IMPACT OF CYBERSECURITY ON DIGITAL BUSINESS IN SAUDI ARABIA & GLOBALLY

Bader Aldossary, Imam Abdulrahman Bin Faisal University
Abdulaziz Al-Towairqi, Imam Abdulrahman Bin Faisal University
Hussam Alomari, Imam Abdulrahman Bin Faisal University
Mahmud Maqsood, University of Bahrain
Hoda Mahmoud AboAlsmh, Imam Abdulrahman Bin Faisal University
Ibrahim Tawfeeq Alsedrah, Imam Abdulrahman Bin Faisal University
Zahra Afridi, Imam Abdulrahman Bin Faisal University

ABSTRACT

Cybersecurity is becoming an urgent requirement that requires our immediate attention in today's digital environment. Protecting systems, networks, and programs from cyberattacks is the practice of cybersecurity. These hacks typically try to disrupt regular corporate operations, extort money from users through ransomware, or access, alter, or delete important information.

The Saudi Arabian government recognized the importance of having a safe and reliable national cyberspace as a critical enabler for development and prosperity. The expansion of technology use also creates new opportunities for cyber threats, necessitating the improvement of cybersecurity to secure networks, information technology systems, industrial control systems, and operational technologies, as well as the hardware and software that make up those systems. Along with providing a secure and reliable infrastructure that supports government services and the digital transformation, data and services must also be secured from cyber threats and dangers like amendment, disruption, illegal use, and exploitation.

The National Cybersecurity Authority (NCA) was created by the Saudi Arabian government to be the governmental organization in charge of the nation's cybersecurity and to act as the national authority on those matters. In 2017, a Royal Order formed the NCA. The NCA works closely with public and private organizations to strengthen the nation's cybersecurity posture in order to protect its vital interests, national security, critical infrastructures, high-priority sectors, and government services and activities in line with Vision 2030. The NCA has both regulatory and operational responsibilities related to cybersecurity.

This report will focus on the following:

- *The history of cybersecurity and criticality in the new digital era.*
- *Digital transformation impact on cybersecurity.*
- *Digital risk management and cybersecurity.*
- *The role of the Saudi National Cybersecurity Authority (NCA).*

Keywords: Cybersecurity, computer, Digital Business.

INTRODUCTION

As the computer was developed in the 1940s, there were limited ways to access the computers. In addition, there was no interconnection between computers to transfer files and data. However, in the late 1940s, some theories about viruses were developed. John von

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.

Neumann believed that some mechanical organism could be developed that affects the machine (khurpaderushi, 2022). In the 1950s, hacking was developed although it was not possible to collect data from the computer by hacking.

In the early 1960s, various computer innovations were developed. The hacking of computers developed during this decade. Although hacking during that time was to gain access to the system without the intention of collecting information. MITS Altair 8800 became one of the first computers that could be connected to other computers over a telephone line (khurpaderushi, 2022). This allowed hackers to break into other people's computer systems. This became the turning point in developing cybersecurity strategies. In the 1970s, Cybersecurity was developed, and it started with the Advanced Research Projects Agency Network (ARPANET) project. This project was developed to connect various universities and research centers across the United States. This allowed researchers to share information and collaborate on projects.

In the 1980s, there were several computer viruses created. These viruses were designed to spread through computer networks. They could damage or disable computers and data files. In the 1990s, there was a rise in cybercrime. This refers to the crimes that are committed through the use of computers and computer networks. Cybercrime can include stealing personal information, attacking websites, and other criminal activities (khurpaderushi, 2022).

From the 2000s to now, computer growth has been effective and ready in homes and offices, increasing cybercrime's threats and risks. Various threats have occurred since 2000, including hacking of various information, including credit cards. Cybersecurity is a growing field that protects computer networks and electronic systems from unauthorized access, use, or destruction. Cybersecurity aims to ensure that critical information is protected and systems are not compromised.

The criticality of Cybersecurity in the new digital era has become increasingly apparent as cybercrime has evolved into an ever-growing threat. In the past, attacks were primarily conducted by criminal organizations and governments to steal data or resources for their gain. However, today's cybercrime threats are much more sophisticated and can take many forms, including attacks on businesses, governments, and individuals (Ram, 2021).

