-

EXPLORING THE ROLE OF CYBER SECURITY MEASURES (ENCRYPTION, FIREWALLS, AND AUTHENTICATION PROTOCOLS) IN PREVENTING CYBER-ATTACKS ON E-COMMERCE PLATFORMS

Abdullah Faisal Al Naim

Management Department, College of Business Administration,
King Faisal University, Al-Ahsaa 31982,
Saudi Arabia. Email: afalnaeem@kfu.edu.sa

Arsalan Mujahid Ghouri

School of Business, London South Bank University,
United Kingdom. Email: ghour3@lsbu.ac.uk

─Abstract─

The present study seeks to examine the significance of cybersecurity measures, specifically encryption strength (ES), firewall configuration (FC), and authentication protocols (AP), in protecting e-commerce platforms against cyber-attacks. The data collection process involved the administration of a survey to IT professionals responsible for overseeing e-commerce operations in a range of organisations located in Saudi Arabia. A convenience sampling method was employed to distribute a total of 300 questionnaires, out of which 190 completed responses were selected for analysis. The measurement model, which encompassed variables such as ES, FC, AP, security training (ST), cyber-attack incidents (CAI), customer trust (CT), and incident response time (IRT), was estimated using the structural equation model in Amos. The results of this study provide insights into the relationship between cybersecurity measures and their influence on the frequency of cyberattacks. The study highlights the significance of encryption, firewall configuration, and authentication protocols in strengthening e-commerce platforms. Additionally, this study examines the impact of security training on the improvement of overall cybersecurity posture and its subsequent effect on customer trust. The examination also takes into account the duration of incident response as a critical element in minimising the consequences of cyber incidents. The findings obtained from this study contribute to a more comprehensive comprehension of the cybersecurity environment within the realm of electronic commerce.

Electronic copy available at: https://ssrn.com/abstract=4626041

Consequently, this research offers practical implications for organisations to improve their cybersecurity strategies and safeguard themselves against emerging cyber threats.

Keywords: Encryption Strength (ES) Firewall Configuration (FC) Authentication Protocols (AP) Security Training (ST) Cyber- attack Incidents (CAI) Customer Trust (CT) Incident Response Time (IRT)

INTRODUCTION

Cybersecurity refers to the proactive measures taken to safeguard systems, computers, networks, programmes, personal data, and other digital assets from unauthorised access, digital intrusions, and various forms of threats. Cybersecurity refers to the systematic measures undertaken to safeguard and shield information and communication systems against unauthorised access, alteration, or utilisation. The term "information technology security" serves as a synonym for "cyber security." The field of computer security encompasses various methodologies aimed at safeguarding computers, networks, software applications, and data from unauthorised access or malicious attacks that have the potential to inflict harm or exploit vulnerabilities. Cybersecurity can be defined as a technical methodology employed to safeguard computer systems from unauthorised access and malicious intrusions (Oruj, 2023). In this context, Surya et al. (2023) presents a proposed model for cyber-security that highlights the significance of OTP verification, password safeguarding, and a multi-faceted security strategy in ensuring the security of online transactions. The study conducted by Shaikh, Beniwal, and Iliev (2019) centres on the mitigation of denial-of-service (DoS) attacks in the context of e-commerce. The author proposes the utilisation of a glowworm swarm optimisation-based support vector neural network (GSO-SVNN) and elliptic-curve cryptography (ECC) as potential solutions.

Qasaimeh et al. (2022) and Jamra, Anggorojati, Sensuse, and Suryono (2020) highlight the high occurrence of security incidents within the realm of electronic commerce, including but not limited to hacking, data breaches, fraudulent activities, and instances of identity theft. There is a strong emphasis on the requirement for comprehensive security solutions to effectively tackle these challenges. Qasaimeh et al. (2022) underscores the significance of security in relation to customer satisfaction, underscoring the necessity of effectively addressing vulnerabilities and threats in a transparent manner to enhance trust and foster greater demand for e-commerce applications. In the study conducted by Bansal, Khosla, and Saini (2023), the author examines the security challenges encountered by e-commerce applications and presents an overview of the various techniques utilised to enhance security measures. Mitra, Kulkarni, Pathak, and Natrai (2022) underscores the imperative for e-commerce enterprises to effectively address cyber security challenges, such as credit card fraud and phishing attacks, by giving utmost priority to the preservation of data confidentiality, integrity, and availability. According to Qasaimeh et al. (2022),

Electronic copy available at: https://ssrn.com/abstract=4626041

enhancing customer satisfaction and trust in e-commerce applications can be achieved by effectively addressing security concerns and raising awareness about vulnerabilities.

In the context of the swiftly evolving digital environment, the amalgamation of digitization and cyber threats introduces novel complexities for safeguarding organisational security. The application of a mentality of capability development and preventive protection mechanisms is a fundamental aspect of the evolutionary approach to cyber security (Safitra, Lubis, & Fakhrurroja, 2023). The process involves shifting from traditional static security measures to adaptive defence strategies in response to cyber threats (Abdullayeva, 2023). Organisations can enhance their ability to respond to emerging threats and strengthen their security posture by leveraging evolutionary principles (Nicholson & McGlasson, 2020). The study conducted by Li (2023) provides a thorough examination of contemporary techniques employed in internet measurement for the purpose of enhancing cyber security. The research underscores the significance of conducting comprehensive investigations that incorporate diverse viewpoints and data resources. The study conducted by Alatawi et al. (2023) centres around the field of intrusion detection and presents a novel approach that integrates swarm intelligence and evolutionary algorithms.

The objective of this hybrid method is to enhance the precision and effectiveness of cyber security applications. In the publication by Aslan et al. (2023), an analysis is conducted on the vulnerabilities, threats, and attacks prevalent in the field of cyber security. The author underscores the importance of adopting innovative and practical strategies to effectively mitigate the risks posed by sophisticated cyberattacks. The study conducted by Salih and Abdulrazzaq (2023) delves into the analysis of performance and the challenges encountered in the field of cyber security, with a specific focus on attack detection. The research proposes the adoption of deep learning architectures as a means to improve the effectiveness of detection mechanisms.

LITERATURE REVIEW

The significance of implementing security measures to safeguard e-commerce platforms against cyberattacks is highlighted in the subsequent methods. In a recent study conducted by Bhatia, Shukla, Punhani, and Dubey (2021), the author examined the implementation of security measures such as one-time passwords (OTP) and key management systems (KSM) in the context of safeguarding data on e-commerce platforms such as Amazon and Alibaba. The significance of computer security technology (CST) in mitigating security concerns within the realm of e-commerce was underscored by Wang (2021). This includes the implementation of digital signatures, firewalls, and VIP systems. In another study conducted by Mitra, Kulkarni, Pathak, and Natrai (2022), the author highlights the importance of addressing the various challenges related to cyber security within the context of e-commerce. Specifically, the study

Electronic copy available at: https://ssrn.com/abstract=4626041

emphasises the significance of upholding the pillars of data confidentiality, integrity, and availability.

In a recent study conducted by Qasaimeh et al. (2022), a comprehensive analysis was conducted on the security aspects of e-commerce systems. The study emphasised the difficulties encountered in ensuring robust security and underscored the significance of implementing appropriate security measures. The examination of different cyber security measures in the context of e-commerce has yielded valuable insights regarding the suggested strategies. Thakur et al. (2023) has put forth a security protocol that incorporates blockchain technology to enhance privacy and address vulnerabilities in cloud-based digital twin environments, thereby providing improved security capabilities. Similarly, Aslan et al. (2023) underscored the constraints inherent in conventional protection systems and emphasised the imperative for novel approaches, such as machine learning, deep learning, cloud platforms, big data, and blockchain, to effectively identify intricate cyber-attacks.

