Westcliff International Journal of Applied Research
WIJAR

Westcliff International Journal of Applied Research
Vol. 8, No. 1. Spring 2024
https://doi.org/10.47670/wuwijar202481heq

Management Information Systems and Correlation Between E-Business and Information Security from a Business Intelligence Perspective

Dr. Hajar El Qasemy
Westcliff University

Abstract

The research focus was motivated by the emergence of electronic business which increased during and after the COVID-19 pandemic. The research is a literature review and its purpose is to build awareness about the importance of information security and to analyze the correlation between information security and electronic business in an environment where electronic business is emerging and the gap between electronic business and information security is enlarging. The research is a review of peer-reviewed articles retrieved from case studies, empirical research, case analysis, literature reviews, comparative studies, systematic reviews, and conceptual analysis dating from the years of 2018 to 2023. This literature review defines four business intelligence concepts: management information systems, value driven business, electronic business, and information security. This literature review also reveals the effects of all four business intelligence concepts on organizations' decision-making and financial objectives. Findings of this literature review revealed that electronic businesses need a stronger risk management approach regarding information security. The conclusion shows that the current technological approach and information security tools such as encryption key management, mantraps, and network intrusion detection systems do not ensure trust and/or eliminate digital security risks.

Keywords: Information security, electronic business, management information systems, value driven business, business intelligence

Introduction

The proliferation of coronavirus disease, also referred to as COVID-19, led governments to put in place the indispensable safety measures that would prevent the spread of the virus. The safety measures include prolonged lockdown, quarantine, and isolation (Shah et al., 2020). The impact of the pandemic on people's lifestyle as well as the restrictions of internal movement and international travel pressured brick and mortar businesses to convert into electronic businesses (Bhatti et al., 2020). Electronic business is emerging and the gap between electronic business and information security is enlarging. The purpose of this literature review is to build awareness about the importance of information security and to analyze the correlation between information security and electronic business. Criteria used to analyze the literature includes accuracy, objectivity, currency, and coverage (City University of Hong Kong, 2023).

Accuracy is ensured through peer-reviewed articles and objectivity is maintained through unbiased information. As for the currency, it is confirmed by the recent dates of publications which do not exceed 5 years. The last criteria used to analyze the literature is coverage which evaluates whether the collected information provides a basic coverage or an in-depth coverage that meets the purpose of the literature review. This literature review is thematic as it is organized by content; it defines four business intelligence concepts: management information systems, value driven business, electronic business, and information security and it also reveals the effects of all four business intelligence concepts on organizations' decision-making and financial objectives.

Discussion

It is crucial for organizations to generate profit; thus, managers exploit the available tools that can help their organizations to survive, sustain, and be more profitable. In the context of business intelligence, the available tools include management information systems, value driven business, electronic business, and information security (Baltzan, 2019).

Management Information Systems

Management information system is abbreviated as MIS. It is a computer-based tool that combines organizations' processes and information technology. MIS facilitates storing, visualizing, monitoring, and analyzing information within organizations. MIS makes the organizations' decision-making process simple and efficient (Ali, 2019).

Internet Computer Network System Versus Transmission Control Protocol/Internet Protocol Based System

Toyota standardized its system to benefit more from information available in Japan and overseas. The standardization process consisted of shifting Toyota's internet computer (IC) network system to a transmission control protocol/internet protocol (TCP/IP) based system ("*Information Systems"*, n.d). An IC protocol is a blockchain that runs on nodes enabling decentralized applications to run at web speed while a TCP/IP is a set of communication protocols that allow interconnection between network devices on the internet (Kassab & Darabkh, 2020).

Toyota learned an important lesson from the impact that the world crisis had on its information division in 2008 and improved the efficiency of its system. Toyota's pressure-response to the 2008 crisis included establishment of structural reform of the organization's system development and maintenance. In 2009, the organization implemented new information processing technologies and continued to adapt to the industry's changes simultaneously ("*Information Systems"*, n.d). Changes that occurred within the automotive industry include the appearance of new electronic technologies and compliance with the adjusted global standards (Llopis-Albert et al., 2021). Toyota maximizes its profit by implementing management information systems while other organizations maximize their profit by converting their businesses into value driven businesses.

Value Driven Business

Value Driven Business is abbreviated as VDB. It is a concept that promotes healthy work environments where employees feel valued. The concept also suggests that the organization's core values must always be reflected in the organization's culture. VDB places the purpose of its strategy beyond generating profit and does not compromise its core values during decision-making processes (Nagle et al., 2019). Value driven businesses draw ethical employees who appreciate being valued and recognized by the organization, thus, organizations that converted their businesses into value driven businesses, experienced improvement in terms of employee commitment and brand reputation. The alignment of the organization's employees with the set values not only sustains growth but also builds customers' trust. Customers who appreciate the brands that reflect core values in the organization's culture, are also drawn to value driven businesses (Enholm et al., 2022).

Example of a Value Driven Business

Starbucks is a value driven business. The brand prioritizes human connections and builds communities in its coffee shops. The brand's core values are all reflected in its culture. As an organization, Starbucks mirrors the community vibe even when presenting financial results and expansion possibilities (Musonera, 2021). Some value driven businesses settle for an offline presence to boost their brick-and-mortar experience while other businesses build an online presence to adapt to the current changes in business trends. In the context of business intelligence, changes include but are not limited to the emergence of electronic business which increased during and after the COVID-19 pandemic.