Cybersecurity has become critical in digital business as it protects sensitive information such as social security and bank information. Governments globally focus on establishing strong cybersecurity awareness to protect citizens from cyber threats. As a result, Cybersecurity has become increasingly important. Organizations must have a comprehensive plan to protect their data and systems from attacks and be prepared to respond quickly and decisively if an attack occurs. In addition, businesses must be aware of how cybercriminals can exploit vulnerabilities in their systems to steal data or money.

In addition, Cybersecurity is becoming critical in the digital business as it enables the business to prevent breaching issues that could have negative impacts. To protect sensitive data, organizations must put in place a comprehensive cybersecurity plan that includes appropriate authentication and password management practices, as well as monitoring of network traffic (Ram, 2021). Cybersecurity is more important than ever, as cybercriminals constantly develop new ways to steal data and money. A strong cybersecurity plan & system enables the business and the organization to prevent the breaching of important information.

Additionally, effective Cybersecurity drives potential business decisions. The business objectives rely on the business markets that rely on technological solutions—having inappropriate cybersecurity results in losing important information for the company, adversely impacting the business (Ram, 2021). The companies need to ensure effective management

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.

practices and resilience against cyber threats are addressed, and the business values are improved by integrating effective approaches that address the problem.

Digital Transformation Risks

The digital age has revolutionized how businesses operate. Technology has allowed for a more fluid and instantaneous connection to customers and partners and the ability to conduct business globally with reduced costs. New digital technologies and data analysis are greatly changing the expectations of the organization's employees, customers, and stakeholders. Due to increased reliance on digital technologies and systems, businesses are increasingly susceptible to cyberattacks (Rivera, 2022). Cybersecurity threats can come from various sources, such as malicious insiders, external factors such as hackers, accidental events & social engineers.

Organizations must take a holistic view of their security posture to mitigate the risks of digital transformation and cybersecurity threats. They must deploy a comprehensive security strategy cybersecurity that includes risk assessment, the technology organization's selection, environment, monitoring from and the detection, data incident center response to and the recovery, mobile and mobile devices post-breach and remediation (Rivera, 2022). With increasing digital transformation, organizations rely on third parties to power initiatives such as IoT and robots to generate information and data. Consequently, these organizations must also have strong data governance and compliance policies to protect their proprietary data.

Cybersecurity has transformed effectively, which has influenced how the business operates. The organization needs to implement Cybersecurity that enhances the organization's security. As globalization increases, digital transformation plays an effective role in shaping the business. Digital transformation enables organizations to mitigate the risks and threats they face in the business. In addition, digital transformation help business in preventing data breaching and crucial information.

Digital Risk Management and Cybersecurity

The digital transformation is becoming huge and fast therefor every business and country around the world have to use the new technology and adopt to the new digital technologies and as more they will use the new technologies as more they will face new risks and threats as digital attackers and hackers, therefor the government and organization found it important and give more attention to the Digital Risk Management and Cybersecurity, and they cannot ignore the new digital transformation because it is easier for the government to automate the information, provide and improve the services, increase the quality of operations which lead to increase the happens and increase the quality of their citizen life's, also for the employee to make their work easier and faster and the citizen to make their government services easier and anywhere and at any place, also the organization to continue in the market they have to follow and innovate and to gain more growth all of them have to be digitized and use the new technology, from their there became the need to the Digital Risk Management and Cybersecurity.

In recent years, digital security threats and incidents have increased, leading to Significant economic and social impact on public and private organizations and individuals. Some examples are failures through denial of service or sabotage, direct financial loss, litigation, reputational damage, loss of competitiveness and loss customer trust. More and more stakeholders realize the need Better manage digital security risks to capitalize on the digital economy.

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.

The occupied change to the digital transformation has high priority to the government and the organizations especially at the covid-19 pandemic that make it necessary to do that transformation at the telecommunication and information technology through online education, government meetings and conferences around the world, therefor the countries and organization that build a strong infrastructure is the most successful to adapt during the pandemic period and after by creating a value and use the best resource and to stay competitive, but with all of these advantages there are a huge technological risks.