Data Encryption in Ecommerce:

In their work, Wen (2023) introduces a layered encryption framework known as PABB, which employs a combination of distinct encryption algorithms in order to strike a harmonious equilibrium between security and efficiency considerations. The paper by Blancaflor et al. (2023) examines the application of cryptography, with a specific focus on the RSA algorithm, as a means to enhance data security within the e-commerce sector in the Philippines. The significance of encryption technology in safeguarding sensitive information during data transmission and the incorporation of access control measures are underscored by Li (2023). The study conducted by Shen et al. (2023) introduces a novel approach to safeguarding data privacy and countering collusive attacks on e-commerce platforms. The proposed scheme integrates secret sharing and homomorphic encryption techniques to enable privacy-preserving and verifiable statistical analysis. Previous research has established the importance of encryption in protecting user privacy and ensuring data security within e-commerce platforms.

Firewall Configuration in Ecommerce Platform

In their study, Bringhenti et al. (2022) presents a novel approach to automating the configuration of packet filters within virtual networks. The proposed methodology aims to effectively address security requirements by optimising the utilisation of firewalls and rules, thereby minimising their overall number. In another study conducted by Shin, Carley, Dobson, and Carley (2023), it is proposed that the implementation of a human firewall system within small and medium-sized businesses (SMBs) can serve as a cost-effective alternative to expensive security plans. The research findings indicate that a properly equipped human firewall has the potential to significantly reduce the negative impact of cyberattacks.

Electronic copy available at: https://ssrn.com/abstract=4626041

Authentication Protocols in Ecommerce Platform

In their study, Panja et al. (2022) presents a novel approach for implementing a highly efficient and secure authentication scheme based on fingerprint recognition, employing the principles of elliptic curve cryptography. In Petcu, Pahontu, Frunzete, and Stoichescu's (2023) scholarly work, the author explores an authentication mechanism that prioritises security and decentralisation. This mechanism is built upon the foundations of Web 3.0 and utilises Ethereum blockchain technology. The study conducted by Chaturvedi (2022) involves a comparative analysis of various authentication techniques, with a specific emphasis on the implementation of a resilient JWT authentication system. Although Sagoo (2022) does not present explicit findings, it underscores the significance of effectively implementing authentication and authorization measures within online enterprises. In general, the aforementioned papers underscore the necessity of implementing robust and effective authentication protocols within e-commerce platforms. These studies delve into various methodologies, including biometrics, blockchain, and JSON Web Tokens (JWT), to address this imperative.

Security Training in Ecommerce Platform:

In their work, Nocera, Romano, Francese, and Scanniello (2023) suggests the integration of a Static Analysis Tool (SAT) within the development pipeline of web applications as a means to identify potential security vulnerabilities. The significance of OTP verification, password protection, multi-layered security approaches, and employee training in safeguarding online transactions and mitigating cybersecurity risks is underscored by Surya et al. (2023). The paper by Bansal, Khosla, and Saini (2023) examines the security challenges that arise in the context of e-commerce applications and proposes several strategies to address these challenges. The publication " Pagey, Mannan, and Youssef (2023) " sheds light on the vulnerabilities present in e-commerce platforms that extend beyond the integration of checkout and payment systems. These vulnerabilities encompass store takeover and the listing of illicit products. The article underscores the importance of conducting security evaluations and engaging in responsible disclosure practises to address these issues. In conclusion, the aforementioned studies have indicated the significance of integrating security training, tools, and measures in order to bolster the security of electronic commerce platforms.

Incident Response Time Mediating the Relationship between Cyber Security Measures and Cyber-Attack Incidents:

In his work, Basuki and Adriansyah (2023) presents a methodology aimed at enhancing the response time within vulnerability management systems. The author underscores the significance of expeditious and precise scanning processes in order to effectively minimise the detrimental effects resulting from cyberattacks. Chaudhuri (2023)

Electronic copy available at: https://ssrn.com/abstract=4626041

examines the importance of incident response planning and best practices, emphasising the crucial role of efficient incident response in mitigating the consequences of security issues. In his work published in 2023, Özkan and Tolga (2023) introduces the notion of "zero-day readiness" within the realm of cyberspace. The author underscores the importance of maintaining a state of agile and vigilant cyber readiness in order to effectively counter the ever-changing landscape of threats. The study conducted by Bennett and Robertson (2023) emphasises the significance of training exercises for cyber defence analysts in effectively addressing cyber incidents in real-time, thereby facilitating prompt containment and resolution of security concerns. These studies collectively highlight the significance of prompt incident response time in moderating the association between cybersecurity measures and the occurrence of cyberattack incidents.

Encryption Strength, Firewall Configuration, Authentication Protocols, Security Training positively affects Incident Response Time and Customer Trust:

In their study, Woods, Böhme, Wolff, and Schwarcz (2023) emphasises the significance of cyber insurance and legal factors in shaping incident response. The author points out that the involvement of legal professionals can introduce procedural steps and limitations that may impede the efficiency of the response process. The author, Ashok and Gopikrishnan (2023) examines various security models and their corresponding performance metrics, highlighting their potential influence on incident response time. The significance of implementing preventive measures and acquiring knowledge about prevalent attack techniques in order to mitigate cyberattacks is underscored by AL-Hawamleh (2023). The study conducted by Walter et al. (2023) places emphasis on the preservation of data confidentiality during the process of information exchange within the context of Industry 4.0. The research proposes the use of an architectural analysis methodology as a means to identify and address potential security concerns that may arise. Dimitriadis (2023) emphasised the adverse consequences of network breaches on organisational reputation, specifically noting the potential erosion of customer trust.

The study conducted by Kanaan et al. (2023) primarily examined the domain of e-government services, with a specific focus on the factors of quality, security, and privacy. The findings of the study indicate that these aforementioned factors have a positive impact on the establishment of trust in e-government services. In a study conducted by Wang et al. (2023), an investigation was conducted on the trustworthiness of GPT models. The study specifically focused on identifying vulnerabilities associated with toxicity, bias, privacy, and adversarial robustness. Kim and Kyung (2023) carried out a study to look into the various factors that affect the uptake of electronic authentication services. The findings of the study revealed that perceived benefits, sacrifices, threats, and adoption motives have a significant impact on both trust and adoption intentions.

Electronic copy available at: https://ssrn.com/abstract=4626041

In a similar vein, Sadab, Mohammadian, and Ullah (2023) aimed to investigate consumer perceptions and behaviours in relation to online shopping. Specifically, the research examined the various elements of cybersecurity that influence consumer trust and involvement in online transactions. These factors encompassed apprehensions regarding hacking activities, instances of identity theft, and occurrences of credit card fraud. In their study, Saeed (2023) examined the customer-centric perspective of security and privacy in the context of e-commerce. The author underscored the significance of comprehending customer concerns and perceptions in order to formulate suitable policies and establish secure technological frameworks. Previous research has underscored the importance of implementing sophisticated security protocols, developing novel solutions, and adopting customer-centric strategies to bolster cybersecurity measures in the realm of electronic commerce.

Encryption Strength, Firewall Configuration, Authentication Protocols and Security Training negatively Affects Cyber-attack Incidents in Ecommerce Platform:

