INTERNATIONAL JOURNAL OF eBUSINESS AND eGOVERNMENT STUDIES
Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220
Received: 13.08.2023| **Accepted:** 30.10.2023 | **Published Online:** 05.12.2023

-RESEARCH ARTICLE-

E-BUSINESS PERFORMANCE AND CYBER SECURITY MEASURES: MEDIATING ROLE OF EMPLOYEE CYBERSECURITY BEHAVIOUR AND TECHNOLOGICAL SOPHISTICATION

Abdullah Faisal Al Naim

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

Kwong Wing Chong

School of Professional Studies, Taylor's College, Taylor's Lakeside Campus, No. 1 Jalan Taylor's, 47500 Subang Jaya, Selangor, Malaysia.
Email: wingchong.kwong@taylors.edu.my

─Abstract─

The primary aim of this research is to investigate the interplay among organizational cybersecurity measures, employee behaviour, technological proficiency, and E-business performance. This study, which takes a quantitative research method, examines how employee behaviour and technological proficiency mediate the impact of organisational cybersecurity measures on the performance of e-businesses. A survey was used to gather data from a variety of companies, and Amos was used in structural equation modelling (SEM) to evaluate the intricate correlations between the important factors. Ensuring the robustness and trustworthiness of the findings through methodological rigour allows for a thorough investigation of the study objectives. The empirical results of the study corroborate the moderating impacts of employee cybersecurity behaviour and the profile of technological sophistication in transforming organisational cybersecurity strategies into measurable outcomes for e-business success. Every hypothesis that has been put forth has been proven true, which emphasises how important it is to foster a culture that understands cybersecurity, align technology spending with organisational needs, and ensure that cutting-edge infrastructure supports policies and guidance from upper management. To summarise, this study provides valuable insights into the intricate connections between

Citation (APA): Al Naim, A. F., Chong, K. W. (2023). E-Business Performance and Cyber Security Measures: Mediating Role of Employee Cybersecurity Behaviour and Technological Sophistication. *International Journal of eBusiness and eGovernment Studies, 15*(2), 373-397. doi: 10.34109/ijebeg.2023150220

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

organisational cybersecurity procedures and electronic business activities. This study shows how important it is for businesses to have tech-savvy employees and good staff behaviour when it comes to improving their safety in this digital age. It backs up the idea that how employees act and how well they know how to use technology are very important to the success of an organization's safety and e-business. By presenting evidence-based insights, the study enriches current understanding and provides a nuanced comprehension of the complex dynamics in the digital age.

Keywords: E-business Performance, Employee Cybersecurity Behaviour, Technological Sophistication, Technological Investments, Information Security, Digital Resilience.

INTRODUCTION

An e-business's efficacy transcends mere aesthetics and promotional slogans. Rather, it hinges upon a nuanced examination of the intricate nexus among technology, clientele, and operational metrics, where each user interaction encapsulates a narrative. Satisfaction arises from a seamless online transaction, excitement from discovering a hidden gem amid thoughtfully curated recommendations, and confidence from receiving timely, personalized emails. Primarily, the rapid evolution of technology has been instrumental in augmenting the overall effectiveness and functionality of e-commerce platforms. This encompasses the widespread integration of machine learning, artificial intelligence, and data analytics, empowering businesses to deliver tailored customer experiences and execute data-driven decisions (Policarpo et al., 2021). Moreover, the accessibility of the internet and heightened global interconnectivity have broadened the scope of e-businesses, enabling them to enter new markets and interact with a more diverse clientele (Chen et al., 2020). The advancement of e-business has been further facilitated by the proliferation of mobile technology and the escalating adoption of smartphones, which facilitate streamlined transactions and interactions even in mobile settings (Mthembu et al., 2018) Moreover, the onset of the COVID-19 pandemic in 2019 accelerated the adoption of digital technologies by businesses and underscored the significance of proficient e-business strategies. Mandated lockdowns and social distancing measures precipitated a notable surge in online engagement, prompting businesses to embrace advanced e-commerce methodologies and enhance their digital footprint (Naab & Bans-Akutey, 2021). Yet, the rise of e-business has brought forth fresh challenges, including the requirement for regulatory frameworks to oversee e-business operations and contend with cybersecurity risks (Liu et al., 2022).

The study conducted by Waseem et al. (2019) shows a strong link between employees' awareness of cybersecurity and the overall security status of electronic businesses. Comprehensive training and awareness programs enable staff to identify and address potential risks, thereby enhancing the overall resilience of e-business systems. Furthermore, since cyber threats are constantly evolving, businesses must continually adapt their strategies.

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

The COVID-19 epidemic has accelerated the use of remote work while posing new difficulties. The study by Makarius et al. (2020) emphasises how crucial it is to incorporate cybersecurity concerns into laws pertaining to remote work. It emphasises employees' active participation in upholding a safe virtual environment. When it comes to e-business, which is defined by a high volume of digital transactions and data sharing, employee duties go beyond internal system security. A person's cybersecurity policies have a direct impact on the level of confidence that customers place in an online business, and building consumer trust is essential for success in electronic commerce. Research by Jibril et al. (2020) and Xu and Mahenthiran (2021) examine the relationship between e-business performance, consumer perception, and cybersecurity practices. Companies that place a high priority on employee cybersecurity behaviour and effectively manage it tend to build a reputation for reliability and security, which in turn attracts repeat business and increases overall business efficiency. However, there are a lot of obstacles in managing the relationship between employee cybersecurity behaviour and e-business effectiveness. Organisations need to implement a thorough strategy because of the rapid advancement of technology and the complexity of cyber threats. It is critical that cybersecurity plans match organisational objectives. The research done by Lee (2022) emphasises how important it is for companies to acknowledge cybersecurity as a crucial part of their overall business plan, paying special attention to employee behaviour.

This study examines the relationship between organisational cybersecurity measures and E-business performance, with a particular emphasis on the mediating roles of staff cybersecurity behaviour and technological competency. The study's three main goals are to find out how organisational cybersecurity culture, technology investment, rules, and support from senior management are related to e-business success; to find out how employee cybersecurity behaviour affects organisational cybersecurity and e-business success; and to find out how technological complexity affects the connection between cybersecurity and e-business performance. It helps you understand the ideas better and gives useful tips for the e-business and safety fields.

This question is about the growing dangers that cybercriminals pose to e-businesses and the need for strong security measures. This study looks at something that hasn't been looked into as much: how rules, organisational culture, backing from upper management, and technical investments affect the performance of e-business. To lower cyber risks and make digital processes better, it's important to know how employees behave online and how much they know about technology. The study gives e-businesses useful information on how to deal with the changing world of safety.

LITERATURE REVIEW AND HYPOTHESIS

Building organisational resilience and reducing cyber threats require a strong

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

cybersecurity culture that is defined by efforts that encourage accountability, employee involvement, and leadership support (De Silva, 2023). The overall organisational culture is shaped by organisational characteristics that have an impact on employee cybersecurity behaviour, such as leadership abilities and clearly stated cultural values (Onumo et al., 2021). The relationship between e-business performance and corporate cybersecurity culture is contingent upon employee cybersecurity behaviour, influenced by factors such as security technology, knowledge, and cognitive beliefs. Additionally, gender differences may serve as moderators for the factors affecting attitudes and behaviours concerning cybersecurity (Anwar et al., 2017). In order to optimize e-business performance, organizations ought to prioritize the establishment of a resilient cybersecurity culture while also addressing gender disparities in cybersecurity practices. Effective cybersecurity hinges on the collective embrace of cybersecurity principles and practices within an organization, commonly termed as organizational cybersecurity culture. Gerber et al.'s (2019) research underscores the imperative of fostering a cybersecurity culture that incentivizes employees to prioritize security in their daily tasks. The organizational culture profoundly shapes employees' cybersecurity behaviour and fortifies the overall cybersecurity posture.