Electronic Business

Electronic business is abbreviated as e-business. It signifies that the organization's operations are based online through the internet, world wide web, intranets, and extranets. Contrary to e-commerce, e-business does not only consist of selling and purchasing products and services online, but it also involves many processes, such as supply chain management, enterprise resource planning, online customer support, and electronic ordering (Zebari et al., 2019). Organizations' preference for e-business processes has been increasing along with COVID-19 restrictions (Bhatti et al., 2020) and the increase of the cyber security actions that encouraged online transactions (Xu & Gao, 2021).

E-business resulted in streamlining organizational processes, operations, and communication. Moreover, e-business decreased transaction costs in the supply chain. Retailing evolved because of the emergence of e-business which led to the possibility of targeting larger segments, automating sales, simplifying digital deliveries, tracking information, and reaching optimization (Zhu et al., 2020).

Cloud Computing Platforms and Technology Infrastructures

Amazon is one of the largest cloud computing platforms in the world. Amazon is an online marketplace that has established itself effectively through continuous innovation and mass scale (Jelassi et al, 2020). Unlike small organizations that cannot afford powerful information technology (IT) infrastructures that enable adoption of artificial intelligence (AI), Amazon and Google invested in computing power infrastructure to enable AI algorithms, machine learning in the cloud, and rich data sets (Enholm et al., 2022). Amazon is not only involved in e-business but also in e-commerce which exposes its information to higher security risks.

Information Security

Information is one of the most sensitive assets within organizations. Information is expected to be protected against unauthorized access or use, e.g., malware, identity theft, and phishing attacks. Information security, which is abbreviated as InfoSec, plays the role of a protector; it constitutes a set of physical and digital tools that organizations create or put in place to prevent, identify, record, and limit the risks related to any unauthorized access to digital and non-digital information (Deb & Roy, 2022).

Information Security Tools

Information security tools include encryption key management, mantraps, and network intrusion detection systems. With information security, information is expected to be protected during its four stages: formatting, transition, processing, and storing. Information security aligns with the CIA triad which represents confidentiality, integrity, and availability. Information security is susceptible to be audited to verify its efficacy (Sintaro & Komolafe, 2021).

Correlation Between E-Business and Information Security

Electronic businesses are most likely to be attacked through hacking, sniffing, masquerading, spoofing, and wiretaps. Electronic businesses perceive Denial of Service, also called DoS attacks, as the most dangerous digital menaces. DoS attacks lock information and prevent the organization from accessing its data. The data may not be destroyed, yet the fact of maliciously locking it, results in financial losses. Being unable to provide existing customers with the appropriate services at the time of the attack does not only result in financial loss but it also negatively affects customers' trust. Customers' trust is of higher value and repairing a brand's negative image is time consuming and costly. For this reason, electronic business relies on information security to address concerns about data integrity loss, data privacy, service, and control depletion (Alghamdi et al., 2020).

Information Security Threats in E-Business

Online threats against e-business include hacking, data breach, e-skimming, online payment fraud, cross-site scripting, phishing, malware, and distributed denial of service.

Hacking and Data Breach

Hacks and data breaches indicate that a computer or a private network is being exploited without authorized access. Hacking is an intentional security violation while data breach is an unintentional security incident. Data breach is caused by non-malicious behavior such as human error and negligence. Whenever sensitive data is left in an insecure environment, a security vulnerability is created; any person without authorized access may view, copy, transmit, steal, edit or use the data. The data could comprise confidential personal information or corporate information. Confidential personal information consists of social security numbers, bank accounts, and healthcare reports. Corporate information consists of customer records, intellectual property, and financial materials (Sharma et al., 2020).

E-skimming and Online Payment Fraud

E-skimming indicates that customers' information is being captured by cyber-criminals as it is being entered in the online check out page of an e-commerce website. Whether cyber-criminals rely on cross-site scripting, phishing, brute force attack, or a third-party compromise, they end up gaining access to the e-commerce website. As soon as cyber-criminals get into the system, they introduce malicious skimming codes. Malicious skimming codes redirect online shoppers to spoofed websites and unlock theft of bank card information in real time (Andreianu, 2023). Making online payments with stolen bank card information is called online payment fraud (Balasubramanian & Rajakani, 2019).

Cross-Site Scripting

Cross-site scripting (XSS) indicates that a hacker relies on web applications to inject malicious codes in web pages. According to Cisco's annual security report, 40% of the cyber-attack attempts are due to cross-site scripting. Customers who visit e-commerce websites that are injected with malicious codes, automatically infect their devices, and expose themselves to cyber-attacks such as phishing and malware. XSS attacks often occur in unprotected online forums, message boards, and blogs (Rodríguez et al., 2020).

Phishing

Phishing indicates that a hacker is posing as a legitimate business to deceive customers. Phishing occurs often in e-commerce when hackers pretend to be part of the e-commerce business and send emails to customers emphasizing on urgency and requiring customers' immediate action. The objective of phishing is to deceive customers into exposing their private or confidential information (Gupta et al., 2021).

Malware

Malware is a malicious software that infects devices such as computers, tablets, and mobile phones. The objective of malwares is to redirect users to alternative websites, restrict access to a specific system, steal money, and get a hold of credentials or personal identifiable information (PII). In the case of a ransomware attack which is a type of malware, cyber-criminals encrypt the data of the e-commerce business via malware and demand a ransom payment in exchange of the decryption key (Kim et al., 2018; Xiao et al., 2020).

Distributed Denial of Service

Distributed denial of service (DDoS) indicates that a cyber-criminal is flooding a server with an excessive number of requests to overload the system (Sahoo et al., 2019). DDoS attacks are coordinated by one machine via botnets which are a network of malware-infected devices (Pan et al., 2021). The objective of DDoS attacks is solely to disrupt a business (Anshari et al., 2022). E-commerce businesses that face DDoS attacks, experience operational disruption and suffer significant financial losses that could potentially result in a complete shutdown (Dahiya & Gupta, 2020).