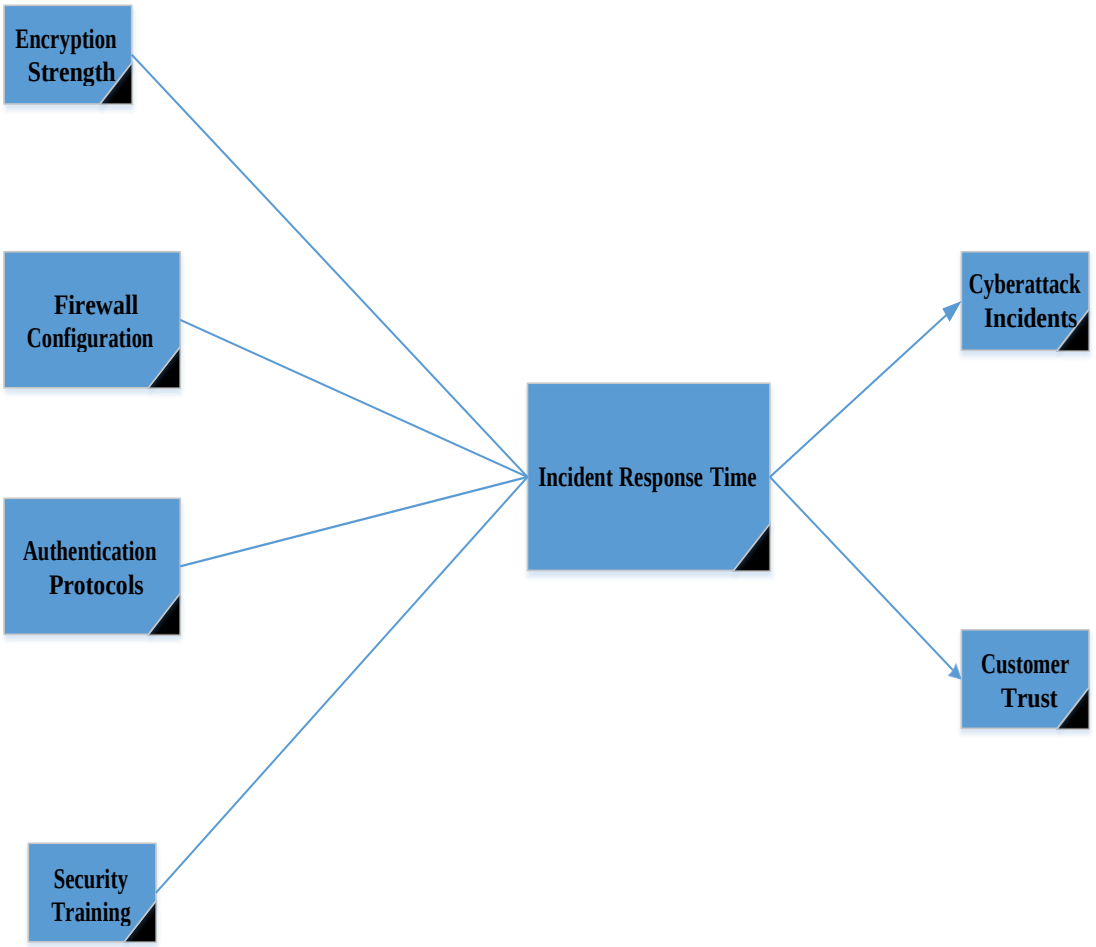
Previous research has indicated that factors such as the level of encryption employed, the configuration of firewalls, the protocols used for authentication, and the provision of security training are all significant in mitigating the occurrence of cyberattacks within e-commerce platforms. Harshavardan and PadmaShani (2023) emphasise the significance of vulnerabilities present in e-commerce platforms and the imperative to mitigate cyber-attacks by effectively addressing the key vulnerabilities identified by OWASP. In the study conducted by Liu and Mackie (2004), the author emphasises the necessity for developers to adopt a systematic approach in identifying and mitigating vulnerabilities within e-commerce applications, with the ultimate goal of enhancing security measures. Treese (2000) examines the fundamental elements of internet security, encompassing firewalls, encryption, authentication, and system hardening. The collective findings indicate that the implementation of robust encryption, the configuration of efficient firewalls, the utilisation of secure authentication protocols, and the provision of security training can effectively reduce the occurrence of cyberattack incidents in e-commerce platforms.

Incident Response Time in Cyber-attacks Incidents can impact Customer Trust in Ecommerce:

According to scholarly researchers, the duration of incident response in instances of cyberattacks has the potential to significantly influence the level of trust customers place in e-commerce platforms. In line with Apau and Koranteng (2019), there is a significant relationship between trust in internet media, perceptions of cybercrime, and users' intention to engage in e-commerce activities. In the study conducted by Su and Manchala (1999), various strategies for identifying and mitigating attacks in the realm

Electronic copy available at: https://ssrn.com/abstract=4626041

of electronic commerce are examined. The author places significant emphasis on the crucial role of trust and security in upholding customer confidence. Natheniel et al. (2017) underscored the importance of effectively managing customer awareness and security measures within the realm of electronic commerce, with the aim of minimising potential risks and enhancing consumer confidence. The present study (Alswiay & Cagiltay, 2018) aims to construct a conceptual model that illustrates the interconnections among various factors that influence trust in business-to-consumer (B2C) electronic commerce. This model is formulated by analysing the findings of prior research investigations. The study conducted by Coles and Smart (2011) reveals that there exists a significant relationship between website design and a consumer's inclination to make a purchase on a website. Web developers play a significant role in bolstering consumer trust. The achievement of this objective can be facilitated by imparting knowledge and fostering confidence in users through the comprehensive design and informative substance of the website, along with the scrupulous curation and integration of various website design components.



Electronic copy available at: https://ssrn.com/abstract=4626041

Measurements:

Measurement Factors	References
"Encryption Strength"	Harvard catalyst Questionnaire
1. "In general, it is known that how to contact the individual or office responsible for information security	
2. In general, it is known that the scope of the data custodian/manager's responsibility	
3. In general, it is known that what would constitute an unauthorized use or disclosure or breach of data/information	
4. In general, it is known that whom to contact in research compliance/administration if there is a suspected unauthorized use or disclosure or breach"	
5. "In general, it is known that whom to contact in IT if there is a suspected unauthorized use or disclosure or breach	
6. In general, it is known that that a data breach is categorized as major when it involves over 500 records	
7. In general, it is known that whom to approach/contact for research data protection and security questions	
8. In general, it is known that the differences between low, moderate, and high-risk data	
9. In general, it is known that on your team understand the differences between low, moderate, and high-risk data	
10. In general, it is known that where to find information about your institutional policies on research data privacy and security?	
11. Is everyone on your team up to date on their required trainings (Human Subjects, Data Security, etc.)	
12. In general, it is known that if documentation on all of the projects is up to date (e.g., data risk assessment, trainings, etc.)	
13. In general, it is known that a data manager record when the data arrives and when the data are destroyed	
14. If research subject identifiable data are stored on any portable devices (e.g., laptop, smart phone, tablet, etc.), are the devices encrypted. In general, it is known that research subject identifiable data off any personal device, home computer, or other privately owned machine	
15. If there is a delay setting up a new team member, do you remind others on the team not to share passwords or account information in the meantime	
16. In general, it is known that regularly monitor and assess the permissions" "and activity of the files and folder for data set(s)	
17. In general, it is known that remove identifiers before sharing data via print, fax, or email	
18. In general, it is known that dispose of printed data that contains identifiers with the office/department shredder or records removal container (e.g., Iron Mountain)	
19. Is there a process for managing and removing an individual's access privileges (e.g., folders and files that contain data sets) to research data when they leave the research project or the institution?	
20. Portable devices (e.g., laptop, smart phone, tablet, etc.) storing research subject identifiable data must be encrypted.	
21. Research subject identifiable data must not be stored on any personal, privately owned device, home computer, or other privately owned device.	
22. If your research study has a Data Use Agreement (DUA), Memo of Understanding (MOU), or other contract, was it was reviewed by the IRB, IT and signed by the appropriate institutional official with signatory authority? In general, it is known that if documentation for the DUA, MOU, or other contract is up to date? (e.g., additions to the study team, extension of time to use data, etc.)	
23. In general, it is known that where to find expiration dates for the DUA(s), MOU(s), or other contracts?	
24. In general, it is known that if your study has more than one DUA or contract?	
25. In general, it is known that where to find the documents that govern use of your data and research projects? (e.g., signed DUA, Protocol Approval Letter, MOU, or another contract, etc.)"	
"Firewall Configuration"	Arjmandi, Boeck,

