DIGITAL TRANSFORMATION VULNERABILITIES: ASSESSING THE RISKS AND STRENGTHENING CYBER SECURITY

Calin Alexandru SERAC

Department of Economics and Business, Faculty of Economic Sciences, University of Oradea, Oradea, Romania
serac.calinalexandru@student.uoradea.ro

Abstract: *Digital transformation has revolutionized the way organizations operate, enabling them to leverage advanced technologies for increased efficiency and productivity. However, along with the benefits, digital transformation also brings new vulnerabilities and risks, particularly in the realm of cybersecurity. This abstract aims to provide an overview of the vulnerabilities associated with digital transformation and highlight the importance of assessing risks and strengthening cybersecurity measures to mitigate potential threats.*

The rapid adoption of cloud computing, Internet of Things devices, and interconnected systems has expanded the attack surface for cybercriminals. Organizations must recognize the potential vulnerabilities introduced by these technologies, such as data breaches, system failures, and unauthorized access. Understanding the specific risks associated with digital transformation is crucial for developing effective cybersecurity strategies.

Assessing risks involves evaluating the organization's digital infrastructure, identifying potential weak points, and determining the likelihood and potential impact of various threats. This process enables organizations to prioritize cybersecurity efforts and allocate resources effectively. It also involves evaluating the security measures in place, including firewalls, intrusion detection systems, encryption protocols, and employee training programs, to ensure they are up to date and resilient against emerging threats.

Strengthening cybersecurity requires a multi-layered approach that encompasses technical measures, organizational policies, and a culture of security awareness. Implementing robust security controls, such as regular software updates, network segmentation, and access controls, helps fortify digital systems against attacks. Additionally, establishing incident response plans and conducting regular security audits aids in identifying vulnerabilities and responding swiftly to cyber incidents.

Furthermore, fostering a culture of cybersecurity awareness among employees is essential. Educating staff on best practices, such as strong password management, phishing awareness, and safe browsing habits, empowers them to become the first line of defence against cyber threats.

Keywords: *digital transformation vulnerabilities, data breaches, cyber threats, cyber security.*

JEL Classification: O30

1 Introduction

Digital transformation has brought about a revolution in the way businesses operate, changing the way companies interact with their customers, employees, and partners. The adoption of digital technologies has led to the creation of new business models, improved efficiency, and better decision-making capabilities. However, with these benefits come new risks and vulnerabilities that organizations must be aware of to protect themselves from cyber threats.

As organizations continue to embrace digital transformation, the dependence on digital infrastructure grows. This dependence makes organizations vulnerable to cyber threats, including ransomware attacks, data breaches, and other malicious activities. The reliance on digital infrastructure also increases the attack surface for cybercriminals, making it easier for them to launch attacks on organizations. Also, digital transformation may lead to a change of the organizational culture. While the innovation and new technologies adoption may be efficient for the companies, they can also create stress among the people in the organization.

2 Literature

In today's digital age, cybersecurity is a growing concern for individuals and organizations alike. With the rise of cybercrime, it has become increasingly important to assess the risks associated with cybersecurity and take measures to strengthen it. This literature review aims to explore the latest research on assessing the risks and strengthening cybersecurity.