Importance of Information Security in E-Business

According to Cisco's annual security report of 2018, each online application has a minimum of one vulnerability (Rodríguez et al., 2020). In 2018, the success rate of cyber-attacks against e-commerce businesses was 32.4% (Badotra & Sundas, 2021). The number of attacks continued to rise every year. Malware variants had doubled in number between the years of 2016 and 2017 to reach a total of 670,000,000 malware variants in 2017 (Xiao et al., 2020). In 2019, approximately 15.1 billion data entries were breached ("*More than 15.1 billion records exposed*", 2020). This indicates that cyber-criminals often target customers' personal data; a concern that became a severe issue in e-commerce (Kim et al., 2018)

Organizations are required to protect their servers, networks, endpoints, and databases. To fulfill this requirement, organizations, notably, e-commerce businesses must invest in robust information security to fix all vulnerabilities before a cyber-criminal launches an online attack, e.g., malware, data breach, hacking, online payment fraud, e-skimming, cross-site scripting, phishing, and distributed denial of service.

As the number of data breach grows, the need for cyber security in e-commerce becomes unavoidable not only to protect customers' confidential data but also to protect the entire organization and its stakeholders. With the rapid evolution of e-commerce, there is an improvement in online transactions and an increase in payment card information collected from customers at online check out. Data on payment card information attracts malicious actors with bad intentions.

Since customers do not wish their information to be compromised, whether it is financial or personally identifiable information such as names, addresses, contact details, and birthdates, customers always avoid electronic business platforms that are known for a history of cyber-attacks or for a reputation of weak cyber-security protocols. Investing in robust information security is the key to ensure that customers remain confident in e-commerce. Otherwise, e-commerce businesses can expect a damage in the perception that customers have for e-business. E-commerce businesses can also expect a shift in consumer behavior and a lack of advocacy or engagement with online brands. The economic impact of data breach is costly in terms of reputation and money-wise. This includes the cost of both data breach and lost business (Liu et al., 2022).

Prevention of Digital Threats in E-business

E-commerce websites prevent digital threats through secure sockets layer certificates, multi-factor authentication, secure payments, firewalls or anti-malware, hardware and software updates, third-party risk management, cyber-security training, access control, and network segmentation.

Secure Sockets Layer *Certificates*

Hypertext transfer protocol secure (HTTPS), is a set of cryptographic network protocols that encrypts and verifies communication between a server and a web browser (Shah & Correia, 2021). HTTPS hosting is sometimes referred to as secure sockets layer (SSL) or transport layer security (TLS). Implementation of HTTPS hosting requires a secure sockets layer certificate. The SSL certificate is a digital certificate that binds a cryptographic key to the organization's details allowing encrypted connections (Dastres & Soori, 2020).

Multi-Factor Authentication

Multi-factor authentication (MFA) requires users to provide a minimum of two authentication methods to confirm their identity before accessing their online accounts. Besides a username and a complex password that must be changed periodically, the MFA which is also referred to as two-factor authentication, requires a one-time PIN, a valid response to a security question, identity verification through a mobile application, and/or a biometric scan (Ibrokhimov et al., 2019).

MFA may seem time-consuming, yet it is more secure than a single password and less time-consuming than mitigation against a successful data breach. E-businesses make sure that their stakeholders use MFA and encourage their customers to provide a minimum of two authentication methods to confirm their identity before accessing their online accounts (Ibrokhimov et al., 2019).

Secure Payments

E-businesses secure payments by redirecting customers to a third-party website at check-out. PayPal and Stripe are third-party websites that manage payment transactions independently, keeping customers' credit card details out of the e-business website (Karthick, 2019).

Firewalls, Anti-Malware, Antivirus

Anti-malware, antivirus, and firewalls are software that detect and delete viruses and other malicious software from the system. Anti-Malware, antivirus, and firewalls provide a baseline defense against external threats (Deepak & Varun, 2019). The latest device protection systems combine artificial intelligence and machine-learning (ML) (Al-Tarawneh & Bani-Salameh, 2023).

A firewall is one of the network security measures that helps to record users' activities and prevent data alteration as well as other fraudulent transactions. Firewalls also prevent confidential information from leaving the network without the e-business knowledge. E-businesses always update their firewalls to allow proper traffic control and restriction of data transmission (Deepak & Varun, 2019; Taherdoost, 2023).

Hardware and Software Update

Software updates fix bugs, improve performance, enhance features, and address security vulnerabilities. Most software updates are mainly developed for security purposes. Unpatched hardware or software are not equipped with the latest vital security patches to defend against the most recent digital threats, leaving the opportunity to cyber-criminals to exploit the organization's vulnerabilities (Mugarza et al., 2020).

Third-Party Risk Management

E-businesses' cloud service providers, partners, and suppliers are all part of the supply chain and must be protected from cyber-attacks. Third parties constitute potential weaknesses that must be managed by the e-business, especially if the functionality of the e-business relies tremendously on the third-party. Third-party management includes monitoring, understanding, and remediating risks which could be challenging, especially if hundreds of providers, partners, and suppliers are involved (Radu et al., 2020).

