified risk: According to the previously identified incident, the likelihood of a DDoS attack being successful was 2 (as per the previous incident). Table XI was used to derive the loss event frequency (likelihood) and total risk category to be input into the risk matrix.

2) Impact identification: The table below shows the total impacts due to loss of availability. Impact types varied between lost revenue, the cost of hiring an incident response team, and the cost of investigating the crime (i.e., forensics cost; see Table XII).

Table XIII shows the availability impact scale used by the company to identify the severity of an impact for the risk matrix.

TABLE XI. LIKELIHOOD SCALE FOR DDOS RISK

Score	Rating	X	Description
4	Very high (VH)		More than 5 likelihood of occurrence
3	High (H)		4–5 likelihood of occurrence
2	Medium (M)	X	2–3 likelihood of occurrence
1	Very low to unlikely (L)		0–1 likelihood of occurrence

TABLE XII. TOTAL IMPACT

Impact Type	Min. (1–2 h downtime)	Most Likely (3–5 h downtime)	Max. (10 h downtime)
Lost revenue	1,050,000	2,625,000	5,250,000
Incident response team(internal)	5,000	7,800	10,000
Forensics (external)	50,000	56,250	60,000
Total	1,105,000	2,689,050 (rounded) 2,700,000	5,320,000

TABLE XIII. AVAILABILITY IMPACT SCALE

Risk Rating	Impact
Low	• no significant effect on operations and services • asset can be replaced within an acceptable time frame • insignificant interruption costs
Medium	• no significant effect on operations and services • asset can be replaced within a medium time frame • low interruption costs
High	• effect on individual operations and services • critical assets cannot be replaced by manual methods • high interruption costs
Very High	• significantly affects multiple operations and services • critical assets cannot be replaced by manual methods • very high interruption costs

According to the scenario provided by the company's IT team, the DDoS attack was repeated twice, resulting in an approximate downtime of four hours (see Table XIV).

3) Risk matrix: The following risk matrix includes two factors: impact and likelihood. Both factors have a rating scale of 1–4, as shown in the previous scaling tables. The IT team identified the likelihood of the risk occurring as stated in the scenario (i.e., twice a year; medium rating = 2), and the teams also measured the loss impact of four hours of total system downtime (very high rating = 4). The risk level was then calculated as the likelihood of risk occurrence * impact of a loss, resulting in a risk level of eight (see Table XV).

The company's main risk objective was to protect the organization's information and technology assets by maintaining confidentiality, integrity, and availability of service effectively with minimum cost and without affecting business operations. The strategy for responding to risks

depended on the individual risk situation and was based on risk assessments and recommendations from decision-makers. As shown in Table XV, the risk level was relatively high and needed to be managed; hence, the transportation company decided to mitigate the risk by applying appropriate countermeasures. A list of countermeasures suggested by IT experts was prepared by the transportation company's IT team (see Fig. 2).

a) Internal controls

Procedures: enhance the DDoS Response Plan with:

- a systems checklist including all assets to ensure advanced threat identification and assessment.
- notifications and escalation procedures for quick recovery.

Training:

- train special teams to extensively monitor traffic and look for abnormalities, including unexplained traffic spikes and visits from suspect IP addresses and geolocations.
- create additional response teams to minimize the impact of attacks.

TABLE XIV. IMPACT SCALE FOR A DDOS ATTACK

Score	Rating	X	Description
4	Very high	X	More than 3 h downtime
3	High		1–3 h downtime
2	Medium		30 min–1 h downtime
1	Low		Less than 30 min downtime

TABLE XV. DDOS RISK MATRIX

Likelihood				
4	4	8	12	16
3	3	6	9	12
2	2	4	6	8
1	1	2	4	5

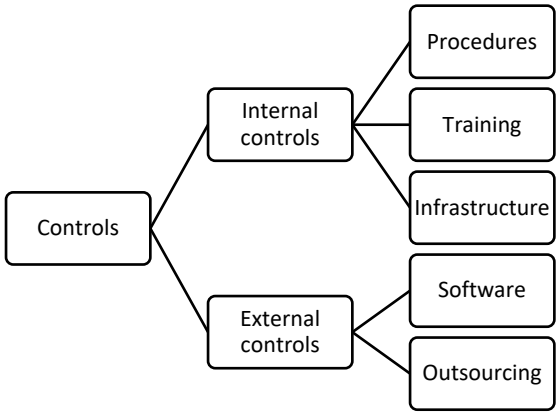

Fig. 2. List of Suggested Countermeasures.