Electronic copy available at: https://ssrn.com/abstract=4626041

1. "The software (Windows Vista Firewall) is easy to use 2. I will be able to learn how to use all the facilities if offered in this software 3. The contents of the menus and toolbars match my needs 4. Finding the options that I want in the menus and toolbars is easy 5. It is easy to make the software do exactly what I want 6. Discovering new features is easy 7. This software is satisfying to use"	Raja, and Viswanathan (2007).
"Authentication Protocols"	Guest et al. (2021).
1. "The installed setup has proper process of failed SAS eligibility re-check 2. The installed setup has proper process of Duplication/Already enrolled 3. The installed setup has proper process of case study participant attempts to enrol 4. The installed setup has proper process of passed; referred to manual authentication 5. The installed setup has proper process of failed, no checklist completed (duplicate) 6. The installed setup has proper process of failed manual checklist and removed 7. The installed setup has proper process of passed and enrolled 8. The installed setup has proper process of Timestamp fail 9. The installed setup has proper process of Suspicious pattern survey response fail 10. The installed setup has proper process of social media check fail (if provided)"	
"Security Training"	Wilson and Hash (2003).
1. "Normally, employees received adequate training to fulfil their security responsibilities 2. Normally, employee training and professional development documented and monitored? " 3. "The percentage of employees with significant security responsibilities who have received specialized training 4. To gauge the level of expertise among designated security roles and security responsibilities for specific systems within the agency 5. Normally, significant security responsibilities defined, with qualifications criteria, and documented 6. Normally, records kept of which employees have specialized security responsibilities? 7. Normally, employees in your agency (or agency component, as applicable) have significant security responsibilities 8. Normally, training records maintained? (Training records indicate the training that specific employees have received.) 9. Normally, training plans state that specialized training is necessary 10. If all personnel have not received training, state all reasons that apply: o Insufficient funding o Insufficient time o Courses unavailable o Employee has not registered o Other (specify) "	
"Cyber-attack Incidents"	Al-Mohannadi et al.

Electronic copy available at: https://ssrn.com/abstract=4626041

1. "In general, it is known that, In terms of your security duty, do you have a defined checklist for your daily duty 2. In general, it is known that you recognize any of the terms during a cyberattack 3. In general, it is known that the following Indicator of compromise (IoC) is the most/least difficult to trace in your environment 4. In general, it is known that the common alerts do you handle daily 5. In general, it is known that In case of repetitive attacks, what action do you take" 6. "In general, it is known that you have any procedure to follow in case of attacks 7. In general, it is known that you use any (firewall, IDS, IPS, router etc.) log data to understand activities in the network 8. In general, it is known that you have an operation centre to monitor all attacks? 9. Is your workstation/Server implemented using a managed client/server architecture, or in a stand-alone to push the policy configuration and update? 10. In general, it is known that you have demilitarized zone (DMZ) for external and firewall for internal cross-site 11. In general, it is known that it helps in isolating or preventing the attack 12. In general, it is known that you recognise any of the components from the following during a cyber-attack Hash values IP Address Domain Name Network Artefact Host Artefact Attack tools (e.g., used same tool before by attacker) Other special techniques 13. In general, it is known that which one is the most/least difficult to trace for supporting the alert system 14. In general, it is known that what kind of alert you get 15. In general, it is known that if you see same kind of attack happening in your network, what action do you take 16. In general, it is known that you have any procedure to follow 17. In general, it is known that you use any (firewall, router etc.) log data to understand activities in the network 18. In general, it is known that you any operation centre to monitor all attacks" 19. "In general, it is known that all the pc/ machine has the same configuration and update in the operation room 20. In general, it is known that the firewalls are flat or cross site"	(2018).
"Customer Trust"	Setyadi, Rahman,

Electronic copy available at: https://ssrn.com/abstract=4626041

1. "There are still problems, difficulties, and problems with IT (Computer / WIFI / LCD projector / Printer) at school 2. IT access (Computer / WIFI / LCD projector / Printer) in schools is easy to use / connect with other systems (notebook / netbook). 3. IT is used efficiently by the user (resources / systems are still minimal). 4. IT is used effectively by users (maximum results). 5. IT is used productively by users (efficient and effective) 6. IT is used to help users work. 7. IT is used to control work / help users. 8. IT supports and completing users work. 9. IT encourages users to achieve their work goals. 10. IT supports users to better understand their work than other workers. 11. IT (computer/printer/LCD projector/WIFI) is foreign to users 12. IT (computers) are not supported by a good operating system. 13. IT (computer / printer / LCD projector / WIFI) is confusing to users. 14. IT (computers) is not easy to use (especially to use an operating system). 15. IT (WIFI, Computer) is not free to use (There is a password to protect system). 16. IT (computer / WIFI/ printer / LCD) is not safe for users to use. 17. IT (computer / WIFI / printer / LCD) causes harm to users. 18. IT causes less interaction with other users. 19. IT causes users not to focus on other jobs. " 20. "IT damaged the tool system. 21. IT (computer / LCD projectors / printers) is accurate and easy to learn. 22. IT (WIFI) can be accessed (no password) in use. 23. IT (WIFI) has speed and efficient access as needed. 24. IT (computer / WIFI/ printer / LCD projector) works efficiently. 25. IT (computer / WIFI/ printer / LCD projector) works effectively. Variable Questions 26. IT (LCD / access WIFI / computer usage) is convenient to use (fast / safe / easy). 27. IT (LCD / WIFI access / computer usage) is easy to use. 28. IT (LCD / WIFI access / computer usage) fast access / response when used. 29. IT (LCD / WIFI access / computer usage) is modern / sophisticated school / and according to user needs. 30. IT provides services according to the functions that are needed by users. 31. IT has good and fast connection / usage (WIFI) access. "	and Subiyakto (2019).
"Incident Response Time"	Line et al. (2006).

Electronic copy available at: https://ssrn.com/abstract=4626041

Supervisory Control and Data Acquisition **During a period (d.ap.)** 1. "The installed system has estimated the rating system for the incident response management system 2. The installed system has estimated the assessment of information security culture regarding incident response 3. The installed system has estimated the number of incidents responded to d.ap. 4. The installed system has estimated the total consequences of incidents d.ap 5. The installed system has estimated the number of incidents of high loss d.ap 6. The installed system has estimated the downtime of SCADA systems d.ap" 7. "The installed system has estimated the total costs related to incident response d.ap 8. The installed system has estimated the average order of feedback d.a.p."	

METHODOLOGY

Sample and Data Collection and Analysis

The data was gathered from employees who are employed in Information Technology (IT) departments and hold responsibilities related to e-commerce operations within different organisations in Saudi Arabia. A survey questionnaire was employed to gather data through the use of convenience sampling methodology. A total of 300 questionnaires were distributed, and subsequently, 190 fully completed questionnaires were received and utilised for the purpose of analysis. The data analysis was conducted using SPSS and Amos-20, which is a software programme commonly used for Structural Equation Modelling (SEM).

Measurement

The researcher employed a meticulously crafted instrument for data collection. The researcher placed significant reliance on a well-established instrument due to its high levels of reliability and validity. The researchers employed a five-point Likert scale to capture the responses of the participants. The questionnaire consisted of inquiries pertaining to the constructs under investigation in the present study.

Data analysis

The currently ongoing investigation incorporates latent variables, which are comprised of multiple items. Therefore, the utilisation of structural equation modelling (SEM), a multivariate technique, is deemed the most suitable approach for conducting the analysis in the present study. Consequently, the researcher employed structural equation modelling in the software AMOS to estimate the necessary measurement model. The use of structural equation modelling (SEM) is recommended for analysing data collected through survey-based instruments that involve latent variables. Researchers have found that the use of the Structural Equation Modelling (SEM) technique in AMOS software yields more precise and reliable outcomes (Byrne, 2013).

Electronic copy available at: https://ssrn.com/abstract=4626041

Reliability and Validity

The study employed confirmatory factor analysis to conduct tests on the reliability and validity of the measures. The researcher conducted an analysis of the validity and reliability of the factors following the determination of their loading. Hair, Risher, Sarstedt, and Ringle (2019) stated that a factor loading must meet or exceed a minimum threshold level of 0.60 in order to be considered for inclusion in subsequent analyses. Hence, for the purpose of inclusion in the analysis, it is necessary that all factors exhibit loadings exceeding 0.60. In addition, it is essential for the construct's reliability to exceed a threshold of 0.70, while the variable should possess an Average Variance Extracted (AVE) value higher than 0.50. Purwanto (2021) asserts that the composite reliability of the construct should exceed a threshold of 0.70. Table 1 demonstrates that the data is suitable for subsequent analysis and satisfies all the aforementioned criteria for data fitness. Thus, the data meets all the defined criteria (including reliability and validity). Furthermore, the discriminant validity of the construct was assessed by comparing the average variance extracted (AVE) values with the squared correlation values. Specifically, it was determined that the AVE values along the diagonal should exceed the squared correlation values.