To evaluate the digital risk management, we have to analyze the systems and determine the potential threats and the probability of every threat to be happen and how to deal with it when it happens and how to prevent this threat from happening.

Digital Risk Management Assessment

Digital risk management Figure 1 refers to the digital process of improving risk assessment and monitoring-which include cybersecurity risk, third-party risk, operational risk, technological risk, privacy risk, Data Leakage, Regulations risk and anonymity risk.

These risks may affect the government and company's financial performance, operations, or reputation.

FIGURE 1
DIGITAL RISK MANAGEMENT SYSTEM

The Cybersecurity Risk

There is huge risk as cybersecurity and the systems that connected to a high-risk element that is more improved which will make the cyberattacks to be a high risk to the government and the organizations, Protect the digital environment Use and Protection of Unauthorized Access Confidentiality and Integrity of Technology system. Critical controls may include platforms Hardening, Network Architecture, Application Security, Vulnerability Management and Security monitor.

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.

Privacy Risk

To protect the privacy in the digital world is becoming so hard and to protect the information's and the identity of the government information is one of the biggest risks that facing the government today, the risk of the privacy appears because we are dealing with personal, sensitive, and secured information's for the government, employees and citizens which will impact the privacy and security of the government, employees, and citizens.

Third Party Risk

Third party are those who will be participated from outside the organization or government employee and they are important to expand the resource and get better technology to your system or your supply demand so the government cannot leave them out of the context but the must be evaluated and assess their participation to face their risk and get the best participation and available resources.

Data Leakage Risk

The data is one of the most important factors at the digital transformation for government and any organization but also one of the biggest risks therefore government and organization nowadays must make sure and give huge attention to protect their data and information and how they will classify, write, process, save, encrypt, and secure their data.

Operations Risk

The operations of every government or an organization will involve how to do this operation in the digital transformation and it will lead to invisible risk that will lead to a high risk and challenges that will affect the government and the whole community.

Any operation will have impact to the ability of the government or an organization to complete the business or the operation itself should be secured and has its own procedure to be highly secured from risks.

Regulations Risk

The regulations risk in every government or organization while they are applying the digital transformation should be highly evaluated Compliance with legal requirements, including technology laws, sectoral laws, and regulations. This includes the regulatory universe of electronic communications and transactions. This is a general application and sector-specific regulation that includes financial services, insurance, and health insurance to the extent applicable.

Technological Risk

As more the technology helped the government and organizations to apply the digital transformation and to make everyone life easier but also it is coming with high and huge risk Possible loss due to technology error or old technology, risks related to technology affect systems, people, and processes. Key risk areas may include scalability, compatibility, and functional accuracy of his technology implemented.

Anonymity Risk

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.

The digital transformation and the new technology make it easy to the attackers or hackers to cover their identity and stay uncovered and this is a high risk to the government and organization to find those who attack the systems or the community therefor the government have to secure their data and systems from those individual and improve their employees to prevent this from happening and make the community aware about this threats.

Dealing with Digital Risk

FIGURE 2
DEALING WITH DIGITAL RISK

Keep the risk: If we can deal with risk and we can manage to handle these threats when it's happen then we will keep the risk and we will deal with it if its happen and control at.

Prevent the risk: We have to prevent the risk that will make a lost or damage which is high risk and because it is hard to be dealing with its huge risk the government or organization have to prevent this kind of risk from happening rather than spending her resources in correcting the process when it happens.

Transfer the risk: If the government or the organization can take some actions or procedure that will lead to reduce the lost from the digital transformation.

Review, update and evaluate the risk: In this rapid digital world, the risk is updated and developed every period so the government and organization should always review and test their system and evaluate the new risk and how to prevent them from happening Figure 2.

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.

Approach to Establish Effective Risk Management in Digital Transformation

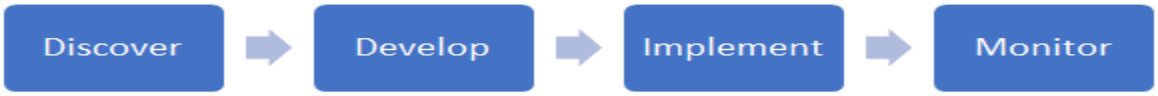

FIGURE 3
APPROACH TO ESTABLISH EFFECTIVE RISK MANAGEMENT IN DIGITAL TRANSFORMATION

Discover: The government and organizations should first discover the risks that facing its digital transformation and analyze every possible risk they might face during the transformation and after.