Cyber-security Awareness and Training

Non-malicious behavior such as human error and negligence are the primary cause of data breach. Hence, the importance of cyber-security awareness and training. E-businesses build awareness and authentic engagement through cyber-security strategies. For instance, a cyber-security strategy could indicate that dissemination of the cyber-security culture would start at the C-suite level, filtered down throughout the organization through internal campaigns, consistent cyber-security updates, simulations, and drills. In addition to building cyber-security awareness, e-businesses schedule adequate cyber-security training for employees. Cyber-security training differs based on the exposure risk of each employee or team (Alahmari et al., 2023).

Access Control and Network Segmentation

Access control designates the stakeholders who can access sensitive information and resources. Access control systems reduce the attack surface by designating and controlling the number of stakeholders who can access certain personal data (Neykova & Miltchev, 2019). Network segmentation keeps confidential data separated from the rest of the existing information in the network. In network segmentation, confidential data is firewalled and always monitored (Mhaskar et al., 2021).

Impact of Information Security on E-Business

Information security protects customers' information and prevents online threats against organizations. Information security allows online shoppers to enjoy their shopping experience, make safe financial transactions, and build trust in electronic business platforms. The stronger information security is, the more a brand upholds its reputation and protects itself from fraud and cyber-attacks (Kala, 2023). Based on Juniper Research (2021), e-businesses are expected to lose 206 billion U.S. dollars in online payment frauds between the years of 2021 and 2025. This amount demonstrates why information security must be a top priority in e-business.

Information security indicates that adequate measures are in place to mitigate the risk of facing information security threats (Hrischev, 2020). Thus, saving e-businesses' time, energy, reputation, and assets including cash and inventory. For instance, multi-factor authentication verifies and confirms the identity of both e-business employees and customers through a mobile application, and/or a biometric scan (Ibrokhimov et al., 2019), saving e-businesses' time and energy spent in traditional verification methods. Secure payments via third-party websites keeps customers' credit card details out of the e-business's website. Should a data leak occur, all payment transactions would not be found in the e-business database (Karthick, 2019), saving the e-business from reputational damage.

Network segmentation prevents lateral movements between stakeholders and cyber-criminals (Jha, 2023) while access control systems limit the pathways that could be taken by cyber-criminals to access the e-business system (Kedah, 2023). Network segmentation results in a decrease in the risk of data breach and/or contamination via malware from other parts of the network (Jha, 2023) while access control systems allow the e-business to easily determine the source of data breach and/or contain malicious software (Kedah, 2023).

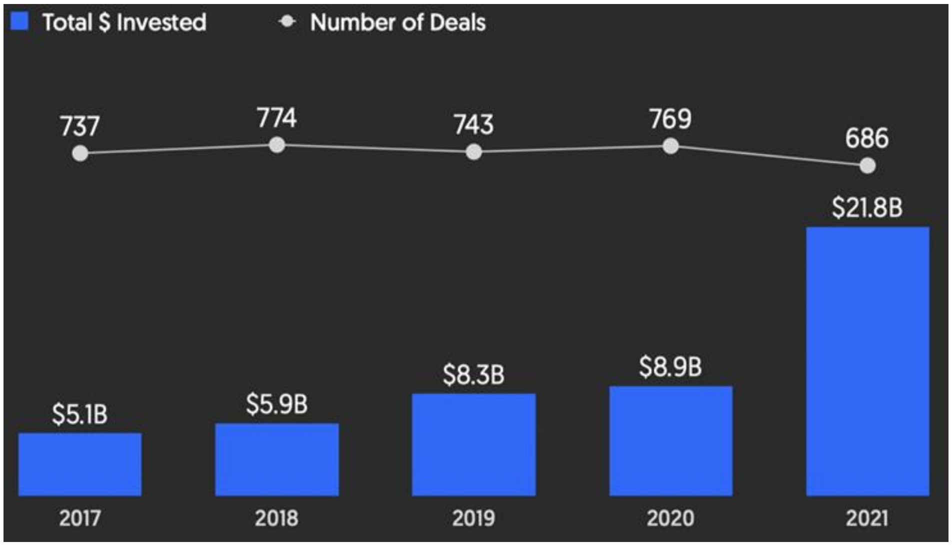
HTTPS provides another layer of connection security that encrypts transferred data. Encryption of transferred data protects e-businesses and challenges hackers who have the intention to read, intercept, or transfer data without authorization (Shah & Correia, 2021). Anti-malware, ant-virus, and particularly firewalls help to record users' activities on e-business websites and prevent data alteration as well as other fraudulent transactions. Firewalls also prevent confidential information from leaving the network without the e-business knowledge (Deepak & Varun, 2019; Taherdoost, 2023). Hardware and software updates provide the latest vital security patches to defend e-businesses against the most recent digital threats, reducing the vulnerabilities that could be exploited by cyber-criminals (Mugarza et al., 2020).

Cyber-security awareness and training reduce the cost associated with human error and negligence which are the primary cause of data breach in e-business. A mature cyber-security culture shapes employees who are capable of detecting, reporting, and remediating suspicious activities within the e-business (Alahmari et al., 2023). Finally, third-party risk management protects the entire supply chain which includes the external contributors who are essential for the functionality of the e-business, e.g., partners, suppliers, and distributors. Third-party risk management ensures continuous flow of operations, allows maintenance of a healthy inventory, and eliminates the cost of disruption (Radu et al., 2020). Yet, although solutions such as Up Guard Vendor Risk exist, third-party risk management is challenging especially if hundreds of partners, suppliers, and distributors are involved (West & Zentner, 2019).

Protection Against Information Security Threats is Never at 100%

Governments are creating cyber-security laws and policies (Luo & Choi, 2022) while e-commerce businesses invest more money to address cyber-security concerns (Vinoth et al., 2022). Figure 1 shows that yearly investment in cyber-security increased between the years of 2017 and 2021 (Metinko, 2022).