H1: *Employee cyber security behaviour mediates the relationship between organizational cybersecurity culture and E-business performance.*

The effectiveness of a firm's cybersecurity infrastructure correlates directly with its investment in cybersecurity technology resources. Implementation of cutting-edge technologies, including intrusion detection systems, firewalls, and encryption tools, holds the potential to substantially bolster the cybersecurity defences of an organization. However, the attitudes and cybersecurity culture prevalent among employees within the company are pivotal determinants of the efficacy of these technologies. Inadequate training or negligent employee behaviours have the capacity to nullify the benefits of even the most sophisticated cybersecurity measures. Several research works have explored the various elements that influence the connection between technology use and organisational effectiveness. Al-Ayed and Al-Tit (2024) discusses about how digitalized customer relationship management (CRM) can help improve performance when digitalized customers behave in a certain way. Nuryanto et al. (2024) contends that organisational innovation acts as a bridge between how employees act and how they use Big Data and IoT technologies. Almarashdah (2024) shows that company culture has a big effect on how workers are trained and how well they do their jobs. Nguyen et al. (2024) delves into more detail about how views towards e-tax affect how it is used and how useful people think it is. In the past few years, more money has been put into hacking technology, which is important for businesses' security plans. In their study, Chen et al. (2020) explain how cutting-edge technologies like artificial intelligence and machine learning can improve the ability to find and respond to threats. This helps businesses reach their goals by lowering risks and keeping digital systems safe.

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

H2: *Employee cyber security behaviour mediates the relationship between investment in cybersecurity technology and E-business performance.*

Cybersecurity rules spell out what employees should do and how they should use technology to keep sensitive information and systems safe. For policies to be followed and put into action correctly, there needs to be a strong culture around cybersecurity and backing from the top. This makes defences against cyberattacks stronger. Studies by Humaidi and Alghazo (2022) and Sulaiman et al. (2022) explain how the Protection Motivation Theory shapes how employees behave when it comes to hacking. Ruth et al. (2022) addresses the importance of moral behaviour in hacking, and Duzenci et al. (2023) focuses at how different ways of making decisions affect compliance. Li et al. (2022)'s study shows that strong cybersecurity policies are shaped by government laws and industry standards. These policies affect how employees act and how organisations respond to attacks. Support from senior management has a big impact on how well protection policies work.

H3: *Employee cyber security behaviour mediates the relationship between cybersecurity policy stringency and E-business performance.*

It is absolutely necessary to have the backing of top management in order to have a healthy basis for cybersecurity initiatives. CEOs are very important when it comes to getting the whole company behind hacking efforts by helping to pay for solutions and training for employees. If higher authorities don't back up cybersecurity policies with enough resources and attention, they might not work as well as they should. Verkijika (2020) states that psychological control and self-efficacy have a big effect on how people act when it comes to protecting their mobile devices. Sulaiman et al. (2022) clarified the influence of protection motive theory on government employees' cybersecurity behaviour in his study. Meanwhile, Ergen et al. (2021) concluded his research by delineating the barriers and facilitators of safe online behaviour, stressing the importance of adequate education and regulations for promoting safe online practices. According to Alqahtani (2023)'s research, upper management is crucial in allocating resources, cultivating a culture of cybersecurity awareness, and setting priorities for cybersecurity projects. The cultivation of a proactive cybersecurity culture and the alignment of cybersecurity strategies with overarching business objectives necessitate such support.

H4: *Employee cyber security behaviour mediates the relationship between top management support for cybersecurity and E-business performance.*

It is imperative to recognize the reciprocal relationship between e-business performance and cybersecurity. A secure online environment, fostering consumer trust, safeguarding sensitive data, and ensuring uninterrupted operations, positively influences

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

performance. Conversely, the efficacy of e-business operations affects the allocation and prioritization of cybersecurity resources. Thriving e-commerce enterprises often confront escalating cyber risks, necessitating continual enhancement of cybersecurity protocols. The efficacy of e-business operations within the organisation is significantly impacted by the cybersecurity risks that the organisation can properly handle. Many factors, such as the organization's cybersecurity policies, its technology investments, and the strictness of its regulations, affect this outcome. Smith Jr (2022)'s study investigates the tight connection between cybersecurity regulations and e-business performance. Strong cybersecurity policies increase a company's chances of gaining partners and customers, which boosts its online performance. The primary findings of the Miswanto et al. (2024)'s study demonstrate a strong and positive correlation between financial literacy and supply chain management. Both elements have a significant impact on sustainability and financial performance. The study also showed that financial performance has a big impact on sustainability. The study also presents a new correlation model of these factors that is specifically designed for small and medium-sized businesses (SMEs), an area that has not been studied before. According to Khan (2024), there is a positive correlation between SC-Ambidexterity and SC-Resilience, and SC-Agility plays a critical role as an intermediate in this relationship. This emphasises how crucial it is to implement simultaneous and coordinated supply chain capabilities in order to increase resilience and achieve sustainability and long-term prosperity.

H5: *Technological sophistication profile mediates the relationship between organizational cybersecurity culture and E-business performance.*

An organization's technical sophistication profile defines its readiness to integrate and use cutting-edge technologies. There is a clear relationship between having a high degree of technological proficiency and being able to successfully apply cutting-edge cybersecurity solutions. But the effective application of these technologies depends on a number of variables, including the organization's cybersecurity culture, the strictness of the regulations, and senior management's support. Without a firm understanding of these areas, it's possible that the best use of cutting-edge technologies to strengthen cybersecurity defences won't be possible. The relationships between technology and performance are mediated by mindset and performance in marketing, respectively, as highlighted by Nguyen et al. (2024) and Udayana et al. (2023). According to these studies, the relationship between investments in cybersecurity technology and e-business performance may depend on the degree of technological innovation. Similarly, Mbaidin et al. (2024) highlights the significance of management commitment and investment willingness in guaranteeing the success of e-learning and blockchain technology, respectively, both of which are essential for their efficacy. Furthermore, these elements might act as intermediaries in the connection between cybersecurity technology and the operation of e-businesses.

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

According to Krishna and MP (2021) and Huang and Madnick (2019), cybersecurity must be prioritised in order to promote economic success and maximise corporate utilisation. Huang also says that this kind of commitment can unintentionally promote the development of an open digital trading system. These observations are relevant to the inquiry because they shed light on the possible consequences of making investments in cybersecurity technologies for the effectiveness of online business operations. However, Podesva et al. (2021) provides a thorough analysis by examining the investment strategies used to ensure cybersecurity and information security. This analysis facilitates comprehension of the precise mechanisms through which such investments impact the performance of online businesses. Integral to the cybersecurity landscape is the behaviour of employees concerning cybersecurity. This conduct is shaped by multiple factors, encompassing the organizational culture, regulatory rigor, and support provided by senior management. The research conducted by Kumar et al. (2021) underscores the significance of focused training and awareness initiatives in effectively altering employee behaviour. There exists a distinct correlation between the behaviours exhibited by employees and the overall security stance of an organization, consequently impacting the performance of the firm in e-business contexts.