Infrastructure:

- create redundant network (FW/IPS) resources so that, if one server is attacked, the others can handle extra network traffic.

b) External controls

Software:

- purchase threat intelligence software to monitor social media and the dark Web for threats, suspicious conversations, and boasts that may hint at an incoming attack.

Outsourcing:

- use third-party DDoS testing (i.e., pen testing) to simulate attacks against IT infrastructure so that the company can be prepared for any real threats.
- Use DDoS-as-a-service to provide improved flexibility for environments that combine in-house and third-party resources, or cloud and dedicated server hosting.
- outsource DDoS prevention to cloud-based service providers operated by software engineers whose job consists of monitoring the Web for the latest DDoS tactics. For decision-makers to choose between countermeasures for mitigating DDoS attacks, IT experts used the following scale to evaluate the effectiveness of each control.

Each control had a corresponding estimated cost and effectiveness rating (see Table XVI and XVII). The following criteria were used to choose the appropriate controls:

- If the control will reduce the risk more than needed, a less expensive alternative should be used.
- If the control will cost more than the risk reduction provided, an alternative should be used.
- If the control does not sufficiently reduce the risk, either more or different controls should be used.
- If the control provides sufficient risk reduction and is the most cost-effective option, use it.

TABLE XVI. CONTROL EFFECTIVENESS SCALE

Risk Rating	Impact
Ineffective	• poor control design • significant control gaps • does not treat root causes • does not operate effectively
Partially effective	• satisfies control design needs • partially treats the root causes of the risk • not very effective
Substantially effective	• designed correctly • treats most of the root causes of the risk • requires improvements to operate effectively
Fully effective	• well designed • addresses and treats all root causes • effective and reliable at all times

TABLE XVII. ESTIMATED COST FOR EACH CONTROL

#	Control	Estimated Cost	Effectiveness
1	Enhance the DDoS response plan	10,000	Ineffective
2	Train special teams	30,000	Partially effective
3	Create additional response teams	45,000	Partially effective
4	Use third-party DDoS testing	75,000	Substantially effective
5	Purchase threat intelligence software	100,000	Substantially effective
6	Create redundant network resources	200,000	Substantially effective
7	DDoS-as-a-service provision	350,000	Fully effective
8	Outsource DDoS prevention to a cloud-based service	500,000	Fully effective

c) Suggested controls for implementation: A cost–benefit analysis was conducted to identify the most appropriate controls and provide the greatest benefit to the company given the available resources. Two selected controls were recommended for implementation based on a cost–benefit analysis performed to justify why decision-makers should implement them (see Table XVIII).

TABLE XVIII. SUGGESTED CONTROLS FOR IMPLEMENTATION

#	Control	Estimated Cost	Effectiveness
3	Create additional response teams	45,000	Partially effective
6	Create redundant network resources	200,000	Substantially effective
Total Cost		245,000	Substantially effective

E. Cost–Benefit Analysis

The selected controls minimized the likelihood of a DDoS risk occurring twice to 0 or 1 (very low rating = 1), while the impact of DDoS was reduced from a total downtime of three hours to a medium impact (30 min–1 h), with a score of 2 (see Tables XIX and XX).

TABLE XIX. LIKELIHOOD OF A RISK AFTER IMPLEMENTING SELECTED COUNTERMEASURES

Score	Rating	X	Description
4	Very high (VH)		More than 5
3	High (H)		4–5 likelihood of occurrence
2	Medium (M)		2–3 likelihood of occurrence
1	Very low to unlikely (L)	X	0–1 likelihood of occurrence

TABLE XX. IMPACT OF THE RISK AFTER IMPLEMENTING THE SELECTED COUNTERMEASURES

Score	Rating	X	Description
4	Very high		More than 3 h downtime
3	High		1-3 h downtime
2	Medium	X	30 min–1 h downtime
1	Low		Less than 30 min downtime

As shown in the risk level matrix (see Table XXI), the new risk level was calculated as the likelihood of risk occurrence * impact of a loss, resulting in a residual risk level of two.

TABLE XXI. RESIDUAL RISK AFTER IMPLEMENTING CONTROLS

Likelihood				
4	4	8	12	16
3	3	6	9	12
2	2	4	6	8
1	1	2	4	5
	1	2	3	4

III. CONCLUSION

As shown in the case study scenario, the risk assessment identified the most critical attacks on the transportation company's booking system and provided suitable countermeasures to minimize the risk of attacks. The risk level decreased from eight to two, indicating the effectiveness of the selected countermeasures. Risk assessment was extremely useful for assessing potential risks and suggesting useful controls. Moreover, the two identified DDoS attacks were mitigated by implementing suitable controls, and recommendations were made to analyze and monitor incidents and increase the company's preparedness for another wave of DDoS or other attacks.