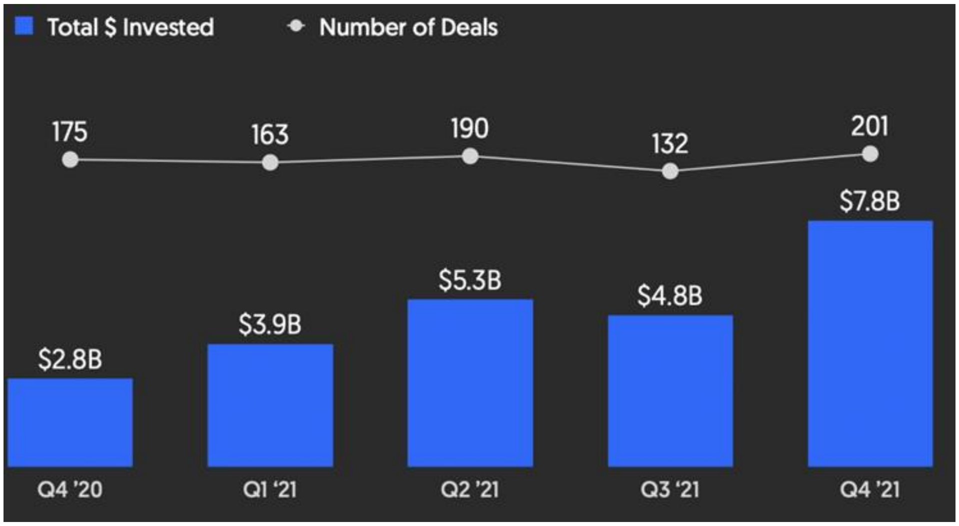
Figure 1
Yearly Investment in Cyber-Security



Note. Adapted from Cybersecurity venture funding surpasses $20B in 2021, fourth quarter smashes record, by C. Metinko, 2022 (https://news.crunchbase.com/news/cybersecurity-venture-funding-2021-record/). In the public domain

Figure 2 shows that quarterly investment in cyber-security increased between the last quarters of 2020 and 2021. Conspicuously, there was a sudden increase in cyber-security investments between the third and fourth quarters of 2021; a remarkable jump from 4.8 billion to 7.8 billion U.S. dollars, respectively, implying that cyber-security concerns are worsening (Metinko, 2022).

Figure 2
Quarterly Investment in Cyber-Security



Note. Adapted from Cybersecurity venture funding surpasses $20B in 2021, fourth quarter smashes record, by C. Metinko, 2022 (https://news.crunchbase.com/news/cybersecurity-venture-funding-2021-record/). In the public domain.

According to the conceptual analysis of social engineering, denial of services, malware, and attacks on personal data, cyber risks can be reduced but not eliminated (Liu et al., 2022). In the loop of never-ending cyber security risks, there are cyber-criminals constantly searching for vulnerabilities and new online users joining e-commerce. New online users, whether e-business owners or customers, are generally more vulnerable compared to old users and are more likely to be detected and attacked by hackers and attackers (Liu et al., 2022).

E-business cannot be protected from information security threats at 100% despite utilizing standard authentication techniques combined with SSL/TLS certificates and multi-factor authentication. Technology is developing and the volume of information security solutions is rising, yet hackers' intelligence is rising too (Gull et al., 2022). Any data being collected is at risk of being compromised regardless of the e-commerce security precautions in place. What matters the most in this unsafe environment is how proactive and well-prepared is the e-business to manage potential cyber risks (Liu et al., 2022). Preparedness comprises implementation of data backups and formulation of incident response plans (Fitri et al., 2023; Kavitha & Ramajayam, 2021).

Data Backups

Cyber incidents interrupt business operations while back-up systems enable immediate restoration of data and a fast recovery of business operations after cyber incidents (Fitri et al., 2023). Data must be continuously backed-up. In case of a cyber incident occurring, all data must be up to date to keep the business functional during the attack. Backed-up data must be stored in a second network, outside the primary network, e.g., secure cloud storage. Should a cyber incident occur, only the primary network would be breached or contaminated while the second network containing the back-up would remain secure (Fitri et al., 2023). Restoration of relevant data in a cyber crisis is an effective cyber incident response that diminishes the impact of data breaches on business operations (Fitri et al., 2023).

Incident Response Plan

Incident response plans state the existing information security policy (ISP) as well as the roles, responsibilities, and contact details of the parties that will be involved in the cyber incident response, if it ever occurs. Incident response plans are constantly checked for accuracy of policy, roles, responsibilities, and contact details of the parties involved (Kavitha & Ramajayam, 2021). Incident response plans clearly formulate the steps that should be followed in a cyber crisis and explain how stakeholders should coordinate what happens after the cyber incident (Kavitha & Ramajayam, 2021).

Management of a cyber crisis is an effective cyber incident response that not only saves the organization's reputation, but also time and resources that could be wasted on unsuccessful attempts to solve sudden cyber-attacks without preparation (Kavitha & Ramajayam, 2021).

Business Intelligence from a Multilateral Point of View

Business intelligence (BI) is characterized by its speed, efficiency, and accuracy. Although no model was created for the analysis of the effects of business intelligence on organizations' decision-making, business intelligence is perceived as an automatic system that helps organizations to make informed strategic decisions that perfectly align with the business's major objectives (Tavera Romero, 2021). A significant number of models were created for the implementation of business intelligence. However, no model was created for the analysis of the effects of business intelligence on organizations' decision-making. Therefore, some suspect that business intelligence may not have any effects on the organization's decision-making. The environment dynamic as well as the pressures and/or other external factors, such as, the threats and opportunities may affect the organization's decision-making (Aghaei & Asadollahi, 2013; Tavera Romero, 2021).