H6: *Technological sophistication profile mediates the relationship between investment in cybersecurity technology and E-business performance.*

The degree of technological complexity acts as a mediator in the connection between the stringency of cybersecurity regulations and the operation of online enterprises. In simple terms, this suggests that the level of technological innovation within the company is the key determinant of how effective stringent cybersecurity measures are in enhancing the performance of electronic commerce. El Khoury et al. (2022) emphasizes the positive influence of cybersecurity capabilities on e-business performance, highlighting the mediating role of e-government maturity. Siddiqui et al. (2013) stresses the importance of standardized security measures in e-business, indicating its significant role in cybersecurity competency. These studies demonstrate that implementing a comprehensive cybersecurity policy with advanced technological measures can improve e-business performance. Kilani (2020) found that factors driving cybersecurity indirectly impact organizational activities, particularly through data expansion and technical control.

Huang and Madnick (2019) demonstrates the way the growth of e-government changes the connection between cybersecurity knowledge and the accessibility of digital trade. Geleta (2018) stresses how important cyber security indicators are for judging success. Several studies show that cybersecurity tactics are very important for keeping digital assets and customer trust safe. Kim and Lee (2021)'s study shows how thorough cybersecurity policies can help prevent security breaches and protect the purity of IT operations. The link between cybersecurity policies and security outcomes is very

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

important for the growth of e-businesses and is still being studied. Liu et al. (2020) finds that businesses that are good with technology use advanced security measures, such as intrusion detection and threat analysis. Dhatt et al. (2017) indicates how technical skills can help balance strict laws and company performance goals by connecting cybersecurity rules to e-commerce measures through new technology.

H7: *Technological sophistication profile mediates the relationship between cybersecurity policy stringency and E-business performance.*

For e-commerce to work, strong cybersecurity measures are needed to keep data safe, keep customers trusting, and keep business running smoothly. Research shows that support from top management is very important for making sure that cybersecurity measures work. This support means that top executives are actively involved in and prioritise cybersecurity activities. Several studies have shown that executive leadership has a big effect on how secure a company is.

Sun et al. (2018) study shows that support from upper management has a big effect on how resources are used, how cybersecurity policies are made, and how secure an organization's culture is overall. It's imperative to recognise that the effectiveness of e-businesses is impacted gradually and intricately by top management support. Evidence highlighting the mediating function of technical sophistication is provided by Chen et al. (2017). The study's conclusions highlight how vital technology advancements are to boosting cybersecurity measures' efficacy. According to their research findings, businesses equipped with advanced technological capabilities demonstrate greater resilience against cyberattacks and encounter fewer disruptions in performance. The degree of technological competence within an organization emerges as a pivotal determinant in establishing a correlation between top management support for cybersecurity and the performance of information technology enterprises.

Given the pivotal role of information technology in distinguishing high-tech firms from their competitors, its importance is paramount in these enterprises (Islam & Stafford, 2017). Geleta (2018) underscores the significant role of cybersecurity measures in assessing e-business performance. Onumo et al. (2021) accentuates that adopting security technology can mitigate the impact of employee cognitive beliefs on cybersecurity compliance, achievable through technology utilization. Nonetheless, the growing utilization of computers and the internet in e-commerce introduces new security vulnerabilities, necessitating the deployment of threat and risk assessments (Pournouri & Craven, 2014).

H8: *Technological sophistication profile mediates the relationship between top management support for cybersecurity and E-business performance.*

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

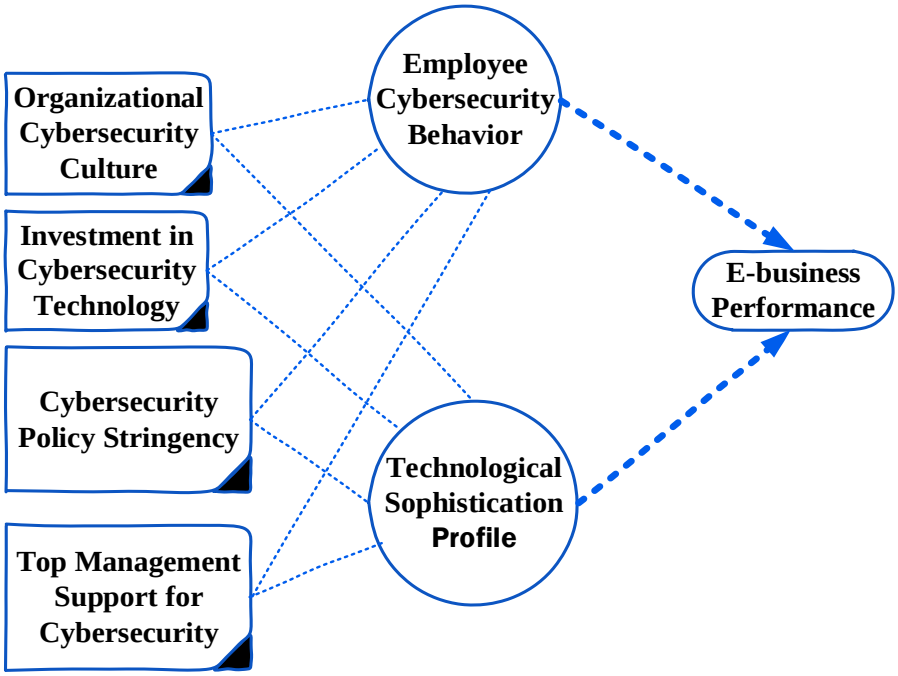

Figure 1: Conceptual Framework.

METHODOLOGY AND DATA SAMPLING

The study administered and scrutinized data obtained from Saudi E-business personnel utilizing two distinct questionnaires. Questionnaire 1 was distributed among 231 employees to gauge Organizational Culture (OCC), Customer Perceived Satisfaction (CPS), Technological and Managerial Support for Change (TMSC), E-Business Capabilities (ECB), and Technological and Social Processes, delving into organizational dynamics and individual perspectives on E-business practices. Questionnaire 2, on the other hand, was circulated among 85 supervisors within the same firms, aimed at eliciting responses concerning ICT and E-business performance. This questionnaire was tailored for supervisors, who hold critical roles in overseeing the organizational implementation of E-business initiatives.

Through purposive sampling, the study ensured that participants actively engaged in Saudi enterprise E-business operations. The surveys were meticulously distributed to secure a representative sample that accurately reflected the job roles and responsibilities within the selected firms. Participants were guaranteed anonymity and encouraged to provide candid, impartial feedback to enhance the credibility of the data.

Factor Loadings Reliability, Convergent Validity

The primary findings of the study are shown in Table 1, along with their factor loadings, convergent validity, and reliability values. The researchers used Cronbach's alpha (), average

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

variance extracted (AVE), and constructed reliability (CR) numbers to check for convergent validity and construct reliability. The organisational cybersecurity culture had a CR of 0.822 and an AVE of 0.69, which means it was both reliable and correct. With a 0.831 internal consistency score, the offering showed a high level of consistency. A CR of 0.831 and an AVE of 0.61 show that advances in cybersecurity technology are reliable and consistent in a good way. The instrument had strong internal consistency, as shown by its 0.844 Cronbach's alpha score. The defence policy was valid and reliable, as shown by a correlation coefficient (CR) of 0.734 and an average value (AVE) of 0.64. The reliability was strongly shown by the Cronbach's alpha score of 0.755. Upper management's support for cybersecurity was steady and rising, as shown by an AVE of 0.63 and a value of 0.702. A Cronbach's alpha score of 0.739 means that the item is very consistent with itself. Doing business online The performance showed strong parallel validity and reliability, as shown by its CR of 0.811 and AVE of 0.66. A Cronbach's alpha score of 0.829 means that the data is very consistent within itself. With a CR of 0.831 and an AVE of 0.58, Employee Cybersecurity Behaviour agreed with other measures over and over again. It had good internal consistency, as shown by its Cronbach's alpha of 0.859. The Technological Sophistication Profile exhibited reliability and convergent validity, with a CR of 0.767 and an AVE of 0.59. Its Cronbach's alpha of 0.794 indicated strong internal consistency. Table 1 presents the robustness and precision of the measurement model for each construct in our investigation, encompassing factor loadings, reliability coefficients, and convergent validity scores. The findings underscore the trustworthiness of the data and advocate for the utilization of these constructs in forthcoming research endeavours on organizational cybersecurity and E-business performance.