Table 1. Factor Loadings Reliability, Convergent Validity

	CR	**AVE**	**α**
Encryption Strength (ES)	0.73	0.56	0.78
Firewall Configuration (FC)	0.80	0.51	0.73
Authentication Protocols (AP)	0.81	0.50	0.81
Security Training (ST)	0.84	0.59	0.86
Cyber- attack Incidents (CAI)	0.75	0.54	0.87
Customer Trust (CT)	0.72	0.59	0.88
Incident Response Time (IRT)	0.77	0.62	0.79

Table 2. Discriminant Validity

	1	**2**	**3**	**4**	**5**	**6**	**7**
ES	**0.58**						
FC	0.20**	**0.57**					
AP	0.25**	0.12**	**0.60**				
ST	0.18**	0.19**	0.23**	**0.55**			
CAI	0.20**	0.20**	0.18**	0.09**	**0.50**		
CT	0.22**	0.28**	0.11**	0.24**	0.28**	**0.60**	
IRT	0.29**	0.26**	0.09**	0.17**	0.26**	0.23**	**0.57**

*Note: values of AVE on diagonal higher than squared correlations values. † p < 0.100; * p < 0.050; ** p < 0.010; *** p < 0.001*

Electronic copy available at: https://ssrn.com/abstract=4626041

Table 4. Measurement Model Fit

Overall Model Measure	Overall Model Score	Acceptable Model Fit	Acceptable Baseline
CFI	**0.95**	**Accept**	≥0.90
AGFI	**0.88**	**Accept**	≥0.80
RMSEA	**0.047**	**Accept**	≤0.08
CMIN/df	**1.67**	**Accept**	≤3
TLI	**0.91**	**Accept**	≥0.90
IFI	**0.92**	**Accept**	≥0.90

Table 4 presents the model fit indices of the structural model of the study. It can be seen that all of the fit indices for structural model are within the suggested ranges which shows that the structural model is a good fit.

Table 5. Structural Model Fit

Overall Model Measure	Overall Model Score	Acceptable Model Fit	Acceptable Baseline
CFI	**0.96**	**Accept**	≥0.90
AGFI	**0.89**	**Accept**	≥0.80
RMSEA	**0.031**	**Accept**	≤0.08
CMIN/df	**1.20**	**Accept**	≤3
TLI	**0.94**	**Accept**	≥0.90
IFI	**0.96**	**Accept**	≥0.90

Model Testing:

Following the completion of confirmatory factor analysis, an assessment was conducted to evaluate the construct's validity and reliability. Following the completion of data cleaning and the assessment of data reliability and validity, the researcher proceeded to conduct structural equation modelling using AMOS to analyse the proposed model. The results obtained from the analysis are presented below.

Direct and Indirect Hypothesis

The examination of different Information Security Controls (IV) and their influence on Incident Response Time (Med1), Cyberattack Incidents (DV1), and Customer Trust (DV2) yields significant findings. To begin with, it can be observed that there is a positive correlation between Encryption Strength (IV1) and incident response time (Med1). This is supported by a coefficient of 0.029 and a statistically significant value of 2.33. This implies that as the level of encryption increases, there is a corresponding improvement in incident response time, which has the potential to enhance an organisation's capability to effectively manage and mitigate security incidents. On the

Electronic copy available at: https://ssrn.com/abstract=4626041

other hand, there is an inverse relationship between Encryption Strength (IV1) and cyberattack incidents (DV1), as evidenced by a coefficient of 1.24 and a significance level of 1.22. This suggests that an increase in encryption strength is associated with a decrease in the occurrence of cyberattack incidents.

The study reveals that there is a positive correlation between Firewall Configuration (IV2) and incident response time (Med1), as evidenced by a coefficient of 0.034 and a significance level of 3.01. A properly configured firewall is correlated with expedited incident response durations. The study found that there is a negative relationship between Firewall Configuration (IV2) and cyberattack incidents (DV1), as indicated by a coefficient of 1.01 and a significance level of 1.64. These results suggest that implementing stringent firewall configurations may result in a reduction in cyberattack incidents.

The relationship between Authentication Protocols (IV3) and incident response time (Med1) demonstrates a statistically significant positive correlation, as indicated by a coefficient of 0.014 and a significance level of 4.66. Enhancements in authentication protocols have been found to positively impact the efficiency of incident response processes, resulting in faster resolution times. On the contrary, the implementation of Authentication Protocols (IV3) exhibits a negative correlation with cyberattack incidents (DV1), as evidenced by a coefficient of 0.029 and a significance level of 3.69. These findings suggest that the use of enhanced authentication protocols has the potential to mitigate the occurrence of cyberattacks.

The study found a positive correlation between Security Training (IV4) and incident response time (Med1), with a coefficient of 0.021 and a significance level of 4.37. The provision of sufficient security training has a positive effect on the promptness and effectiveness of incident response. Additionally, the impact of Security Training (IV4) on cyberattack incidents (DV1) is found to be negative, as indicated by a coefficient of 0.014 and a significance level of 3.33. This highlights the importance of training in reducing cyber risks.

The variable of Encryption Strength (IV1) exhibits a negative influence on Customer Trust (DV2), as indicated by a coefficient of 0.97 and a significance level of 1.80. This negative impact is observed despite the positive effect it has on incident response time. This suggests that the implementation of stronger encryption may not necessarily result in an increase in customer trust. The negative influence of Firewall Configuration (IV2) on customer trust (DV2) is observed, with a coefficient of 0.68 and a significance level of 1.24. In contrast, the impact of Authentication Protocols (IV3) and Security Training (IV4) on customer trust (DV2) is found to be positive. This suggests that the implementation of strong authentication protocols and the provision of effective security training have a beneficial effect on the establishment and sustenance of customer trust. The coefficients associated with these factors are 0.021 (significance level: 4.69) and 0.015 (significance level: 4.09), respectively.

Electronic copy available at: https://ssrn.com/abstract=4626041

Table 6. Summary of Effects

Variables	Direct Effects	Indirect Effects	Total Effects
Encryption strength → incident response time (Med1).	0.324		0.324
Firewall configuration →incident response time (Med1).	0.246		0.246
Authentication protocols (IV3→ incident response time (Med1).	0.461		0.461
Security training (IV4) →incident response time (Med1).	0.401		0.401
Encryption strength (IV1) → cyber-attack incidents (DV1).	0.246	0.358	0.604
Firewall configuration (IV2) → cyber-attack incidents (DV1).	0.214	0.487	0.701
Authentication protocols (IV3) → cyber-attack incidents (DV1).	0.200	0.401	0.601
Security training (IV4) → cyber-attack incidents (DV1).	0.106	0.341	0.447
Encryption strength (IV1) → customer trust (DV2).	0.169	0.299	0.468
Firewall configuration (IV2) →customer trust (DV2).	0.277	0.487	0.764
Authentication protocols (IV3) → customer trust (DV2).	0.197	0.540	0.737
Security training (IV4) →customer trust (DV2).	0.235	0.533	0.768

Table 7 below provides the summary of the acceptance/rejection status of all the hypotheses of the study in accordance with the results presented in Table 7 above.