Assessing the Risks

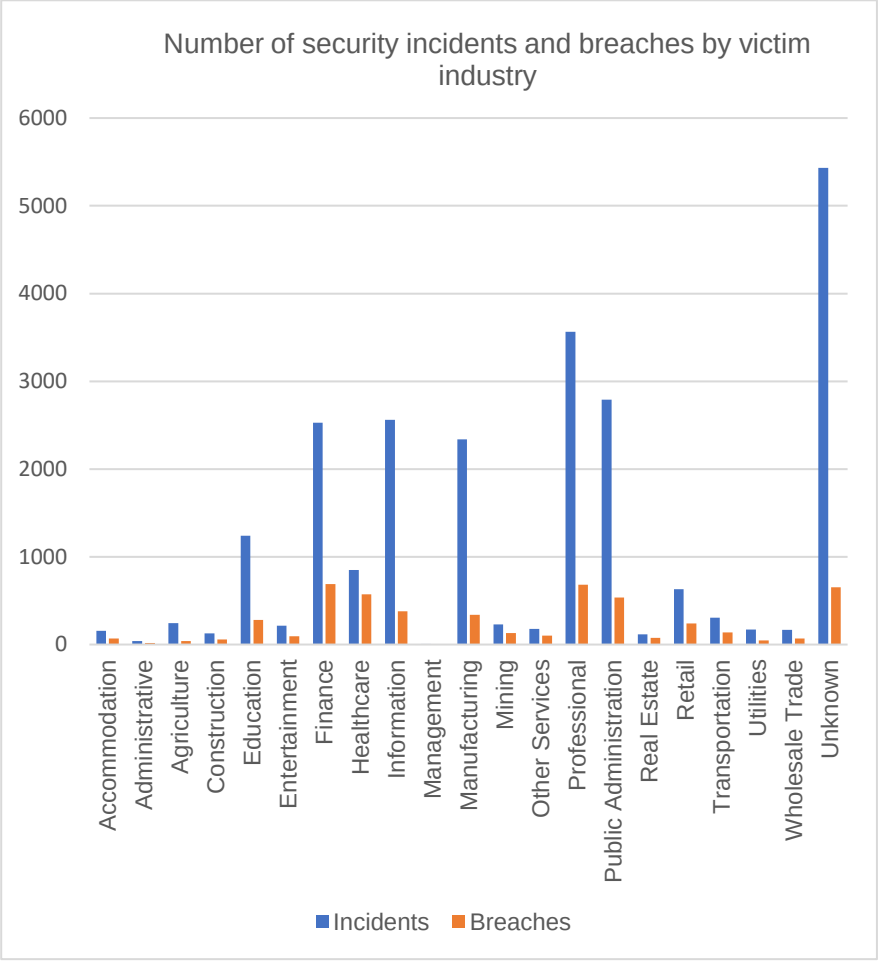
Assessing the risks associated with cybersecurity and taking measures to strengthen it is critical in today's digital age. According to a study by Böhme et al. (2010), risk assessment involves identifying the assets at risk, the potential threats, and the vulnerabilities of the system. This can be achieved through various methods, such as conducting a risk assessment survey, performing vulnerability scanning, and penetration testing. Several tools, such as the Common Vulnerability Scoring System (CVSS) and the Open Web Application Security Project (OWASP), can also be used to assess the risks associated with cybersecurity.

Various methods, such as risk assessment surveys, vulnerability scanning, and penetration testing, can be used to assess the risks associated with cybersecurity.

Additionally, implementing frameworks such as NIST and strategies such as DiD, and utilizing advanced technologies like AI, ML, and blockchain can help to enhance cybersecurity. This literature review highlights the importance of assessing risks and implementing measures to protect against cyber threats.

Methods of research

Verizon's annual cyber-attack studies, known as the "Verizon Data Breach Investigations Report" (DBIR), provide valuable insights into the cybersecurity landscape. Comprehensive Data Analysis: The DBIR leverages a vast dataset collected from various sources, including Verizon's own investigations, partner organizations, and contributors from around the world. This comprehensive approach provides a holistic view of cyber threats and trends. Global Perspective: The studies cover a wide range of industries and sectors, offering a global perspective on cyber-attacks. This includes data from organizations of all sizes, from small businesses to large enterprises, across different regions. Industry-specific Insights: Verizon's DBIR often includes industry-specific breakdowns, highlighting unique challenges faced by various sectors. This allows organizations to gain sector-specific insights and tailor their security strategies accordingly.
Analysing the data (23,896 incidents and 5,212 breaches) provided by this report for the year 2022, we noticed that not all incidents turn into breaches, and from the table below that in some areas the number of incidents is exponentially higher than that of breaches, which indicates a higher security of the systems, but in other areas the number of incidents is comparable to that of breaches, which denotes a poor security of system (https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf).



A comprehensive approach to cybersecurity research can help organizations identify potential cyber threats and take measures to protect against them. Here are some methods of research for assessing the risks and strengthening cybersecurity:

Risk Assessment Surveys: A risk assessment survey is a method of research that involves collecting information about the organization's assets, vulnerabilities, and threats. The survey can be conducted in various forms, such as questionnaires or interviews, to identify potential cyber threats and their likelihood of occurrence.

Vulnerability Scanning: Vulnerability scanning is a method of research that involves using automated tools to scan networks, systems, and applications for known vulnerabilities. This method can help identify weak spots in an organization's cybersecurity infrastructure.

Penetration Testing: Penetration testing is a method of research that involves simulating cyber-attacks to identify potential vulnerabilities in an organization's infrastructure. This method can help identify potential weaknesses that could be exploited by attackers.