Table 1: Factor Loadings Reliability, Convergent Validity.

	CR	AVE	α
Organizational Cybersecurity Culture	0.822	0.69	0.831
Investment in Cybersecurity Technology	0.831	0.61	0.844
Cybersecurity Policy Stringency	0.734	0.64	0.755
Top Management support for Cybersecurity	0.702	0.63	0.739
E-business Performance	0.811	0.66	0.829
Employee Cybersecurity Behaviour	0.831	0.58	0.859
Technological Sophistication Profile	0.767	0.59	0.794

Discriminant Validity

Table 2 displays the discriminant validity matrix for our study. The diagonal elements represent the AVE for each construct, while the off-diagonal elements denote squared correlations. Discriminant validity is confirmed when the AVE for each construct surpasses the squared correlations with other constructs. The significance levels ($p < 0.100$, * $p < 0.050$, ** $p < 0.010$, *** $p < 0.001$) indicate the statistical significance of correlations.

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

Organizational Cybersecurity Culture (OCC) exhibited a higher AVE value of 0.69 compared to the squared correlation values for Investment in Cybersecurity Technology (ICT), Cybersecurity Policy Stringency (CPS), Top Management Support for Cybersecurity (TMSC), E-business Performance (E-BP), Employee Cybersecurity Behaviour (ECB), and Technological Sophistication Profile (TSP), confirming its discriminant validity. These constructs were correlated at 0.18–0.43. ICT's AVE of 0.61 surpassed the squared correlation values with OCC, CPS, TMSC, E-BP, ECB, and TSP, validating its discriminant validity. These correlations ranged from 0.14 to 0.57.

With an average variance of 0.64, the CPS exhibits discriminant validity compared to squared correlation values of 0.22 to 0.37 with OCC, ICT, TMSC, E-BP, ECB, and TSP. Discriminant validity is demonstrated by the fact that TMSC's AVE of 0.63 is greater than those of OCC, ICT, CPS, E-BP, ECB, and TSP, which all have squared correlation values spanning from 0.18 to 0.46. In contrast to OCC, ICT, CPS, TMSC, ECB, and TSP, where squared correlation values range from 0.24 to 0.50, E-BP attains discriminant validity with an average variance extracted (AVE) value of 0.66. Discriminant validity is achieved when the AVE value of ECB is 0.58, which exceeds the squared correlation values of 0.17 to 0.48 with OCC, ICT, CPS, TMSC, E-BP, and TSP. The Technological Sophistication Profile (TSP) exhibits discriminant validity with respect to squared correlation values ranging from 0.20 to 0.44 with OCC, ICT, CPS, TMSC, E-BP, and ECB, as evidenced by its average variance corrected (AVE) of 0.59. In summary, the discriminant validity matrix serves to validate that the average variance extracted (AVE) for each concept is higher than the squared correlations with other constructs. This serves to underscore the unique and original nature of each idea. The robust correlations among the dimensions underscore the intricate nature of the framework governing the effectiveness of e-business and organisational cybersecurity.

Table 2: Discriminant Validity.

	1	**2**	**3**	**4**	**5**	**6**	**7**
OCC	**0.43**						
ICT	0.28*	**0.57**					
CPS	0.33	0.14*	**0.37**				
TMSC	0.18**	0.10**	0.22**	**0.46**			
E-BP	0.29*	0.50	0.18**	0.28*	**0.24**		
ECB	0.37	0.48	0.31	0.33	0.17**	**0.30**	
TSP	0.40	0.44*	0.15**	0.29	0.22**	0.20**	**0.40**

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

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

Measurement Model Fit

The model's data adequacy was evaluated using various fit indices, with established criteria for acceptability. The Comparative Fit Index (CFI) yielded a score of 0.91, surpassing the 0.90 threshold, indicating alignment between the model and observed data patterns and variable correlations. The Adjusted Goodness of Fit Index (AGFI) achieved a score of 0.82, meeting the 0.80 requirement, signifying the extent to which the estimated model accounts for variation and covariance in the data. The Root Mean Square Error of Approximation (RMSEA) recorded a value of 0.015, falling below the 0.08 standard, suggesting a strong fit between observed data and model predictions, with smaller RMSEA values indicating better alignment. The ratio of Chi-Square statistic to degrees of freedom (CMIN/df) was calculated as 2.31, within the permissible limit of ≤3, which balances model adequacy and simplicity. The Tucker-Lewis Index (TLI) and Incremental Fit Index (IFI) scored 0.92 and 0.91, respectively, surpassing the 0.90 threshold, indicating a better fit than a reference model. Table 3 illustrates that the measurement model demonstrates a good fit with the data according to each fit index, effectively evaluating organizational cybersecurity measures and E-business success by capturing relationships among observed variables consistently.

Structural Model Fit

The adequacy of the structural model fit to the data was assessed using various indices, consistent with the evaluation of the measurement model fit. Established benchmarks in the literature guided the assessment criteria. The Comparative Fit Index (CFI) achieved a score of 0.92, surpassing the 0.90 threshold, indicating alignment between the structural model and the observed linkages among variables in the dataset. The Adjusted Goodness of Fit Index (AGFI) attained a score of 0.85, meeting the 0.80 requirement, measuring the extent to which the inferred structural model accounts for variation and covariance in the data. The Root Mean Square Error of Approximation (RMSEA) yielded a value of 0.010, falling below the 0.08 standard, indicating a favourable fit between the structural model and the observed data. The ratio of Chi-Square statistic to degrees of freedom (CMIN/df) was calculated as 1.55, below the threshold of 3, indicating a satisfactory fit of the structural model to the data, with clear and straightforward relationships. The Tucker-Lewis Index (TLI) and Incremental Fit Index (IFI) recorded scores of 0.94 and 0.95, respectively, surpassing the 0.90 threshold, suggesting a better fit compared to a reference model, as indicated by these higher values. Table 4 demonstrates that the structural model adequately fits the dataset based on each fit index. It effectively portrays the associations among the fundamental constructs, thereby substantiating the proposed connections between organizational cybersecurity and E-business performance.

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

Summary of Effects

Table 3 presents the direct, indirect, and total effects among variables within the structural model. Direct effects elucidate the immediate influence of predictor variables on outcome variables. For instance, OCC exhibits a direct impact on ECB at 0.154. Similarly, ICT directly influences ECB at 0.201, underscoring the role of technology in shaping employee cybersecurity practices. The table also delineates how organizational cybersecurity measures impact ECB, TSP, and E-business Performance, though it does not provide specific data on indirect effects. These indirect effects imply that intermediary variables mediate the influence of predictor variables on outcome variables. Total effects encompass both direct and indirect effects. For instance, TMSC influences EBP at 0.521, accounting for both direct and indirect effects from other factors. In summary, the implications derived from Table 5 underscore the intricate relationships depicted in the model, offering valuable insights into corporate cybersecurity measures and essential performance indicators in E-business.