Table 7. Result of Analyses and Hypotheses

Hypotheses		P-value	t-value	Accept or Reject
H1	Encryption strength (IV1) positively affects incident response time (Med1).	0.029	2.33	**Accept**
H2	Firewall configuration (IV2) positively affects incident response time (Med1).	0.034	3.01	**Accept**
H3	Authentication protocols (IV3) positively affect incident response time (Med1).	0.014	4.66	**Accept**
H4	Security training (IV4) positively affects incident response time (Med1).	0.021	4.37	**Accept**
H5	Encryption strength (IV1) negatively affects cyberattack incidents (DV1).	1.24	1.22	**Reject**
H6	Firewall configuration (IV2) negatively affects cyberattack incidents (DV1).	1.01	1.64	**Reject**
H7	Authentication protocols (IV3) negatively affect cyberattack incidents (DV1).	0.029	3.69	**Accept**
H8	Security training (IV4) negatively affects cyberattack incidents (DV1).	0.014	3.33	**Accept**
H9	Encryption strength (IV1) positively affects customer trust (DV2).	0.97	1.80	**Reject**
H10	Firewall configuration (IV2) positively affects customer trust (DV2).	0.68	1.24	**Reject**
H11	Authentication protocols (IV3) positively affect customer trust (DV2).	0.021	4.69	**Accept**
H12	Security training (IV4) positively affects customer trust (DV2).	0.015	4.09	**Accept**

p-value <0.05 (Hair, Money, Samouel, & Page, 2007), t-value > 1.96 (Bhatti & Sundram Kaiani, 2015)

Electronic copy available at: https://ssrn.com/abstract=4626041

DISCUSSION

Based on the findings of the study, the independent variable of Encryption Strength was examined to determine its impact on Incident Response Time, yielding positive results. This observation implies that the implementation of more robust encryption measures has a beneficial impact on the speed at which incidents are addressed and resolved. This suggests that there is a negative correlation between the level of encryption strength and the response time to incidents. One potential explanation for this phenomenon is that the implementation of robust encryption measures may enhance the overall resilience and security of a system. Consequently, this can facilitate the prompt detection and effective resolution of security incidents.

According to the preliminary investigation, the implementation of an ES appears to have a detrimental impact on the occurrence of cyberattack incidents. Nevertheless, the hypothesis positing that increased encryption has a detrimental impact on cyberattack occurrences is refuted. This observation is intriguing and suggests that although encryption plays a crucial role in incident response, its efficacy in preventing cyber-attacks entirely may be limited. The preliminary findings provide evidence that the ES has a detrimental impact on Customer Trust. The hypothesis asserting a positive correlation between stronger encryption and customer trust is deemed invalid. The counterintuitive nature of this outcome arises from the expectation that stronger encryption would bolster customer trust through the safeguarding of data confidentiality and integrity. Additional investigation is required in order to gain a more comprehensive understanding of this association.

In response to the findings of the pilot study, it has been observed that Firewall Configuration has a positive impact on Incident Response Time. The hypothesis regarding the positive impact of firewall configuration on incident response time has been accepted. The implementation of a properly configured firewall can effectively detect and thwart unauthorised access, thereby enhancing the efficiency of incident response protocols. However, it is important to note that Firewall Configuration can have a detrimental impact on the occurrence of cyberattack Incidents. The hypothesis positing a negative relationship between firewall configuration and cyberattack incidents is found to be unsupported. This discovery implies that although firewalls can assist in incident response, their effectiveness in preventing cyberattacks may be limited. However, it should be noted that FC (fake content) has a detrimental impact on the level of trust that customers place in a given entity. The hypothesis positing a positive relationship between firewall configuration and customer trust has been refuted. This finding suggests that customers may not necessarily link firewall configuration directly to trust, or there may be other influential factors that have a greater impact on customer perceptions.

Electronic copy available at: https://ssrn.com/abstract=4626041

Likewise, in the initial investigation, it can be inferred that the implementation of Authentication Protocols has a favourable impact on the duration of Incident Response Time. The hypothesis asserting that authentication protocols have a positive impact on incident response time is deemed valid. The implementation of robust authentication mechanisms facilitates the prompt detection and mitigation of security incidents pertaining to unauthorised access. On the contrary, the utilisation of applications (APs) has been found to have a detrimental impact on the occurrence of cyberattack incidents. The hypothesis positing a negative correlation between authentication protocols and cyberattack incidents has been accepted. This implies that robust authentication measures have the potential to serve as a deterrent or obstacle against cyberattacks. Contrarily, the positive impact of Aps on Customer Trust. The hypothesis positing a positive relationship between authentication protocols and customer trust has been accepted. The implementation of robust authentication measures can engender a sense of confidence among customers with regards to the security of their accounts and data, thus making it an intuitive approach.

According to the results obtained from the aforementioned study, it has been determined that Security Training has a beneficial impact on the duration of Incident Response Time. The hypothesis positing a positive correlation between security training and incident response time has been accepted. Professionals who have received comprehensive training are more inclined to exhibit a higher level of effectiveness when it comes to addressing security incidents. On the contrary, Security Technology (ST) has a detrimental impact on the occurrence of cyberattack incidents. The hypothesis positing a negative relationship between security training and cyberattack incidents is supported. This statement underscores the significance of education and awareness in mitigating the probability of successful cyberattacks. On the other hand, it can be observed that ST has a favourable impact on the establishment of Customer Trust. The hypothesis positing a positive relationship between security training and customer trust is deemed valid. This observation underscores the notion that customers are more likely to place trust in organisations when they possess a high level of confidence in the security awareness and competence of the personnel responsible for handling their information.

Theoretical Implications and Practical Implications

The implementation of robust encryption, firewalls, and authentication protocols enhances the capacity to promptly identify and address cyber threats, thereby mitigating the potential harm that may be incurred. The implementation of robust security measures serves as a deterrent, thereby reducing the occurrence and effectiveness of cyber-attacks on e-commerce platforms. The implementation of robust cybersecurity protocols not only safeguards confidential information but also fosters customer confidence, thereby enhancing the e-commerce platform's reputation. There are strict

Electronic copy available at: https://ssrn.com/abstract=4626041

regulations governing the protection of data in many different geographical areas. The implementation of cybersecurity measures serves to guarantee adherence to regulatory requirements and mitigate potential legal ramifications. This study provides empirical evidence that supports the theoretical frameworks that propose a positive correlation between encryption, firewall configuration, authentication protocols, and the effectiveness of incident response.

The inverse relationship between encryption strength and cyberattack incidents supports the deterrence theory by showing that strong security measures have the ability to deter potential attackers. The positive effects of implementing cybersecurity measures on customer trust are consistent with theoretical frameworks that propose a direct relationship between perceived security and user trust in online platforms. The incorporation of security training underscores the theoretical significance of providing personnel with education to mitigate cyber threats, thereby emphasising the role of human factors in the realm of cybersecurity.

Limitations and Future Research Directions

Limitations:

The findings of this study imply that contextual factors, such as the unique circumstances and size of the operations, can affect the effectiveness of cybersecurity measures in e-commerce operations. The rapid pace of technological advancements has the potential to render certain research findings obsolete as cyber threats and corresponding protective measures continuously evolve. The study may not comprehensively consider unforeseeable human behaviours that could potentially influence the effectiveness of security measures, such as password management or vulnerability to social engineering. The implementation of robust cybersecurity measures may pose challenges for small or resource-constrained e-commerce platforms, thereby impacting the generalizability of the research findings.