REFERENCES

[1] Y. Hong and S. Furnell, "Understanding cybersecurity behavioral habits: Insights from situational support," Journal of Information Security and Applications, vol. 57, p. 102710, 2021.

[2] Almaiah MA. A New Scheme for Detecting Malicious Attacks in Wireless Sensor Networks Based on Blockchain Technology. Artificial Intelligence and Blockchain for Future Cybersecurity Applications.:217.

[3] Siam AI, Almaiah MA, Al-Zahrani A, Elazm AA, El Banby GM, El-Shafai W, El-Samie FE, El-Bahnasawy NA. Secure Health Monitoring Communication Systems Based on IoT and Cloud Computing for Medical Emergency Applications. Computational Intelligence and Neuroscience. 2021 Dec 13;2021.

[4] Al Nafea R, Almaiah MA. Cyber security threats in cloud: literature review. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 779-786). IEEE.

[5] AlMedires M, AlMaiah M. Cybersecurity in Industrial Control System (ICS). In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 640-647). IEEE.

[6] Alamer M, Almaiah MA. Cybersecurity in Smart City: A systematic mapping study. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 719-724). IEEE.

[7] Ali A, Almaiah MA, Hajjej F, Pasha MF, Fang OH, Khan R, Teo J, Zakarya M. An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. Sensors. 2022 Jan;22(2):572.

[8] Almudaires F, Almaiah M. Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 732-738). IEEE.

[9] Almaiah A, Almomani O. An investigation of digital forensics for shamoon attack behaviour in FOG computing and threat intelligence for incident response. Journal of Theoretical and Applied Information Technology. 2020 Apr 15;98(07).

[10] Qasem MH, Obeid N, Hudaib A, Almaiah MA, Al-Zahrani A, Al-Khasawneh A. Multi-Agent System Combined With Distributed Data

Mining for Mutual Collaboration Classification. IEEE Access. 2021 Apr 20;9:70531-47.

[11] ALMAIAH A, Almomani O. An Investigator Digital Forensics Frequencies Particle Swarm Optimization for Dectection And Classification of Apt Attack in Fog Computing Enviroment (IDF-FPSO). Journal of Theoretical and Applied Information Technology. 2020 Apr 15;98(07).

[12] Almaiah MA. An Efficient Smart Weighted and Neighborhood-enabled Load Balancing Scheme for Constraint Oriented Networks.

[13] Almaiah MA, Al-Zahrani M. Multilayer Neural Network based on MIMO and Channel Estimation for Impulsive Noise Environment in Mobile Wireless Networks. International Journal of Advanced Trends in Computer Science and Engineering. 2020;9(1):315-21.

[14] Adil M, Khan R, Almaiah MA, Al-Zahrani M, Zakarya M, Amjad MS, Ahmed R. MAC-AODV based mutual authentication scheme for constraint oriented networks. IEEE Access. 2020 Mar 4;8:44459-69.

[15] Adil M, Khan R, Ali J, Roh BH, Ta QT, Almaiah MA. An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment. IEEE Access. 2020 Aug 31;8:163209-24.

[16] Bubukayr MA, Almaiah MA. Cybersecurity concerns in smart-phones and applications: A survey. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 725-731). IEEE.

[17] Almomani O, Almaiah MA, Alsaaidah A, Smadi S, Mohammad AH, Althunibat A. Machine Learning Classifiers for Network Intrusion Detection System: Comparative Study. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 440-445). IEEE.

[18] Al Hwaitat AK, Almaiah MA, Almomani O, Al-Zahrani M, Al-Sayed RM, Asaifi RM, Adhim KK, Althunibat A, Alsaaidah A. Improved security particle swarm optimization (PSO) algorithm to detect radio jamming attacks in mobile networks. Quintana. 2020;11(4):614-24.

[19] Almaiah MA, Dawahdeh Z, Almomani O, Alsaaidah A, Al-khasawneh A, Khawatreh S. A new hybrid text encryption approach over mobile ad hoc network. International Journal of Electrical and Computer Engineering (IJECE). 2020 Dec;10(6):6461-71.