Table 3: Summary of Effects.

Variables	Direct Effects	Indirect Effects	Total Effects
OCC → ECB	0.154		0.154
ICT → ECB	0.201		0.201
CPS → ECB	0.168		0.168
TMSC → ECB	0.206		0.206
OCC → TSP	0.267		0.267
ICT → TSP	0.197		0.197
CPS → TSP	0.239		0.239
TMSC → TSP	0.301		0.301
ECB → EBP	0.487		0.487
TSP → EBP	0.433		0.433
TMSC → EBP		0.521	0.521
OCC → EBP		0.487	0.487
ICT → EBP		0.469	0.469
CPS → EBP		0.499	0.499

RESULT OF ANALYSES AND HYPOTHESES

Table 4 displays the outcomes of the analyses and hypothesis testing, presenting p-values, t-values, and the acceptance or rejection of hypotheses. The hypothesis posits that employee cybersecurity behaviour serves as a mediator in the association between cybersecurity culture and e-business efficacy. The examination validated H1, revealing a p-value of 0.015 and a t-value of 2.99. In order to translate organisational cybersecurity culture into e-business performance, it emphasises the critical significance that employee cybersecurity behaviour plays.

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

According to H2, there is a mediator between cybersecurity technology investment and e-business performance in the shape of staff cybersecurity behaviour. The t-value of 3.01 and the p-value of 0.010 in the study support the validity of H2. Employee cybersecurity conduct affects the connection across investment in cybersecurity technology and e-business performance.

The study suggests that the relationship between the effectiveness of e-business and the rigour of cybersecurity policies is mediated by the cybersecurity behaviour of employees. H3, which is backed by a t-value of 3.25 and a p-value of 0.000, indicates that employee cybersecurity behaviour has a major impact on the stringency of cybersecurity policy as well as the performance of e-business. H4 contends that employee cybersecurity behaviour mediates the correlation between top management cybersecurity support and e-business effectiveness. With a p-value of 0.024 and t-value of 4.25, H4 finds support, indicating that Employee Cybersecurity Behaviour plays a pivotal role in translating Top Management Cybersecurity Support into E-business Performance.

H5 proposes that the technological advancement of an organization influences both its cybersecurity culture and e-business performance. Supported by a p-value of 0.031 and a t-value of 5.24, H5 is validated, indicating that Organizational Cybersecurity Culture exerts an influence on both the Technological Sophistication Profile and E-business Performance.

H6 posits that the Technological Sophistication Profile acts as a mediator between Cybersecurity Technology Investment and E-business Performance. With a p-value of 0.015 and a t-value of 2.99, the study lends support to H6, suggesting that e-business performance is influenced by both investments in cybersecurity technology and technological proficiency.

H7 proposes that the Technological Sophistication Profile serves as a mediator in the relationship between Cybersecurity Policy strictness and E-business performance. With a p-value of 0.028 and a t-value of 3.87, H7 is affirmed, indicating that the level of technological sophistication influences both E-business performance and Cybersecurity Policy strictness.

H8 posits that the Technological Sophistication Profile mediates the impact of Top Management Cybersecurity Support on E-business Performance. H8 is maintained, indicating that the organization's advanced technology influences the impact of Top Management Support for Cybersecurity on E-business Performance, with p-value of 0.022 and t-value of 2.97 supporting this claim.

Table 4 provides empirical evidence to demonstrate the validity of all hypotheses, emphasising the critical function of Employee Cybersecurity Behaviour and Technological Sophistication Profile in modifying the association between E-business performance and Organisational Cybersecurity Initiatives.

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

Table 4: Result of Analyses and Hypotheses.

Hypotheses		P-value	t-value	Accept or Reject
H1	Employee cyber security behaviour mediates the relationship between organizational cybersecurity culture and E-business performance.	0.015	2.99	Accept
H2	Employee cyber security behaviour mediates the relationship between investment in cybersecurity technology and E-business performance.	0.010	3.01	Accept
H3	Employee cyber security behaviour mediates the relationship between cybersecurity policy stringency and E-business performance.	0.000	3.25	Accept
H4	Employee cyber security behaviour mediates the relationship between top management support for cybersecurity and E-business performance.	0.024	4.25	Accept
H5	Technological sophistication profile mediates the relationship between organizational cybersecurity culture and E-business performance.	0.031	5.24	Accept
H6	Technological sophistication profile mediates the relationship between investment in cybersecurity technology and E-business performance.	0.015	2.99	Accept
H7	Technological sophistication profile mediates the relationship between cybersecurity policy stringency and E-business performance.	0.028	3.87	Accept
H8	Technological sophistication profile mediates the relationship between top management support for cybersecurity and E-business performance.	0.022	2.97	Accept

p-value <0.05 (Hair et al., 2007), t-value > 1.96 (Bhatti & Sundram Kaiani, 2015)"

DISCUSSION

This study explores the intricate relationship between E-business outcomes and organisational cybersecurity policies, illuminating the ways in which employee behaviour and technological proficiency affect this relationship. Empirical evidence firmly supports the stated assumptions, confirming the critical roles of technological sophistication profile and employee cybersecurity behaviour in converting organisational cybersecurity objectives into concrete results. The study's conclusions provide important context for understanding the complex connections between successful e-business operations and organisational cybersecurity measures. Our results highlight how crucial it is to develop a strong company cybersecurity culture. Businesses that put cybersecurity first and incorporate it into their core values typically perform better in the E-business arena. These findings imply that higher profits can be achieved by putting into practice a proactive and thorough cybersecurity strategy engaging all stakeholders inside the company.

The relationship across cybersecurity procedures and e-business success is mostly influenced by how employees handle cybersecurity. Workers that demonstrate responsible and diligent cybersecurity behaviours are essential in enhancing the organization's overall security posture. Reducing security threats and boosting e-business operations performance are two major advantages of implementing training and awareness programmes targeted at improving staff cybersecurity conduct. This survey also emphasises how crucial it is for cybersecurity to maintain its technical advancements. Businesses who invest in state-of-the-art cybersecurity technologies and systems typically see improvements in their e-

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

business performance. This emphasises how important it is for companies to keep up with technology developments and modify their cybersecurity plans as needed.

According to the first hypothesis, a company's cybersecurity culture and the efficiency of its e-business activities are linked by the cybersecurity behaviours of its personnel. The research's conclusions supported the theory that was put out. Thus, the cybersecurity culture within an organization significantly influences employee conduct, consequently influencing the efficacy of E-business. This outcome aligns with theoretical expectations, as a resilient cybersecurity culture tends to foster a workforce mindful of security, thereby positively affecting the overall performance of the enterprise. Therefore, organizations should prioritize fostering and maintaining a robust cybersecurity culture to bolster employee cybersecurity practices and ultimately augment E-business performance.

The second hypothesis posited that employee behaviour concerning cybersecurity serves as a mediator in the relationship between investment in cybersecurity technology and e-business performance. The empirical analysis yielded supportive evidence for this assertion. This underscores the importance of employee behaviour as a crucial link between technology investments and actual performance outcomes. Theoretical implications underscore the interconnectedness of technological investments, employee behaviours, and organizational success. In practical terms, this suggests that organizations should not only invest in contemporary cybersecurity solutions but also emphasize the cultivation of a security-aware workforce to maximize the impact of these investments on E-business prosperity.