Develop: After discovering the potential risks that might face the digital transformation, we have to develop an effective way to prevent this risk from happening to the environment of the digital transformation.

Implement: After we develop the way, we will prevent the risk we have to implement the system or the protocol to prevent any risk from happening by implementing the correct secured Risk Management.

Monitor: Establish a continuous process through the risk management to monitor and evaluate the new risk and how the implementation of the risk management is working and how it is updated to reduce and prevent the new risk from happening Figure 3.

National Cybersecurity Authority (NCA)

NCA was created by the Saudi Arabian government to be the governmental organization in charge of the nation's cybersecurity and to act as the national authority on those matters (NCA). In 2017, a Royal Order formed the NCA (NCA). The NCA works with public and private organizations to strengthen the nation's cybersecurity posture to protect its vital interests, national security, critical infrastructures, high-priority sectors, and government services and activities in line with Vision 2030. The NCA has both regulatory and operational responsibilities related to cyber security (NCA).

Why NCA is Important

A security threat is a potential cause of an unwanted event that may damage systems or networks. Attacks on networks and computers are becoming more commonplace in today's society due to the increased number of devices linked to the internet (Alelyani & Kumar, 2018). Computers that are connected to the internet are exposed to worms, viruses, and hacker attacks. These attacks or threats could endanger the security of individual users, organization users, or entire nation security. The United States economy, according to Barack Obama, the 44th president, is dependent on cyber security. Therefore, it has become extremely important to combat these computers and network threats (Alelyani & Kumar, 2018).

Cyberattacks on the Middle East

In the Middle East, the Stuxnet attack on the Iranian nuclear facilities in 2009 triggered the cyberattack. With the Stuxnet attack, nations worldwide discovered how vulnerable

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.

infrastructures were to cyberattacks and how disastrous the potential repercussions could be (Baezner, 2018). As a result, Duqu, a malware, was employed in Iran and Sudan in 2011 to collect data from several targets that may potentially be used in future cyberattacks. Another malware known as Flame, which used the same design as Stuxnet, attacked the Iranian oil ministry and national oil company in 2012. The second largest producer of liquid natural gas in Qatar, Ras Gas, a corporation with a base in Qatar, was infected by malware. A group of hacktivists named "Parastoo" began attacking Israel's public targets in September 2012 and September 2013 in September 2012 to assist Iran's nuclear program. In 2015 Duqu 2.0 victims were discovered in many locations in the Middle East (Zetter, 2015).

Cyberattacks on the Kingdom of Saudi Arabian

Saudi Arabia witnessed a series of cyberattacks in the past few years due to its economic and political positions. Shamoon is a very harmful malware called a wiper. Malware that erases hard drives is categorized as wipers (Alelyani & Kumar, 2018). Normally, deleted data cannot be recovered so far, Shamoon has been the most well-known wiper (Alelyani & Kumar, 2018). Shamoon launched the initial attack on August 15, 2012, with Saudi Aramco as the intended target. Saudi Aramco (Saudi Arabian Oil Company) is a state-owned company responsible for oil exploration, production, and refining. The market value of Aramco has been estimated at up to $10 trillion, making it the world's most valuable organization. Threats against Aramco can put Saudi Arabia's national security in danger. Aramco needed over two weeks to repair the damage (Alelyani & Kumar, 2018).

Shamoon 2.0 is a newer version of it that has additional functionality Figure 4. Shamoon 2.0 initially targeted the KSA on November 17, 2016, then again on November 29, 2016, and then again on January 23, 2017. 15 public and private organizations had been affected by Shamoon 2 these organizations in Saudi Arabia were from several essential industries (Trouble, 2017).