Future Research Directions:

This study intends to explore adaptive security models that possess the capability to dynamically adapt and respond to emerging cyber threats, taking into account the rapid evolution of technology. Examine the incorporation of security measures that prioritise the needs and preferences of users, recognising the significant involvement of end-users in both the prevention of cyber-attacks and the response to security incidents. This analysis aims to evaluate the economic consequences associated with the adoption of comprehensive cybersecurity measures, taking into account the cost-effectiveness and advantages for e-commerce platforms of different scales. This study aims to conduct comparative analyses across various industries in order to determine whether the efficacy of cybersecurity measures differs between the e-commerce sector and other

Electronic copy available at: https://ssrn.com/abstract=4626041

sectors. The integration of behavioural studies into the analysis of user responses to security measures offers valuable insights for the development of user-friendly and efficient cyber security protocols**.**

Acknowledgment: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant 4587]

REFERENCES

Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results in Control and Optimization, 12*, 100268. doi: https://doi.org/10.1016/j.rico.2023.100268

AL-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. *International Journal of Advanced Computer Science and Applications, 14* (2), 2023. doi: http://dx.doi.org/10.14569/IJACSA.2023.0140292

Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M., & Musa, A. (2018). Understanding awareness of cyber security threat among IT employees. In *2018 6th international conference on future internet of things and cloud workshops (ficloudw)* (pp. 188-192). IEEE. doi: https://doi.org/10.1109/W-FiCloud.2018.00036

Alatawi, M. N., Alsubaie, N., Ullah Khan, H., Sadad, T., Alwageed, H. S., Ali, S., & Zada, I. (2023). Cyber security against intrusion detection using ensemble-based approaches. *Security and Communication Networks, 2023*. doi: https://doi.org/10.1155/2023/8048311

Alswiay, S., & Cagiltay, N. E. (2018). Trust Factors Affecting B2C E-Commerce. In *Türkiye Bilişim Derneği, 34. Bilişim Kurultayı Bildiriler Kitabı* (pp. 133-138). Retrieved from https://ceur-ws.org/Vol-2045/27_Bilisim_2017_paper_20.pdf

Apau, R., & Koranteng, F. N. (2019). Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior. *International Journal of Cyber Criminology, 13*(2), 228-254. doi: http://dx.doi.org/10.5281/zenodo.3697886

Arjmandi, P., Boeck, R., Raja, F., & Viswanathan, G. (2007). Usability of windows vista firewall: a laboratory user study. *EECE 412 Term Paper*. Retrieved from https://courses.ece.ubc.ca/cpen442/term_project/reports/2007-fall/Usability_of_Windows_Vista_Firewall--A_Laboratory_User_Study.pdf

Ashok, K., & Gopikrishnan, S. (2023). Statistical analysis of remote health monitoring based iot security models & deployments from a pragmatic perspective. *IEEE Access, 11*, 2621-2651. doi: https://doi.org/10.1109/ACCESS.2023.3234632

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), 1333. doi: https://doi.org/10.3390/electronics12061333

Electronic copy available at: https://ssrn.com/abstract=4626041

Bansal, A., Khosla, T., & Saini, V. K. (2023). Security challenges and various methods for increasing security in e-commerce applications. *International Journal for Research in Applied Science and Engineering Technology*.

Basuki, A., & Adriansyah, A. (2023). Response time optimization for vulnerability management system by combining the benchmarking and scenario planning models. *International Journal of Electrical & Computer Engineering (2088-8708), 13*(1). doi: https://doi.org/10.11591/ijece.v13i1.pp561-570

Bennett, K. W., & Robertson, J. (2023). Cyberspace exercises: defending against malicious cyber actors. *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications V, 12538*, 57-72. doi: https://doi.org/10.1117/12.2663514

Bhatia, N. L., Shukla, V. K., Punhani, R., & Dubey, S. K. (2021). Growing aspects of cyber security in e-commerce. In *2021 International Conference on Communication information and Computing Technology (ICCICT)* (pp. 1-6). IEEE. doi: https://doi.org/10.1109/ICCICT50803.2021.9510152

Bhatti, M. A., & Sundram Kaiani, V. P. (2015). *Business research: quantitative and qualitative methods* (1st ed.). Pearson Singapore.

Blancaflor, E. B., Competente, L. A. M., Fallar, J. D., Magadan, N. F. J., Piopongco, K. J. R., & Salinas, L. N. L. (2023). A Case Study of using Cryptography for the Improvement of Data Security in E-commerce Industry in the Philippines. In *2023 8th International Conference on Computer and Communication Systems (ICCCS)* (pp. 695-700). IEEE. doi: https://doi.org/10.1109/ICCCS57501.2023.10150939

Bringhenti, D., Marchetto, G., Sisto, R., Valenza, F., & Yusupov, J. (2022). Automated firewall configuration in virtual networks. *IEEE Transactions on Dependable and Secure Computing, 20*(2), 1559-1576. doi: https://doi.org/10.1109/TDSC.2022.3160293

Byrne, B. M. (2013). *Structural equation modeling with Mplus: Basic concepts, applications, and programming*. Routledge. doi: https://doi.org/10.4324/9780203807644

Chaturvedi, A. (2022). Comparison of different authentication techniques and steps to implement robust JWT authentication. In *2022 7th International Conference on Communication and Electronics Systems (ICCES)* (pp. 772-779). IEEE. doi: https://doi.org/10.1109/ICCES54183.2022.9835796

Chaudhuri, A. (2023). Network forensics and incident response. *International Journal of Scientific and Research Publications, 13*(5). doi: http://dx.doi.org/10.29322/IJSRP.13.05.2023.p13702

Coles, G. M., & Smart, W. J. (2011). Building trust in online customers. In *12th ACIS International Conference on Software Engineering Artificial Intelligence, Networking and Parallel/Distributed Computing* (pp. 93-98). Los Alamitos, Calif.: IEEE Computer Society. doi: https://doi.org/10.1109/SNPD.2011.31

Dimitriadis, C. (2023). Consumer trust and perspectives on cyber security. *Computer Fraud & Security, 2023*(5). doi: https://doi.org/10.12968/S1361-3723(23)70020-1

Guest, J. L., Adam, E., Lucas, I. L., Chandler, C. J., Filipowicz, R., Luisi, N., et al. (2021). Methods for authenticating participants in fully Web-based mobile app trials from the iReach project: cross-sectional study. *JMIR mHealth and uHealth, 9*(8), e28232. doi: https://doi.org/10.2196/28232

Electronic copy available at: https://ssrn.com/abstract=4626041

Hair, J. F., Money, A. H., Samouel, P., & Page, M. (2007). Research methods for business. *Education+ Training, 49*(4), 336-337. doi: https://doi.org/10.1108/et.2007.49.4.336.2

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European business review, 31*(1), 2-24. doi: https://doi.org/10.1108/EBR-11-2018-0203

Harshavardan, K., & PadmaShani, R. (2023). Secure practices to prevent cyber attacks in e-commerce sites. In *2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS)* (pp. 665-670). IEEE. doi: https://doi.org/10.1109/ICISCoIS56541.2023.10100357

Jamra, R. K., Anggorojati, B., Sensuse, D. I., & Suryono, R. R. (2020). Systematic review of issues and solutions for security in e-commerce. In *2020 International Conference on Electrical Engineering and Informatics (ICELTICs)* (pp. 1-5). IEEE. doi: https://doi.org/10.1109/ICELTICs50595.2020.9315437

Kanaan, A., AL-Hawamleh, A., Abulfaraj, A., Al-Kaseasbeh, H., & Alorfi, A. (2023). The effect of quality, security and privacy factors on trust and intention to use e-government services. *International Journal of Data and Network Science, 7*(1), 185-198. doi: http://dx.doi.org/10.5267/j.ijdns.2022.11.004

Kim, E., & Kyung, Y. (2023). Factors affecting the adoption intention of new electronic authentication services: A convergent model approach of VAM, PMT, and TPB. *IEEE Access, 11*, 13859-13876. doi: https://doi.org/10.1109/ACCESS.2023.3243183

Li, L. (2023). Data security technology in electronic commerce system development. In *2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC)* (pp. 1-6). IEEE. doi: https://doi.org/10.1109/ICAISC58445.2023.10200851

Line, M. B., Albrechtsen, E., Johnsen, S. O., Longva, O. H., & Hillen, S. (2006). Monitoring of incident response management performance. *IT-Incident Management & IT-Forensics-IMF 2006*. Retrieved from https://sintef.no/en/publications/publication/1386961

Liu, C., & Mackie, B. G. (2004). Developing security for e-commerce applications: A teaching case. *Communications of the IIMA, 4*(2), 4. doi: https://doi.org/10.58729/1941-6687.1243

Mitra, D., Kulkarni, P., Pathak, P., & Natrai, N. (2022). Importance of coping with cyber security challenges in e commerce business. In *2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC)* (pp. 1596-1601). IEEE. doi: https://doi.org/10.1109/IIHC55949.2022.10059851