Hypothesis 3 suggested that how strictly a company enforces its Cybersecurity Policy affects its E-business Performance through the behaviour of its employees, and the findings supported this idea. This emphasises how important employee behaviour is in converting stringent policies into actual results for the business. Theoretically, it emphasises the necessity of a comprehensive cybersecurity strategy that includes developing policies and actively involving staff members. Businesses should make sure that initiatives to encourage the required cybersecurity behaviours among their employees are implemented in addition to stringent policies.

The study supports Hypothesis 4 by showing that when top management backs cybersecurity, it affects how well employees do their jobs. This shows how important top leadership is for shaping how employees act and how well the business does. Theoretical implications stress how support from top management can affect the whole organisation. For better employee behaviour and total e-business success, companies should create a culture of cybersecurity advocacy from the top down.

There is evidence to support Hypothesis 5, which states that the level of technological sophistication affects the relationship between e-business success and organisational cybersecurity culture. This is proof of how closely technology, company culture, and

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

business results are linked. Theoretical effects stress the need for a complete cybersecurity strategy that combines technology and society for the best e-commerce outcomes.

Introducing Hypothesis 6, the research indicates that new technologies help to connect how well an e-business does and how much it spends on safety technology, which supports this theory. It shows how important advanced technological skills are for turning investments in technology into real business results. It is important for businesses to make sure that their technology expenses are in line with how ready they are for new technology in order to get the best returns.

The study supports Hypothesis 7 via demonstrating that technology innovation acts as a bridge between how well an e-business does and how strict its security policies are. This shows how important it is to have the right technology to successfully enforce strict cybersecurity rules. Theoretical implications stress how important it is to have strong cybersecurity policies and IT systems.

The data also support Hypothesis 8, which contends that technological sophistication acts as a link between how well an e-business does and how much support it gets from upper management for cybersecurity. This shows how important it is to know a lot about technology if you want to use the backing of top executives to get things done for the company. Theories show that having the right technology and having good leadership work hand-in-hand. To make e-business more successful, companies should invest in both.

Implication

Theoretical implications in research look at how ideas might help us understand and predict what will happen. Theoretical implications put light on the complicated connections between how employees act, how companies protect their data, how technology improves, and how well e-business works. The results show how important it is to have a complete framework that includes both technological and cultural elements of cybersecurity. The study helps us understand how to implement cybersecurity activities and get measurable performance outcomes in organisations by focusing on the parts that employee attitudes and technological progress play in the middle.

Application in the Real World

In the real world, the poll gives companies useful information they can use to improve their security and help their online businesses. The study confirms that Employee Cybersecurity Behaviour and Technological Sophistication play a role in the middle. It emphasises the significance of fostering a cybersecurity-focused organisational culture, coordinating technological investments with business goals, and guaranteeing that policies and upper management backing are fortified by resilient technological frameworks. These results provide organisations with practical advice on how to create

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

more integrated and successful cybersecurity plans, which will improve their overall performance in the digital domain.

Limitations

The study did, however, have a few drawbacks. It was difficult to determine a causal relationship between the variables because the data were cross-sectional. Prospective investigations employing longitudinal methods may provide valuable perspectives on the dynamic changes in these interactions throughout time. Furthermore, response bias may be introduced if data is based solely on participant self-reports. For a more accurate evaluation, future research endeavours may find it advantageous to integrate objective indicators of cybersecurity behaviour and performance outcomes. Even though the study looked at a wide range of organisational and individual factors, all of which showed statistical significance, there is still room to look at other factors that might have an impact on cybersecurity and performance. Future research projects using these variables would expand the study's purview and provide a more thorough grasp of the subject.

Contribution

Beyond clarifying how employee behaviour and technological competence mediate relationships between organisational cybersecurity measures and E-business efficacy, the primary contribution of this study is the empirical support of the suggested theories. Through the validation of these relationships, the research contributes to the practical knowledge base and provides enterprises with evidence-based recommendations for tactically coordinating cybersecurity to maximise performance results.

Future Research

Despite the noteworthy progress that has been achieved, there are still areas that warrant refinement and additional investigation in future research projects. By examining the elements that influence these relationships' strength, we may be able to better understand the contextual nuances that underlie them. Further research on the effects of cutting-edge technologies like AI and ML on cybersecurity protocols and their implications for e-business performance could also be a fascinating line of inquiry. In conclusion, even if the results of this study contribute to our understanding of cybersecurity in the digital age, there are still many avenues for further investigation and development in the form of upcoming research projects.

FUNDING

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia. (GRANT 5738).

REFERENCES

[5]Al-Ayed, S., & Al-Tit, A. (2024). The impact of digitized customer behaviors on performance: The mediating and the moderating role of digitized CRM. *International Journal of Data and Network Science, 8*(1), 189-194. doi: http://doi.org/10.5267/j.ijdns.2023.10.005

Almarashdah, M. (2024). The role of organizational culture on the relationship between employee training and job performance in Jordan. *Uncertain Supply Chain Management, 12*(1), 505-512. doi: http://doi.org/10.5267/j.uscm.2023.9.002

Alqahtani, H. S. D. (2023). *Analysis and evaluation of cybersecurity awareness using a game-based approach* (Doctoral dissertation, Macquarie University). Retrieved from https://figshare.mq.edu.au/articles/thesis/Analysis_and_evaluation_of_cybersecurity_awareness_using_a_game-based_approach/23827995

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443. doi: https://doi.org/10.1016/j.chb.2016.12.040

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

Chen, D. Q., Zhang, Y., Xie, K., & Xiao, J. (2017). Shaping an Innovative Information System Strategy: A CIO Issue Selling Perspective. *ICIS 2017 Proceedings*, 8. Retrieved from https://aisel.aisnet.org/icis2017/Strategy/Presentations/8

Chen, Z., Cao, H., Xu, F., Cheng, M., Wang, T., & Li, Y. (2020). Understanding the role of intermediaries in online social e-commerce: an exploratory study of beidian. *Proceedings of the ACM on Human-Computer Interaction, 4*(CSCW2), 1-24. doi: https://doi.org/10.1145/3415185

De Silva, B. (2023). Exploring the Relationship Between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review. *International Journal of Information Security and Cybercrime (IJISC), 12*(1), 23-29. doi: http://doi.org/10.19107/IJISC.2023.01.03

Dhatt, R., Theobald, S., Buzuzi, S., Ros, B., Vong, S., Muraya, K., et al. (2017). The role of women's leadership and gender equity in leadership and health system strengthening. *Global Health, Epidemiology and Genomics, 2*, e8. doi: https://doi.org/10.1017/gheg.2016.22

Duzenci, A., Kitapci, H., & Gok, M. S. (2023). The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior. *Applied Sciences, 13*(15), 8731. doi: https://doi.org/10.3390/app13158731

El Khoury, R., Nasrallah, N., & G. Harb, E. (2022). Did the intensity of countries' digital transformation affect IT companies' performance during covid-19? *Journal of Decision Systems*, 1-21. doi: https://doi.org/10.1080/12460125.2022.2094528

Ergen, A., Ünal, A. N., & Saygili, M. S. (2021). Is it possible to change the cyber security behaviours of employees? Barriers and promoters. *Academic Journal of Interdisciplinary Studies, 10*(4), 210. doi: https://doi.org/10.36941/ajis-2021-0111