Framework Implementation: Implementing cybersecurity frameworks such as the NIST cybersecurity framework can be a method of research to assess and strengthen cybersecurity. This method involves using a framework to identify and prioritize cybersecurity risks and take measures to mitigate them.
Artificial Intelligence and Machine Learning: Using AI and ML to detect and respond to cyber threats in real-time can be a method of research for strengthening cybersecurity. This method involves analysing data to detect patterns and anomalies that may indicate cyber-attacks.
Blockchain Technology: Blockchain technology can be used as a method of research to enhance cybersecurity. This method involves using a decentralized and immutable ledger to provide a secure and tamper-proof record of transactions.
Analysis of Cybersecurity Incidents: Analysing past cybersecurity incidents can be a method of research to identify potential threats and vulnerabilities. This method involves reviewing incident reports to identify common patterns and trends in cybersecurity incidents.

Dependence on digital infrastructure and its vulnerabilities

The threat landscape is constantly evolving, and new cyber threats emerge daily. With the adoption of new technologies, the threat landscape is becoming even more complex, making it challenging for organizations to keep up. According to ENISA report for the period January 2019- April 2020 one can distinguish five tendencies to develop the attacks. Software protagonists are the malware ones in a variety of forms continuously updating and transforming themselves according to the targets, from mobile devices to personal devices used in remote working during the pandemic, ransomware which encrypt the files to blackmail, detected on employees' devices in the public sector but also in private companies and a consequence of the large amount of private stolen files, the report identifies credential stuffing attacks.
As the organizations keep the digital transformation, the digital infrastructure dependency increases and challenges the organizations to be vulnerable in terms of technology operation and human beings. This way, the attacks horizon is expanding, and it is launching a series of attacks upon the organizations and the control of these attacks becomes harder to achieve, the risks become harder to measure, and the costs become higher both from financial perspective and a human one. As a result of a deep measurement of the associated risks of digital transformation, specific to every company, these can identify the nature of the vulnerabilities to schedule the actions to decrease the risk that has a great impact on the organization. These pieces of information may be used to develop an extensive strategy of cybersecurity, the work

being ongoing because of the constant threats so, overtime there can be created a security culture inside the organizations, ideally having all the employees well prepared regarding the best drills for the cybersecurity.
Weak digital technologies that some of the companies use, as an outdated software, insecure networks, or a huge number of IoT devices, that is predicted to reach 41.76 billion devices all over the world until the ending of 2023 (increasing from 35.37 billion in 2022) according to Frost and Sullivan (2022), all these may become an easy to enter gateway for malware. The operational vulnerability of the companies comes from the weak points of their processes and procedures: easy to crack passwords, not enough access controls, or inadequate backups of the files. Human errors or poorly training of the staff play an important role in phishing actions or some ransomware or spyware programs entering. Deliberate actions of complaining staff in a company may bring a series of significant prejudices and this is again on of the vulnerabilities we have already mentioned, human ones.

3 Strengthening Cybersecurity

There are several strategies for strengthening cybersecurity that organizations can implement. One such strategy is the use of security controls, such as firewalls, intrusion detection systems, and anti-virus software. In their study Kuipers et al. (2021) found that security controls were a critical component of any cybersecurity strategy and could help to prevent or mitigate cyber-attacks.
Another approach is to implement the Defence in Depth (DiD) strategy, which involves implementing multiple layers of security controls to protect against cyber threats (Mishra et al., 2020).
In addition to these strategies, organizations can also use advanced technologies to strengthen their cybersecurity. For example, artificial intelligence (AI) and machine learning (ML) can be used to detect and respond to cyber threats in real-time. Blockchain technology can also be used to enhance cybersecurity by providing a decentralized and immutable ledger of transactions.
Another strategy for strengthening cybersecurity is employee training and awareness. This involves providing employees with training on how to recognize and respond to potential cyber threats, as well as implementing policies and procedures for data protection and access control.
To improve their cybersecurity, the organizations must adopt a proactive approach. This includes the implementing of the best procedures of cybersecurity, like login with two or more factors (2FA or MFA), regular software updates and training of employees. The most employed security systems are:

Firewall to prevent unauthorized access from outside the network by filtering the network traffic, set up on some predefined criteria, like IP address, network ports and the employed protocol. Firewall's purpose is to protect devices against unauthorized access from outside the network.