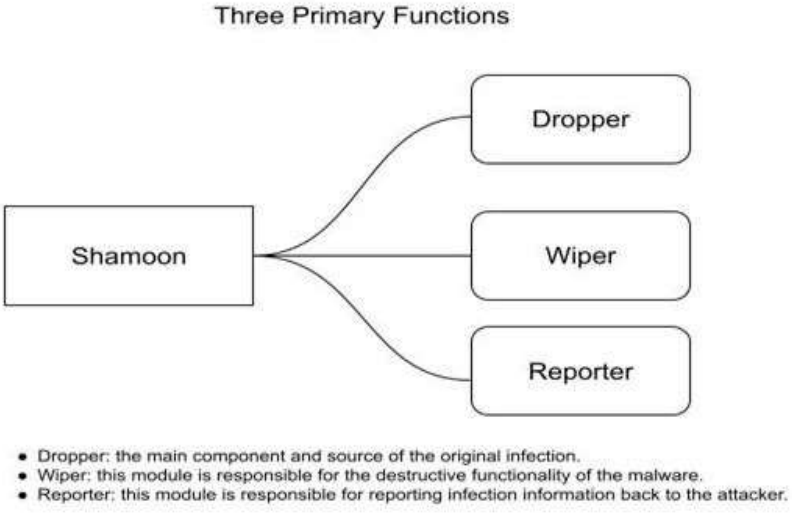

FIGURE 4
SHAMOON 2.0 FUNCTIONALITY

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.

NCA Role

The goal of NCA is the protection from unauthorized hacking, obstruction, modification, access, use, or exploitation of information technology systems and networks, as well as elements of operating technologies, which include hardware and software, with the services provided (NCA). The NCA has an overall national authority that includes, but is not limited to, developing the national strategy for cybersecurity and directing its implementation, establishing cybersecurity frameworks, controls, and compliance, establishing and running cybersecurity operation centers, building and operating cybersecurity awareness campaigns, improving the development of human ability in cybersecurity, and promoting the growth of the cybersecurity industry and encouraging innovation and investment and building connections with equivalent organizations abroad and with private organizations to share information and experience in cybersecurity (NCA) Figure 5.

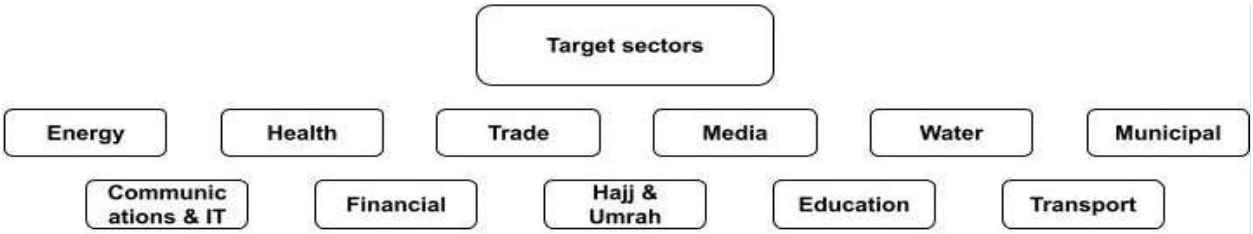

FIGURE 5
TARGET SECTORS

NCA along with Vision 2030

The Kingdom Vision 2030 aims to enhance overall the country and its security. One of the main objectives of the Vision is the transformation into the digital world and constant improvement of the digital infrastructure to keep up with the fast global progress in digital services, renewable networks, and IT systems, along with improved computer processing, massive data storage, and data exchange capabilities, to be ready to handle artificial intelligence and (NCA).

Cybersecurity Guidelines for e-Commerce

NCA is responsible for creating and publishing cybersecurity regulations. The cybersecurity rules for e-commerce service providers and the cybersecurity guidelines for e-commerce consumers were subsequently released in collaboration with the Saudi E-Commerce Council (NCA).

E-commerce Consumers

After thoroughly examining numerous national and international cybersecurity e-commerce guidelines, related national initiatives, statistics, and regulatory requirements, as well as reviewing and utilizing cybersecurity best practices and analyzing prior cybersecurity incidents and consumer attacks, NCA developed the Cybersecurity Guidelines for E-commerce Consumers (NCA).

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.

Facts & Drivers

Approximately 58% of people in the Kingdom have purchased online at least once every three months, with an average annual expenditure of SAR 4,000. These figures are probably higher given the rising popularity of mobile applications like smartphone applications and the simplicity of online buying (NCA).