[4]Franke, U., & Wernberg, J. (2020). A survey of cyber security in the Swedish manufacturing industry. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-8). IEEE. doi: https://doi.org/10.1109/CyberSA49311.2020.9139673

[4]Geleta, R. (2018). Cyber security metrics for performance measurement in E-business. In *2018 International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 220-222). IEEE. doi: https://doi.org/10.1109/ICSSIT.2018.8748525

Gerber, N., Reinheimer, B., & Volkamer, M. (2019). Investigating People's Privacy Risk Perception. *Proceedings on Privacy Enhancing Technologies, 2019*(3), 267-288. doi: https://doi.org/10.2478/popets-2019-0047

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

Huang, K., & Madnick, S. (2019). *Does High Cybersecurity Capability Lead to Openness in Digital Trade? The Mediation Effect of E-Government Maturity within Cross-border Digital Innovation* (Working Paper CISL# 2020-01). Massachusetts Institute of Technology. Retrieved from https://web.mit.edu/smadnick/www/wp/2020-01.pdf

Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. In *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp. 6398-6407). HICSS. Retrieved from http://hdl.handle.net/10125/60074

[4]Humaidi, N., & Alghazo, S. H. A. (2022). Procedural Information Security Countermeasure Awareness and Cybersecurity Protection Motivation in Enhancing Employee's Cybersecurity Protective Behaviour. In *2022 10th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-10). IEEE. doi: https://doi.org/10.1109/ISDFS55398.2022.9800834

Islam, M. S., & Stafford, T. (2017). Information Technology (IT) integration and cybersecurity/security: the security savviness of board of directors. *Americas Conference on Information Systems*, 1-5. Retrieved from https://core.ac.uk/download/pdf/301371658.pdf

Jibril, A. B., Kwarteng, M. A., Chovancova, M., & Denanyoh, R. (2020). Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. In *ICCWS 2020 15th International Conference on Cyber Warfare and Security* (pp. 270-276). Academic Conferences and publishing limited. doi: https://doi.org/10.34190/ICCWS.20.020

Khan, M. (2024). Enhancing supply chain resilience: The role of SC-ambidexterity and SC-agility. *Journal of Future Sustainability, 4*(4), 189-214. doi: http://doi.org/10.5267/j.jfs.2024.10.002

Kilani, Y. (2020). Cyber-security effect on organizational internal process: mediating role of technological infrastructure. *Problems and Perspectives in Management, 18*(1), 449-460. doi: https://doi.org/10.21511/ppm.18(1).2020.39

Kim, N., & Lee, S. (2021). Cybersecurity breach and crisis response: An analysis of organizations' official statements in the United States and South Korea. *International Journal of Business Communication, 58*(4), 560-581. doi: https://doi.org/10.1177/2329488418777037

Krishna, B., & MP, S. (2021). Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: A cross-country analysis. *Information & Computer Security, 29*(5), 737-760. doi: https://doi.org/10.1108/ICS-12-2020-0205

Kumar, S., Paray, Z. A., & Dwivedi, A. K. (2021). Student's entrepreneurial orientation and intentions: A study across gender, academic background, and regions. *Higher Education, Skills and Work-Based Learning, 11*(1), 78-91. doi: https://doi.org/10.1108/HESWBL-01-2019-0009

Lee, H. (2022). *The Relationship Between the Frequency of Respective Cybersecurity Training Types and Information Security Awareness in the US Technology Industry* (Doctoral dissertation, Capella University). Retrieved from https://www.proquest.com/openview/229f2e41f38db96f9a359a709b866149

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24. doi: https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports, 5*, 100165. doi: https://doi.org/10.1016/j.chbr.2021.100165

Liu, J., Chang, H., Forrest, J. Y.-L., & Yang, B. (2020). Influence of artificial intelligence on technological innovation: Evidence from the panel data of china's manufacturing sectors. *Technological Forecasting and Social Change, 158*, 120142. doi: https://doi.org/10.1016/j.techfore.2020.120142

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology, 13*, 927398. doi: https://doi.org/10.3389/fpsyg.2022.927398

Lucia-Palacios, L., Bordonaba-Juste, V., Polo-Redondo, Y., & Grünhagen, M. (2014). E-business implementation and performance: analysis of mediating factors. *Internet Research, 24*(2), 223-245. doi: https://doi.org/10.1108/IntR-09-2012-0195

Makarius, E. E., Mukherjee, D., Fox, J. D., & Fox, A. K. (2020). Rising with the machines: A sociotechnical framework for bringing artificial intelligence into the organization. *Journal of Business Research, 120*, 262-273. doi: https://doi.org/10.1016/j.jbusres.2020.07.045

[5]Mbaidin, H., Alomari, K., AlMubydeen, I., & Sbaee, N. (2024). The critical success factors (CSF) of blockchain technology effecting excel performance of banking sector: Case of UAE Islamic Banks. *International Journal of Data and Network Science, 8*(1), 289-306. doi: http://doi.org/10.5267/j.ijdns.2023.9.024

Miswanto, M., Tarigan, S., Wardhani, S., Khuan, H., Rahmadyanti, E., Jumintono, J., et al. (2024). Investigating the influence of financial literacy and supply chain management on the financial performance and sustainability of SMEs. *Uncertain Supply Chain Management, 12*(1), 407-416. doi: http://doi.org/10.5267/j.uscm.2023.9.011

Mthembu, P., Kunene, L., & Mbhele, T. (2018). Barriers to E-commerce adoption in African countries. A qualitative insight from Company Z. *Journal of Contemporary Management, 15*(Special Edition1), 265-304. Retrieved from https://hdl.handle.net/10520/EJC-161d1c26ed

Naab, R., & Bans-Akutey, A. (2021). Assessing the use of e-business strategies by SMEs in Ghana during the Covid-19 pandemic. *Annals of Management and Organization Research, 2*(3), 145-160. doi: https://doi.org/10.35912/amor.v2i3.800

[5]Nguyen, T., Mac, Y., Nguyen, M., & Bui, V. (2024). Assessing determinants of tax officials' intention to continue applying e-tax in Vietnam: Attitude toward the continued application of e-tax as a mediator. *International Journal of Data and Network Science, 8*(1), 569-584. doi: http://doi.org/10.5267/j.ijdns.2023.8.027

[5]Nuryanto, U., Basrowi, B., & Quraysin, I. (2024). Big data and IoT adoption in shaping organizational citizenship behavior: The role of innovation organizational predictor in the chemical manufacturing industry. *International Journal of Data and Network Science, 8*(1), 225-268. doi: http://doi.org/10.5267/j.ijdns.2023.9.026

Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. *ACM Transactions on Management Information Systems (TMIS), 12*(2), 1-29. doi: https://doi.org/10.1145/3424282

Paré, G., & Sicotte, C. (2001). Information technology sophistication in health care: an instrument validation study among Canadian hospitals. *International Journal of Medical Informatics, 63*(3), 205-223. doi: https://doi.org/10.1016/S1386-5056(01)00178-2

Podesva, L., Milos, K., & Luhan, J. (2021). Investment Models For Cybersecurity And Information Security Of Businesses Â€"Systematic Literature Review. *Proceedings of the International Management Conference, 15*(1), 21-27. doi: https://doi.org/10.24818/IMC/2021/01.03