Natheniel, O. E., Grace, E., Ifeanyi, A. A., Oluwatomi, A. K., & Ali, O. A. (2017). Customers influx, awareness and security management in E-Commerce. *Scholars Journal of Engineering and Technology (SJET), 5*(10), 513-523. doi: https://doi.org/10.36347/sjet.2017.v05i10.001

Nicholson, J., & McGlasson, J. (2020). CyberGuardians: improving community cyber resilience through embedded peer-to-peer support. In *Companion Publication of the 2020 ACM designing interactive systems conference* (pp. 117-121). ACM. doi: https://doi.org/10.1145/3393914.3395871

Electronic copy available at: https://ssrn.com/abstract=4626041

Nocera, S., Romano, S., Francese, R., & Scanniello, G. (2023). Training for security: planning the use of a SAT in the development pipeline of web Apps. In *2023 IEEE/ACM 45th International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET)* (pp. 40-45). IEEE. doi: https://doi.org/10.1109/ICSE-SEET58685.2023.00010

Oruj, Z. (2023). Cyber Security: contemporary cyber threats and national strategies. *Distance Education in Ukraine: Innovative, Normative-Legal, Pedagogical Aspects*, (2), 100-116. doi: https://doi.org/10.18372/2786-5495.1.17309

Özkan, B. E., & Tolga, İ. B. (2023). Zero-day operational cyber readiness. In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (pp. 199-215). IEEE. doi: https://doi.org/10.23919/CyCon58705.2023.10181814

Pagey, R., Mannan, M., & Youssef, A. (2023). All your shops are belong to us: security weaknesses in e-commerce platforms. In *Proceedings of the ACM Web Conference 2023* (pp. 2144-2154). ACM. doi: https://doi.org/10.1145/3543507.3583319

Panja, A., Mondal, S., Islam, K. A., Ghosh, T. K., & Karforma, S. (2022). an efficient and secure fingerprint based authentication scheme using elliptic curve cryptography. *Webology, 19*(2). Retrieved from https://www.webology.org/data-cms/articles/20220208125715pmwebology%2019%20(2)%20-%20152.pdf

Petcu, A., Pahontu, B., Frunzete, M., & Stoichescu, D. A. (2023). A secure and decentralized authentication mechanism based on web 3.0 and ethereum blockchain technology. *Applied Sciences, 13*(4), 2231. doi: https://doi.org/10.3390/app13042231

Purwanto, A. (2021). Partial least squares structural squation modeling (PLS-SEM) analysis for social and management research: a literature review. *Journal of Industrial Engineering & Management Research*. Retrieved from https://ssrn.com/abstract=3982764

Qasaimeh, M., Halemah, N. A., Rawashdeh, R., Al-Qassas, R. S., & Qusef, A. (2022). Systematic review of e-commerce security issues and customer satisfaction impact. In *2022 International Conference on Engineering & MIS (ICEMIS)* (pp. 1-8). IEEE. doi: https://doi.org/10.1109/ICEMIS56295.2022.9914393

Sadab, M., Mohammadian, M., & Ullah, A. B. (2023). Key factors related to cyber security affecting consumer attitude in online shopping: A study in Bangladesh. In *2023 6th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-4). IEEE. doi: https://doi.org/10.1109/ISCON57294.2023.10112129

Saeed, S. (2023). A customer-centric view of E-commerce security and privacy. *Applied Sciences, 13*(2), 1020. doi: https://doi.org/10.3390/app13021020

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15*(18), 13369. doi: https://doi.org/10.3390/su151813369

Sagoo, J. (2022). The state-of-the-art in authentication. *Biometric Technology Today, 2022*(1). doi: https://doi.org/10.12968/S0969-4765(22)70001-X

Salih, A. A., & Abdulrazzaq, M. B. (2023). Cyber security: performance analysis and challenges for cyber attacks detection. *Indonesian Journal of Electrical Engineering and Computer Science, 31*(3), 1763-1775. doi: http://dx.doi.org/10.11591/ijeecs.v31.i3.pp1763-1775

Electronic copy available at: https://ssrn.com/abstract=4626041

Setyadi, R., Rahman, A., & Subiyakto, A. (2019). Statistical and interpretative analyses for testing customer trust questionnaires on IT governance. *IOP Conference Series: Materials Science and Engineering, 662*(2), 022094. doi: https://doi.org/10.1088/1757-899X/662/2/022094

Shaikh, J. R., Beniwal, R., & Iliev, G. (2019). Cryptography and optimization-driven support vector neural network to mitigate DoS attacks in E-commerce. In *Applications of Computing, Automation and Wireless Systems in Electrical Engineering: Proceedings of MARC 2018* (pp. 551-561). Springer. doi: https://doi.org/10.1007/978-981-13-6772-4_48

Shen, H., Wu, G., Xia, Z., Susilo, W., & Zhang, M. (2023). A privacy-preserving and verifiable statistical analysis scheme for an e-commerce platform. *IEEE Transactions on Information Forensics and Security*. doi: https://doi.org/10.1109/TIFS.2023.3269669

Shin, J., Carley, L. R., Dobson, G. B., & Carley, K. M. (2023). Modeling and simulation of the human firewall against phishing attacks in small and medium-sized businesses. In *2023 Annual Modeling and Simulation Conference (ANNSIM)* (pp. 369-380). IEEE. Retrieved from https://ieeexplore.ieee.org/abstract/document/10155371

Su, J., & Manchala, D. W. (1999). Trust vs. threats: recovery and survival in electronic commerce. In *Proceedings. 19th IEEE International Conference on Distributed Computing Systems (Cat. No. 99CB37003)* (pp. 126-133). IEEE. doi: https://doi.org/10.1109/ICDCS.1999.776513

Surya, S., Jagtap, S. R., Ramnarayan, R., Priyadarshini, M., Ibrahim, R. K., & Alazzam, M. B. (2023). Protecting online transactions: A cybersecurity solution model. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 2630-2634). IEEE. doi: https://doi.org/10.1109/ICACITE57410.2023.10183282

Thakur, G., Kumar, P., Jangirala, S., Das, A. K., & Park, Y. (2023). An effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environment. *IEEE Access, 11*, 26877-26892. doi: https://doi.org/10.1109/ACCESS.2023.3249116

Treese, W. (2000). Putting it together: data collection and consumer privacy. *Networker, 4*(4), 9-11. Retrieved from https://dl.acm.org/doi/fullHtml/10.1145/354573.354577

Walter, M., Hahner, S., Bureš, T., Hnětynka, P., Heinrich, R., & Reussner, R. (2023). Architecture-based attack propagation and variation analysis for identifying confidentiality issues in Industry 4.0. *at-Automatisierungstechnik, 71*(6), 443-452. doi: https://doi.org/10.1515/auto-2022-0135

Wang, B., Chen, W., Pei, H., Xie, C., Kang, M., Zhang, C., et al. (2023). DecodingTrust: A comprehensive assessment of trustworthiness in GPT models. *arXiv preprint arXiv:2306.11698*. doi: https://doi.org/10.48550/arXiv.2306.11698

Wang, S. (2021). Study on the Application of Computer Security Technology in E-commerce. *Journal of Physics: Conference Series, 1915*(4), 042044. doi: https://doi.org/10.1088/1742-6596/1915/4/042044

Wen, J. (2023). A layered encryption model PABB based on user privacy in E-commerce Platforms. *Frontiers in Business, Economics and Management, 9*(3), 10-14. doi: https://doi.org/10.54097/fbem.v9i3.9428

Electronic copy available at: https://ssrn.com/abstract=4626041

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication, 800*(50), 1-39. Retrieved from https://profsite.um.ac.ir/kashmiri/nist/new/NIST-SP800-50.pdf

Woods, D. W., Böhme, R., Wolff, J., & Schwarcz, D. (2023). Lessons lost: Incident response in the age of cyber insurance and breach attorneys. In *Proceedings of the 32nd USENIX Security Symposium, Anaheim, California* (pp. 2259-2273). USENIX Association. Retrieved from https://www.usenix.org/conference/usenixsecurity23/presentation/woods

Electronic copy available at: https://ssrn.com/abstract=4626041