Recommendations

Recommendations for Practice

Findings of this literature review indicates that a risk management approach must be implemented, but prior to implementing a risk management approach, each industry should set the standard needs and determine the best information security tools for its operations. A certification authority should be provided to organizations, notably, e-businesses that comply with and respond to the selected information security criteria. The best information security tools and certification can then be converted into fundamental information security standards for electronic businesses in each industry.

Recommendations for Future Research

Based on the findings of this literature review, a significant number of models were created for the implementation of business intelligence. However, no model was created for the analysis of the effects of business intelligence on organizations' decision-making. Future quantitative research studies with the purpose of accepting or denying the hypothesis of BI having a direct impact on organization's decision-making would build upon the findings of this literature review. Other qualitative research studies with the purpose of revealing the exact impact of BI on organization's decision-making, if any, would also help to fill the gap in the literature.

Conclusion

The purpose of this literature review was to build awareness about the importance of information security and to analyze the correlation between information security and electronic business in an environment where electronic business is emerging and the gap between electronic business and information security is enlarging. Information security threats such as malware variants doubled in number from 2016 to 2017 and approximately 15.1 billion data entries were breached in 2019. As the number of data breaches continues to rise every year at a high success rate, the need for information security in e-commerce becomes unavoidable. Organizations, notably, e-commerce businesses must invest in robust cyber-security solutions to fix all vulnerabilities and protect servers, networks, endpoints, and databases. Adoption of AI based cyber-security requires powerful IT infrastructures that can support extremely large amounts of computing power. Successful e-businesses invest in powerful IT infrastructures to run or complete complex algorithms, process large data sets, and/or perform machine learning. Nonetheless, e-businesses still cannot operate with confidence because they are most likely to be attacked through hacking, sniffing, masquerading, spoofing, and wiretaps. Network security measures such as firewalls and anti-malware, provide real-time threat detection and obstruct cyber-criminals' attempts to perform fraudulent transactions. Access control, network segmentation, and cryptographic network protocols are additional layers of connection security in e-business. Yet, despite investment in network and connection security, the challenge of the cyber-security landscape is worsening. Cyber-criminals are gaining practical experience and acquiring profound knowledge in cyber-attacks. Regardless of how much e-business implements cyber security protocols or training and how much sophisticated technology is used to conduct day-to-day activities, the challenge of cyber-security threats is still present and cyber-attacks are still sudden. E-businesses' existence is threatened by the increasing number of cyber-security attacks, notably, DoS which is perceived as the most dangerous digital menace. Findings of this literature review revealed that there is a need for a strong risk management approach in the field of information security because the current technological approach and information security tools such as encryption key management, mantraps, and network intrusion detection systems do not ensure trust and/or eliminate security risks.

References

Aghaei, M., & Asadollahi, A. (2013). Analysis of business intelligence on strategic decision making. *International Journal of Scientific Management and Development, 2*(1), 20-35. https://www.researchgate.net/publication/303631722_Analysis_of_Business_Intelligence_on_Strategic_Decision_Making

Al-Tarawneh, B. A., & Bani-Salameh, H. (2023). Classification of firewall logs actions using machine learning techniques and deep neural network. *Proceedings of the 4th International Computer Sciences and Informatics Conference, Jordan, 2979*(1). https://doi.org/10.1063/5.0174750

Alahmari, S., Renaud, K., & Omoronyia, I. (2023). Moving beyond cyber security awareness and training to engendering security knowledge sharing. *Information Systems and*

E-Business Management, *21*(1), 123-158. https://doi.org/10.1007/s10257-022-00575-2

Alghamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Ali, M. M. (2019). Impact of management information systems (MIS) on decision making. *Global Disclosure of Economics and Business*, *8*(2), 83-90. https://doi.org/10.18034/gdeb.v8i2.100

Andreianu, G. (2023). Protecting your e-commerce business. Analysis on cyber security threats. *Proceedings of the International Conference on Cybersecurity and Cybercrime, Romania, 10*, 127-134. https://doi.org/10.19107/CYBERCON.2023.17

Anshari, M., Almunawar, M. N., & Al-Mudimigh, A. (2022). Digital marketplace as a new frontier of electronic commerce. In P. Ordóñez de Pablos, X. Zhang, M. Almunawar, & J. Gayo (Eds.), *Handbook of research on big data, green growth, and technology disruption in Asian companies and societies* (pp. 122-137). IGI Global. https://doi.org/10.4018/978-1-7998-8524-5.ch007

Badotra, S., & Sundas, A. (2021). A systematic review on security of e-commerce systems. *International Journal of Applied Science and Engineering*, *18*(2), 1-19. https://doi.org/10.6703/IJASE.202106_18(2).010

Balasubramanian, K., & Rajakani, M. (2019). Electronic payment systems and their security. In Information Resources Management Association (Ed.), *Digital currency: Breakthroughs in research and practice* (pp. 270-285). IGI Global. https://doi.org/10.4018/978-1-5225-6201-6.ch015

Baltzan, P. (2019). *Business driven information systems*. McGraw-Hill Education.