[20] Adil M, Khan R, Almaiah MA, Binsawad M, Ali J, Al Saaidah A, Ta QT. An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks. IEEE Access. 2020 Aug 11;8:148510-27.

[21] Khan MN, Rahman HU, Almaiah MA, Khan MZ, Khan A, Raza M, Al-Zahrani M, Almomani O, Khan R. Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks. IEEE Access. 2020 Sep 25;8:176495-520.

[22] Adil M, Almaiah MA, Omar Alsayed A, Almomani O. An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. Sensors. 2020 Jan;20(8):2311.

[23] D. P. F. Möller and R. E. Haas, Automotive Cybersecurity: A Guide to Automotive Connectivity and Cybersecurity. Cham: Springer International Publishing, pp. 265–377, 2019.

[24] M. Waheed and M. Cheng, "A system for real-time monitoring of cybersecurity events on aircraft," IEEE, pp. 1–3, 2017.

[25] E. Aboul, M. Hassanien and Elhoseny, Advanced Sciences and Technologies for Security Applications Cybersecurity and Secure Information Systems Challenges and Solutions in Smart Environments.

[26] A. Zarreh, H. Wan, Y. Lee, C. Saygin and R. A. Janahi, "Cybersecurity concerns for total productive maintenance in smart manufacturing systems," Procedia Manufacturing, vol. 38, pp. 532–539, 2019.

[27] G. Pizzi, "Cybersecurity and its integration with safety for transport systems: Not a formal fulfillment but an actual commitment," Transportation Research Procedia, vol. 45, pp. 250–257, 2020.

[28] M. Kevin, F. Ana and K. Alexey, "Smart information systems in cybersecurity," The ORBIT Journal, vol. 2, no. 2, pp. 1–26, 2019.

[29] C. Hess. and E. Ostrom, "A Framework for Analyzing the Knowledge Commons: a chapter from Understanding Knowledge as a Commons: from Theory to Practice, 2005," Conference on Dependability and Complex Systems 2015, pp. 97–106.

[30] K. Cheung, M. G. Bell and J. Bhattacharjya, "Cybersecurity in logistics and supply chain management: An overview and future research directions," Transportation Research Part E: Logistics and Transportation Review, vol. 146, p. 102217, 2021.

[31] P. Lau, W. Wei, L. Wang, Z. Liu and C. Ten, "A cybersecurity insurance model for power system reliability considering optimal defense resource allocation," IEEE Transactions on Smart Grid, vol. 11, no. 5, pp. 4403–4414, 2020.

[32] A. Thaduri, M. Aljumaili, R. Kour and R. Karim, "Cybersecurity for e-maintenance in railway infrastructure: Risks and consequences," International Journal of System Assurance Engineering and Management, vol. 10, no. 2, pp. 149–159, 2019.

[33] E. Kweon, H. Lee, S. Chai and K. Yoo, "The utility of information security training and education on cybersecurity incidents: Empirical evidence," Information Systems Frontiers, pp. 1–13, 2019.

[34] R. Baskerville, F. Rowe and F. Wolff, "Integration of information systems and cybersecurity countermeasures: An exposure to risk perspective." ACM SIGMIS Database: The Database for Advances in Information Systems, vol. 49, no. 1, pp. 33–52, 2018.

[35] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li and S. Huang, "Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems," IEEE Transactions on Systems, Man, and Cybernetics. Systems, vol. 46, no. 10, pp. 1429–1444, 2016.

[36] N. Polatidis, M. Pavlidis and H. Mouratidis, "Cyberattack path discovery in a dynamic supply chain maritime risk management system," Computer Standards & Interfaces, vol. 56, pp. 74–82, 2018.

[37] M. Alali, A. Almogren, M. M. Hassan, I. A. L. Rassa and M. Z. A. Bhuiyan, "Improving risk assessment model of cyber security using fuzzy logic inference system," Computers & Security, vol. 74, pp. 323–339, 2018.

[38] J. Van Erp, "New governance of corporate cybersecurity: A case study of the petrochemical industry in the Port of Rotterdam," Crime, Law and Social Change, vol. 68, no. 1, pp. 75–93, 2017.

[39] G. Lykou, G. Iakovakis and D. Gritzalis, "Aviation cybersecurity and cyberresilience: assessing risk in air traffic management," Critical Infrastructure Security and Resilience. Cham: Springer International Publishing, pp. 245–260, 2019.

[40] I. De La Peña Zarzuelo, "Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue," Transport Policy, vol. 100, pp. 1–4, 2021.