The ease of home deliveries, the time-saving advantages of e-commerce, the attractive Internet offers, and the large selection of goods available are the drivers behind the growth and adoption of e-commerce. However, this has created new types of threats.

Cybersecurity Guidelines for E-commerce Consumers

According to NCA

Protect Your E-commerce Accounts and Devices

a. Anti-virus software
b. Consumers must install antivirus software on all of their devices, especially those that they use for online shopping frequently. Use only official versions of antivirus software programs.
c. Different passwords
d. Shopping on multiple apps or websites requires using a different password for each. Additionally, to secure your online identity, change passwords frequently and never share them with anyone.
e. Create strong passwords
f. Avoid using common everyday words, personal information, and sequential numbers, and do not write it down additionally; make it as long and complicated as possible.
g. Additional verification
h. If available, Consumers should consider using additional verification mechanisms (such as email messages) offered by e-commerce apps or websites.
i. Update applications regularly
j. Keeping the operating system, antivirus, and all of the device's applications up to date.
k. Data back up
l. To prevent losing your data if the device you use for online shopping is infected with viruses, back up your data by copying it, for instance, to your computer or an external hard drive.

Security of E-commerce Transactions

a. Transactions review. Enable SMS notifications on your e-Wallet or credit card to receive notifications whenever there is an account transaction.
b. A dedicated credit card. If using multiple credit cards, use a dedicated one for e-commerce purchases, and use a low-limit card or a pre-paid one.
c. Security of electronic wallet. Make sure to use a strong authentication system to secure access to your e-Wallet. Consumer use of e-Wallets is growing, and as a result, threats involving these payment options are increasing.

Exercise Caution When Communicating Online for E-commerce

a. Protect account against spam. Activate your email's spam filter, inform your email provider right away if you receive any spam, and make an email account specifically for online shopping.
b. Use secure websites. Make sure the website's URL begins with (https ://) instead of (http ://) before entering any personal or financial information.
c. Using secure apps, devices & networks. Be wary of fake websites and apps. By, for instance, downloading apps from the official app stores. Avoid using public devices or Wi-Fi networks to complete online purchases, log onto social media, or enter your login information.

Limit Sharing Your Personal Information

a. Privacy policy Avoid using e-commerce services from companies whose policies enable the misuse of personal information.

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.

b. Permissions granted to apps Consider whether it is necessary to grant mobile apps or websites access to certain data and features on your device.

E-commerce Service Providers

E-commerce is seen as one of the objectives of the national transformation program, which supports the realization of the kingdom's 2030 vision. Saudi e-commerce spending estimation is SAR 26.8 billion in 2019, which makes it one of the largest e-commerce markets in the Middle East and North Africa (NCA).

Facts & drivers

26% of small and medium enterprises in the Kingdom sell their products on social media. Approximately 86% of online SMEs claim to have been actively selling online for three to five years (NCA).

The majority of Small office/Home office (SoHo) e-commerce service providers increase traffic and sales by using social media channels to connect with customers (NCA).

Cybersecurity Guidelines for E-commerce Service Providers

According to NCA

Protect Your Online Shopping Systems

a. Recognize your e-commerce technological resources. To protect your e-commerce systems, you must first identify the hardware and information that are essential to your operation. These are often the resources that are essential to the operation of your e-commerce business.
b. Use antivirus software. Use and keep up-to-date anti-malware software on all of the devices in your e-commerce ecosystem.
c. Update your software frequently across all devices. Keep all of your e-commerce hardware and software updated with security patches.
d. Use encryption on your website. Consider securing your e-commerce website with an encryption protocol. These procedures are a great approach to guarantee the security of any transactions made through your e-commerce website.

Reduce the Effects of Data Breaches

a. Make a data backup. Back up your important data, including customer, business, and social media data.

Protect any e-Commerce-Related Social Media Accounts you have

a. Verifying your social media accounts. Verify your social media accounts. The majority of social media platforms provide a clear indicator.

Defend Your Network

a. Use intrusion prevention systems (IPS) to protect the boundary of your network. These technologies are capable of spotting anomalies in network activity or unusual data traffic patterns that can point to someone trying to attack your systems.
b. Perform frequent penetration tests on your e-commerce systems and whenever there is a significant code update or system upgrade.