Bhatti, A., Akram, H., Basit, H. M., Khan, A. U., Raza, S. M., & Naqvi, M. B. (2020). E-commerce trends during COVID-19 Pandemic. *International Journal of Future Generation Communication and Networking*, *13*(2), 1449-1452. https://doi.org/ 10.12691/ijbrm-4-1-2

City University of Hong Kong. (2023, July 3). Literature Review - Finding the Resources. Run Run Shaw Library. https://libguides.library.cityu.edu.hk/litreview/evaluating-sources#:~:text=Accuracy%2C%20authority%2C%20objectivity%2C%20currency,evaluating%20information%20from%20any%20sources

Dahiya, A., & Gupta, B. B. (2020). An economic incentive-based risk transfer approach for defending against DDoS attacks. *International Journal of E-Services and Mobile Applications. 12*, 60–84. https://doi.org/10.4018/IJESMA.2020070104

Dastres, R., & Soori, M. (2020). Secure socket layer (SSL) in the network and web security. *International Journal of Computer and Information Engineering*, *14*(10), 330-333. https://hal.science/hal-03024764

Deb, R., & Roy, S. (2022). A comprehensive survey of vulnerability and information security in SDN. *Computer Networks*, *206*, 108802. https://doi.org/10.1016/j.comnet.2022.108802

Deepak, I., & Varun, D. (2019). A survey on network security and management, threats & firewalls. *Journal of Emerging Technologies and Innovative Research*. *6*(3), 199-203.

Enholm, I. M., Papagiannidis, E., Mikalef, P., & Krogstie, J. (2022). Artificial intelligence and business value: A literature review. *Information Systems Frontiers*, *24*(5), 1709-1734. https://doi.org/10.1007/s10796-021-10186-w

Fitri, L. S., Larisma, E., & Levina, B. (2023). Cloud computing technology in development e-business (Literature Review). *Journal of Artificial Intelligence and Engineering Applications (JAIEA)*, *3*(1), 10-14. https://doi.org/10.59934/jaiea.v3i1.232

Gull, H., Saeed, S., Iqbal, S. Z., Bamarouf, Y. A., Alqahtani, M. A., Alabbad, D. A., et al. (2022). An empirical study of mobile commerce and customers security perception in Saudi Arabia. *Electronics, 11*(3), 293-312. https://doi.org/10.3390/electronics11030293

Gupta, B. B., Yadav, K., Razzak, I., Psannis, K., Castiglione, A., and Chang, X. (2021). A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment. *Computer*

Communications. *175*, 47–57. https://doi.org/10.1016/j.comcom.2021.04.023

Hrischev, R. (2020). ERP systems and data security. Proceedings of *IOP Conference Series: Materials Science and Engineering*, Bulgaria, *878*(1), 012009. https://doi.org/10.1088/1757-899X/878/1/012009

Ibrokhimov, S., Hui, K. L., Al-Absi, A. A., & Sain, M. (2019). Multi-factor authentication in cyber physical system: A state of art survey. *2019 21st International conference on advanced communication technology* (pp. 279-284). IEEE. https://doi.org/10.23919/ICACT.2019.8701960

Jelassi, T., Martínez-López, F. J., Jelassi, T., & Martínez-López, F. J. (2020). The strategic approach of the world's biggest e-Tailing companies: Amazon and Alibaba. *Strategies for e-Business: Concepts and Cases on Value Creation and Digital Business Transformation* (pp. 467-500). Springer. https://doi.org/10.1007/978-3-030-48950-2_16

Jha, R. K. (2023). Cybersecurity and confidentiality in smart grid for enhancing sustainability and reliability. *Recent Research Reviews Journal*, *2*(2), 215-241. https://doi.org/10.36548/rrrj.2023.2.001

Juniper Research. (2022, August). *Online payment fraud losses to exceed $206 billion over the next five years; driven by identity fraud*. https://www.juniperresearch.com/press/online-payment-fraud-losses-to-exceed-343bn/

Kala, E. M. (2023). The Impact of cyber security on business: How to protect your business. *Open Journal of Safety Science and Technology*, *13*(2), 51-65. https://doi.org/10.4236/ojsst.2023.132003

Karthick, S. (2019). PayPal-online payment method on online shopping. *International Journal of Research and Analytical Reviews*, 6(2). 153-164.

Kassab, W. A., & Darabkh, K. A. (2020). A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. *Journal of Network and Computer Applications*, *163*, 102663. https://doi.org/10.1016/j.jnca.2020.102663

Kavitha, S., & Ramajayam, V. (2021). Emerging trends of e-business: few challenges and advantages. *Nveo-Natural Volatiles & Essential Oils Journal NVEO*, 8(4), 6581-6587.

Kedah, Z. (2023). Use of e-commerce in the world of business. *Startupreneur Business Digital SABDA Journal*, *2*(1), 51-60. https://doi.org/10.33050/sabda.v2i1.273

Kim, J.-Y., Bu, S.-J., and Cho, S.-B. (2018). Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders. *Information Sciences*. *461*, 83–102. https://doi.org/10.1016/j.ins.2018.04.092

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. https://doi.org/10.3389/fpsyg.2022.927398

Llopis-Albert, C., Rubio, F., & Valero, F. (2021). Impact of digital transformation on the automotive industry. *Technological Forecasting and Social Change*, *162*, 120343. https://doi.org/10.1016/j.techfore.2020.120343

Luo, S., and Choi, T. (2022). E-commerce supply chains with considerations of cyber-security: Should governments play a role? *Production and Operations Management*. *31*, 2107–2126. https://doi.org/10.1111/poms.13666

Metinko, C. (2022, January 6). *Cybersecurity venture funding surpasses $20B in 2021, fourth quarter smashes record.* Crunchbase News. https://news.crunchbase.com/news/cybersecurity-venture-funding-2021-record/