Endpoint Detection and Response (EDR) is a cybersecurity option that focuses on detecting and answering the threats on endpoints, like desktops, laptops, or servers, and analysing the activity on them. EDR may detect and prevent cyber-attacks by analysing signs of suspicious activity or unauthorized activity on their device. This also may include protective functions against cyber threats, like anti-virus, anti-malware, or anti-ransomware. An efficient system should probably include both a firewall and an EDR.

Another type of technology is Intrusion Detection System (IDS) that is detecting cyber-attacks through an analysis on network traffic. IDS are searching for unusual activity signals or unauthorized ones, like the attempt to access a system or to send files outside the network. This type of technology can be set up to generate a series of warnings when it is detecting suspicious activity, so that a series of actions can be performed to fight the attacks. IDS may be perceived as a preventing option, while EDR may be perceived as a responsive option, that can be used to fight the attacks that succeeded to pass IDS and reach the level of endpoints.

Another option is Security Information and Event Management (SIEM) that is collecting and analysing files from different sources, like system logs, security warnings and networking events, to identify types and signals of suspicious or unauthorized activity. This system may use AI algorithms or ML to prevent in real-time the threats and it can be integrated with firewall, EDR, or IDS technologies.

Virtual Private Network (VPN): A VPN is a network security system that allows remote workers to securely access a company's network. It creates a secure encrypted connection between a user's device and the company's network, ensuring that sensitive data is protected.

Cloud Security: Cloud security refers to the protection of data stored in cloud computing environments. It involves using various security measures, such as encryption and access controls, to ensure that data is secure and protected from unauthorized access.

Encryption solutions of storage and transmission technologies is used to protect digital data from being accessed or modified by unauthorized users. It involves converting plaintext into ciphertext using a mathematical algorithm and a secret key. Encryption plays a critical role in cybersecurity because it helps to protect sensitive information from being intercepted, stolen, or tampered with during transmission or storage.

There are several encryption solutions available for cybersecurity, including:
Symmetric encryption: This method uses a single key to both encrypt and decrypt data. The key is typically shared between the sender and the recipient and is kept secret to prevent unauthorized access. Symmetric encryption is fast and efficient, but the key must be securely exchanged between the sender and the recipient.
Asymmetric encryption: This method uses a pair of keys, one public and one private, to encrypt and decrypt data. The public key is shared with anyone who wants to send encrypted data, while the private key is kept secret by the recipient. Asymmetric encryption is slower than symmetric encryption, but it eliminates the need for secure key exchange.
End-to-end encryption: This method ensures that data is encrypted from the sender to the recipient and cannot be accessed by any third-party, including service providers. End-to-end encryption is commonly used in messaging apps, email clients, and other communication platforms.
Hashing: This method creates a fixed-length string of characters, known as a hash, that represents the original data. Hashing is commonly used to verify the integrity of data, as any changes to the original data will result in a different hash.
Digital signatures: This method uses a combination of hashing and asymmetric encryption to create a unique digital signature that can be used to verify the authenticity of a document or message.

There are a lot of options to be used at the same time for a more complex approach of the files, devices, and networks security. The prejudices of the cybercrime have been estimated in 2022 to 8.44 trillion USD opposing 1.16 trillion USD in 2019, and the estimates are reaching 24 trillion USD in 2027. International Cybersecurity services market is estimating that will be reaching 304.4 billion USD in 2027 facing a fast-increasing tendency, being double in comparison with 2020 when the value was little under 150 billion USD (https://www.statista.com/statistics/).
An example of a company that has implemented security systems in the products it offers to customers is the technological giant Apple, which offers both the software and the hardware the newest and most complex solutions.

Apple's macOS has several built-in security features that help to protect users and their data from various threats, including malware, phishing attacks, and other forms of cyber-attacks. Some of the key security features of macOS include:
Gatekeeper: This feature helps to prevent users from installing malicious software by restricting installations to apps from the App Store or from identified developers.
System Integrity Protection (SIP): This feature protects key system files and folders from being modified, even by users with administrator privileges. This helps to