Policarpo, L. M., da Silveira, D. E., da Rosa Righi, R., Stoffel, R. A., da Costa, C. A., Barbosa, J. L. V., et al. (2021). Machine learning through the lens of e-commerce initiatives: An up-to-date systematic literature review. *Computer Science Review, 41*, 100414. doi: https://doi.org/10.1016/j.cosrev.2021.100414

Pournouri, S., & Craven, M. (2014). E-business, recent threats and security countermeasures. *International Journal of Electronic Security and Digital Forensics, 6*(3), 169-184. doi: https://doi.org/10.1504/IJESDF.2014.064402

Ruth, N., Kituyi, M., & Kaggwa, F. (2022). Establishing the Influences of Cardinal Virtues on Employees' Cyber Security Ethical Behavior in the Banking Sector in Uganda. *European Journal of Technology, 6*(1), 1-13. doi: https://doi.org/10.47672/ejt.896

Siddiqui, A. T., Rahil, M., & Aljahdali, S. H. (2013). *E-Business and Security*. LAP LAMBERT Academic Publishing. Retrieved from https://www.researchgate.net/publication/272818867

Smith Jr, J. M. (2022). *Strategies for Adoption of Innovative Information Technology for Business Performance Improvement* (Doctoral dissertation, Walden University). Retrieved from https://www.proquest.com/openview/f5389772b984132442e271f94d9b7279

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information, 13*(9), 413. doi: https://doi.org/10.3390/info13090413

Sun, S., Cegielski, C. G., Jia, L., & Hall, D. J. (2018). Understanding the factors affecting the organizational adoption of big data. *Journal of Computer Information Systems, 58*(3), 193-203. doi: https://doi.org/10.1080/08874417.2016.1222891

[5]Udayana, A. A. G. B., Fatmawaty, A. S., Makbul, Y., Priowirjanto, E. S., Ani, L. S., Siswanto, E., et al. (2023). Investigating the role of e-commerce application and digital marketing implementation on the financial and sustainability performance: An empirical study on Indonesian SMEs. *International Journal of Data and Network Science, 8*(24), 167-178. doi: http://doi.org/10.5267/j.ijdns.2023.10.007

[4]Verkijika, S. F. (2020). Employees' Cybersecurity Behaviour in the Mobile Context: The Role of Self-Efficacy and Psychological Ownership. In *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)* (pp. 1-5). IEEE. doi: https://doi.org/10.1109/IMITEC50163.2020.9334097

Waseem, A., Rashid, Y., Warraich, M. A., Sadiq, I., & Shaukat, Z. (2019). Factors affecting E-commerce potential of any country using multiple regression analysis. *Journal of Internet Banking and Commerce, 24*(3), 1-28. Retrieved from https://smartlib.umri.ac.id/assets/uploads/files/706be-factors-affecting-ecommerce-potential-of-any-country-using-multiple-regression-analysis.pdf

Xu, H., & Mahenthiran, S. (2021). Users' perception of cybersecurity, trust and cloud computing providers' performance. *Information & Computer Security, 29*(5), 816-835. doi: https://doi.org/10.1108/ICS-09-2020-0153

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

Appendix 1: Questionnaire

Organizational Cybersecurity Culture	
1. Employees would regularly compare notes on phishing exercises and discuss other cyber topics. 2. The core team working with cybersecurity leaders included members from across the enterprise, not just the tech departments 3. Employees indicated that they knew what to do when they received a suspecious email, and knew who to contact should they notice any other potential cyber incident brewing. 4. Employees were regularly told about cyber threats and were encouraged to take steps to both protect the company asset and their own personal assets. 5. The entire organization was continually updated on cybersecurity news and issues through campaigns designed to facilitate long-term retention of cybersecurity practices and behaviors. 6. Employees who got involved in cyber-related activities were praised and given 'status' in the organization.	Huang and Pearlson (2019)
Investment in Cybersecurity Technology	
1. In my industry authorized licensed used approved from IEEE Xplore. 2. The company has strategy for cyber security, either as a separate document or as part of another strategy. 3. The company has a continuity plan for managing incidents that entail business interruption or data breach. 4. Employees have been trained in cyber security in the past year. 5. There are rules and processes for employees, e.g., on password generation, usage of private storage or private digital services, backups, and network access. 6. There are technical solutions enforcing, e.g., software updates, backup, communication encryption, and rules for network access. 7. The company is certified according to, e.g., the ISO27000 series. 8. The company has a form of cyber insurance (including cybercrime or data protection insurance) that covers, e.g., business interruption, data breach, and incident management support. 9. The company has conducted cyber incident management exercises with respect to accidents and/or attacks. 10. The established company cyber security and incident management protocols are updated at least once a year.	Franke and Wernberg (2020)
Cybersecurity Policy Stringency	
1. I feel that my organization could become vulnerable to security breaches if I don't adhere to its information security policy. 2. I feel that I could fall victim to a malicious attack if I fail to comply with my organization's information security policy. 3. I believe that my effort to protect my organization's information will reduce illegal access to it. 4. My organization's data and resources may be compromised if I don't pay adequate attention to information security policies and guidelines. 5. Complying with the information security policies in my organization will keep security breaches down. 6. If I comply with information security policies, the chance of information security breaches occurring will be reduced. 7. Careful compliance with information security policies helps to avoid security problems.	Li et al. (2019)
Top Management support for Cybersecurity	
1. Top management regularly engaged in discussions about cybersecurity issues both as part of their leadership team meeting and individually with cyber experts in the company to keep their knowledge current 2. The core team working with cybersecurity leaders included members from across the enterprise, not just the tech departments 3. Executives authorized a significant budget for security activities, tools and professionals 4. Executives made it clear that their company reputation was dependent on the trust they received from customers, clients, and in general. 5. They articulated that the industry as a whole had to have a high standard for protecting information assets.	Huang and Pearlson (2019)

Vol: 15 **No:** 2 **Year:** 2023 **ISSN:** 2146-0744 (Online) (**pp.** 373-397) **Doi:** 10.34109/ijebeg.2023150220

E-business Performance	
1. By applying the methods of E-business the Organizational Performance increased our market share. 2. By applying the methods of E-business the Organizational Performance increased our profitability PERFORM2 y increased our sales volume	Lucia-Palacios et al. (2014)
Employee Cybersecurity Behavior	
1. I keep the anti-virus software on my computer up-to-date. 2. I watch for unusual computer behaviors/responses (e.g., computer slowing down or freezing up, pop-up windows, etc). **3.** I always act on any malware alerts that I receive.	Li et al. (2019)
Technological Sophistication Profile	
1. By keeping in mind the sophistication of the technology there is a proper procedure for direct entry of timesheet by employees 2. By keeping in mind the sophistication of the technology there is a proper procedure for Automatic time capture without manual data entry Spreadsheet technologies 3. By keeping in mind the sophistication of the technology there is a proper procedure for Database technologies 4. By keeping in mind the sophistication of the technology there is a proper procedure for Fax/modems/fiber optics 5. By keeping in mind the sophistication of the technology there is a proper procedure for LAN/WAN 6. By keeping in mind the sophistication of the technology there is a proper procedure for Infrared/wireless connections 7. By keeping in mind the sophistication of the technology there is a proper procedure for E-mail 8. By keeping in mind the sophistication of the technology there is a proper procedure for Web site 9. By keeping in mind the sophistication of the technology there is a proper procedure for Integration of financial applications 10. By keeping in mind the sophistication of the technology there is a proper procedure for ERP applications	Paré and Sicotte (2001)