Mhaskar, N., Alabbad, M., & Khedri, R. (2021). A formal approach to network segmentation. *Computers & Security*, *103*, 102162. https://doi.org/10.1016/j.cose.2020.102162

Mugarza, I., Flores, J. L., & Montero, J. L. (2020). Security issues and software updates management in the industrial internet of things (Ilot) era. *Sensors*, *20*(24), 7160. https://doi.org/10.3390/s20247160

Musonera, E. (2021). Strategic marketing case analysis: Starbucks. *Journal of Business and Social Science Review*, *2*(11), 12-22. https://doi.org/10.48150/jbssr.v2no11.2021.a2

Nagle, T., Sammon, D., & Cleary, W. (2019). A new approach to business value driven planning for data projects. https://doi.org/10.31219/osf.io/jg4pr

Neykova, M., & Miltchev, R. (2019). Conceptual approach to introduce an integrated model improving SMEs e-business technologies. *Management Theory and Studies for Rural Business and Infrastructure Development*, *41*(3), 381-399. https://doi.org/10.15544/mts.2019.31

Pan, X., Yamaguchi, S., and Kageyama, T. (2021). Machine-learning-based white-hat worm launcher adaptable to large-scale IoT network. *2021-10th Global conference on consumer electronics* (pp. 283–286). IEEE. https://doi.org/10.1109/GCCE53005.2021.9621895

Radu, R., Săndescu, C., Grigorescu, O., & Rughiniş, R. (2020). Analyzing risk evaluation frameworks and risk assessment methods. In P. Gasner (Ed.), 2020-*19th RoEduNet Conference: Networking in education and research (pp.*1-6). IEEE. https://doi.org/10.1109/RoEduNet51892.2020.9324879

Rodríguez, G. E., Torres, J. G., Flores, P., & Benavides, D. E. (2020). Cross-site scripting (XSS) attacks and mitigation: A survey. *Computer Networks*, *166*, 106960. https://doi.org/10.1016/j.comnet.2019.106960

Sahoo, K. S., Panda, S. K., Sahoo, S., Sahoo, B., & Dash, R. (2019). Toward secure software-defined networks against distributed denial of service attack. *The Journal of Supercomputing*, *75*, 4829-4874. https://doi.org/10.1007/s11227-019-02767-z

More than 15.1 billion records exposed in 2019. (2020, February 13). Security Magazine. Retrieved November 11, 2022, from https://www.securitymagazine.com/articles/91728-more-than-151-billion-records-expose_d-in-2019

Shah, J. N., Shah, J., & Shah, J. (2020). Quarantine, isolation and lockdown: in context of COVID-19. *Journal of Patan Academy of Health Sciences*, *7*(1), 48-57. https://doi.org/10.3126/jpahs.v7i1.28863

Shah, R., & Correia, S. (2021). Encryption of data over HTTP (hypertext transfer protocol)/HTTPS (hypertext transfer protocol secure) requests for secure data transfers over the internet. *2021 International conference on recent trends on electronics, information, communication & technology* (pp. 587-590). IEEE. https://doi.org/10.1109/RTEICT52294.2021.9573978

Sharma, N., Oriaku, E. A., & Oriaku, N. (2020). Cost and effects of data breaches, precautions, and disclosure laws. *International Journal of Emerging Trends in Social Sciences*, *8*(1), 33-4. https://doi.org/10.20448/2001.81.33.41

Sintaro, A. T., & Komolafe, Y. E. (2021). SDP And VPN For Remote Access: A Comparative Study and Performance Evaluation.

Taherdoost, H. (2023). E-Business Security and Control. In H. Taherdoost (Ed.), *E-business essentials: Building a successful online enterprise* (pp. 105-135). Springer. https://doi.org/10.1007/978-3-031-39626-7_5

Tavera Romero, C. A., Ortiz, J. H., Khalaf, O. I., & Ríos Prado, A. (2021). Business intelligence: business evolution after industry 4.0. *Sustainability*, *13*(18), 10026. https://doi.org/10.3390/su131810026

Information Systems. (n.d). Toyota Global. Retrieved June 20, 2023, from https://www.toyota-global.com/company/history_of_toyota/75years/data/company_information/personnel/information_systems/business_data_processing_systems.html

Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., and Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today Proceedings*. *51*, 2172–2175. https://doi.org/10.1016/j.matpr.2021.11.121

West, T., & Zentner, A. (2019). Threats and major data breaches: Securing Third-party vendors. *Available at SSRN 3532024*. http://dx.doi.org/10.2139/ssrn.3532024

Xiao, F., Sun, Y., Du, D., Li, X., and Luo, M. (2020). A novel malware classification method based on crucial behavior. *Mathematical Problems in Engineering*. *2020*, 1–12. https://doi.org/10.1155/2020/6804290

Xu, J., & Gao, X. (2021). Overview and foundation of e-business. In J. Lu (Ed.), *E-Business in the 21st Century: Essential Topics and Studies* (pp. 1-28). Intelligent Information Systems. https://doi.org/10.1142/9789811231841_0001

Zebari, R. R., Zeebaree, S. R., Jacksi, K., & Shukur, H. M. (2019). E-business requirements for flexibility and implementation enterprise system: A review. *International Journal of Scientific & Technology Research*, *8*(11), 655-660. https://www.researchgate.net/publication/337404049_E-Business_Requirements_for_Flexibility_and_Implementation_Enterprise_System_A_Review

Zhu, Z., Zhao, J., & Bush, A. A. (2020). The effects of e-business processes in supply chain operations: Process component and value creation mechanisms. *International Journal of Information Management*, *50*, 273-285. https://doi.org/10.1016/j.ijinfomgt.2019.07.001