Train and Educate Your Staff Continually

a. Create and implement a cybersecurity policy that outlines what employees are permitted to and are not permitted to do when utilizing corporate networks. The policy should clarify the consequences employees would face if they violate it.
b. One of the most frequent places to find malware is unidentified programs. Employees should be instructed only to use business-related software and only to download it from trusted sources.

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.

Strengthen Your Internal E-commerce Infrastructure

a. Install a spam filter on your email server.
b. Require users to confirm by clicking the confirmation link in their email in order to prevent mass registrations.
c. Create a unique form and link if you plan to allow users to register on your website.
d. Use an anti-fraud software solution for e-commerce as this is thought to be a good approach to prevent attacks, including click fraud, mass registration, and inventory abuse.

RECOMMENDATIONS

The business impact of Cybersecurity is the potential for financial loss, reputational damage, or legal liability that could result from a security breach. Adopting effective cyber initiatives influence business operation in many ways, including improving data security and protection, enhancing communication and collaboration across teams, limiting the impact of cyberattacks, and reducing overall costs. In addition to these direct benefits, Cybersecurity supports organizational values and goals, promotes innovation, and strengthens overall business performance.

The theft of confidential information can have a devastating impact on businesses. Appropriate data protection exposes the business to potential fines from the government or consumers, loss of business reputation, and even legal action. Cybersecurity breaches can also lead to the exposure of confidential customer data, which can seriously impact the business. In extreme cases, cyberattacks could even lead to financial ruin for a business. Organizations that adopt effective cybersecurity measures can reduce these risks and improve their overall performance. Protecting their data can reduce the likelihood of a security breach. They can improve their ability to respond to and mitigate cyberattacks by implementing effective communication and collaboration mechanisms. This enables the organization to limit the impact of a breach and improve its overall business performance. Cybersecurity initiatives also promote innovation as businesses take measures to protect themselves from previously unknown threats.

Organizations can achieve Cybersecurity through data encryption, which helps protect the information from unauthorized access. Organizations can also use firewalls to protect their networks from attacks and monitor activity on their systems. They can also deploy anti-virus software and other anti-malware measures to protect their systems from malicious software. Also, they can use encryption to protect the data stored on their systems but most importantly companies should educate their employees to ensure the company is protected from the inside since they are the 1st line of defense when it comes to hackers or social engineers who try to break to steal or destroy companies' data.

CONCLUSION

Digital transformation and Cybersecurity influence business because they are two of the most important drivers of change in the business world. By implementing digital transformation, businesses can improve their ability to compete in a global economy. They can also improve their customer experience and ability to deliver new services. As businesses digitize their operations, they must also take measures to protect their data and systems from cyberattacks.

REFERENCES

Alelyani, S., & Kumar, H. (2018). Overview of cyberattack on saudi organizations.
Baezner, M. (2018). *Cyber and Information warfare in the Ukrainian conflict*, 1, 1-56.

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.

Khurpaderushi, J. (2022) *History of cyber security*, Geeks for Geeks.
Ram, A. (2021). *Cybersecurity is critical in the Digital Transformation Era*, *Times of India Blog*.
Rivera, V. (2022). *The business impact of Cybersecurity in 2022*, *Insight*.
Trouble, D. (2017). A pair of wipers in Saudi Arabia kaspersky lab blog.
Zetter, K. (2015). Kaspersky finds new nation-state attack-in its own network.

Received: 10-Nov-2022, Manuscript No. AJEE-22-12840; **Editor assigned**: 14-Nov -2022, Pre QC No. AJEE-22-12840(PQ); **Reviewed**: 28-Nov-2022, QC No. AJEE-22-12840; **Revised**: 05-Dec-2022, Manuscript No. AJEE-22-12840(R); **Published**: 12-Dec-2022

Citation Information: Aldossary, B., Al-Towairqi, A., Alomari, H., Maqsood, M., AboAlsmh, H.M., Alsedrah, I.T., & Afridi, Z. (2023). Impact of Cybersecurity on Digital Business in Saudi Arabia & Globally. Journal of Entrepreneurship Education, 26(S2), 1-13.