prevent malicious software from hijacking system resources or installing system-level malware.
File Vault: This feature provides full-disk encryption for the Mac's hard drive, protecting all the user's data from unauthorized access.
Firewall: This feature blocks incoming connections to the Mac and helps to prevent unauthorized access to the user's network or system resources.
Safari: Apple's web browser includes several security features, including protection against phishing attacks, malware, and malicious websites.
Automatic security updates: macOS includes automatic security updates, which helps to ensure that users are always running the latest security patches and fixes for known vulnerabilities.
Touch ID and Face ID: On Macs equipped with Touch ID or Face ID, users can use biometric authentication to log in to their accounts, adding an additional layer of security.
The Security Enclave is a component of the Apple-designed M-series chipset used in Macs and iOS devices. It is a secure area of the processor that is designed to protect sensitive data such as biometric information (such as Touch ID and Face ID), encryption keys, and other sensitive data. The Security Enclave is a hardware-based solution that is isolated from the rest of the system, meaning that it is not accessible from any other part of the device. It has its own dedicated processor, memory, and storage, and is designed to perform security-related tasks in a highly secure and efficient manner. One of the key features of the Security Enclave is its ability to perform secure boot and verify the integrity of the operating system before it is loaded. This ensures that the system is running on a trusted and secure operating system, which helps to protect against various types of attacks. The Security Enclave is also responsible for managing the encryption keys used to encrypt sensitive data on the device. These keys are stored securely in the Enclave and are used to encrypt and decrypt data on the fly. This ensures that even if an attacker gains access to the device's storage, they will not be able to access the encrypted data without the encryption keys.
Overall, the Security Enclave is a critical component of Apple's security architecture, providing a highly secure environment for sensitive data and ensuring that the device is protected against a wide range of attacks.

4 Conclusion

Digital Transformation brought a lot of benefits for the organizations, but it also brought new risks and vulnerabilities. As the organizations keep up embracing of

digital transformation, it is highly important that they access the most current and complex security services to protect themselves against new and appropriate types of cyber-attacks, many of them being capable of passing security systems. The COVID-19 pandemic has accelerated the digitalization process, weakening at the same time remote working systems and the companies whose employees used work from home. The latest technological improvements like AI and ML changes the way in which organizations work and think, but it also emphasizes new challenges for the cybersecurity which deserves to be studied in the future. For example, how can cybercriminals use AI to create high-end attacks, and ML to automatize the attacks, situation that make detection and the answer of traditional security systems, difficult to deal with. All these things have happened in the last few years, this being the reason why the introduction of the most current security systems and permanent update can be the most efficient solution which organization might take into consideration, according to the type of activities they perform. Companies should pay special attention on cybersecurity, in a responsible way, and they should manage technological risks and they should focus also on the cultural changes that might occur inside the organization. Analysing the costs that have previously been mentioned, both the preventing and the possible prejudices companies might encounter, it becomes ever more clearly why cybersecurity solutions must be adopted.

References

1.Acosta, Ernesto C. Anti-virus strategies and their functions, CYSE 600, Cybersecurity Principles, 2019

2.Andrade, Norberto Nuno Gomes De, and Antonella Zarra. Artificial Intelligence Act: A Policy Prototyping Experiment: Operationalizing the Requirements for AI Systems part I (2022)

3.Böhme, Rainer; Félegyházi, Márk. Optimal Information Security Investment with Penetration Testing, Decision and Game Theory for Security pp 21-37, Springer 2010

4.Kuipers, S.L.; Schonheit, M. Data breaches and effective crisis communication: A comparative analysis of corporate reputational crises. Corporate Reputation Review. 2021

5.Lin, Iuon-Chang; Liao, Tzu-Chun. A survey of Blockchain Security Issues Ad Challenges, International Journal of Network Security, Vol. 19, No. 5, Pag. 653-659, 2017

6.Mishra, Sakshi; Anderson, Kate; Miller, Brian; Boyer, Kyle; Warren, Adam. Microgrid resilience: A holistic approach for assessing threats, idenifying vulnerabilities, and designing corresponding mitigation strategies, 2020, https://www.sciencedirect.com/science/article/abs/pii/S0306261920302385?via%3Dihub

7.Reis, Joao; Amorim, Marlene; Melao, Nuno; and Patricia Mato. Digital Transformation: A Literature Review and Guidelines for Future Research, h

https://www.researchgate.net/publication/323994364_Digital_Transformation_A_Literature_Review_and_Guidelines_for_Future_Research
8.Rong, Chunming; Nguyen, Son T.; Jaatun, Martin Gilje. Beyound lightning: A survey on security challenges in cloud computing, Computers & Electrical Engineering, Vol. 39, Issue 1, Pag. 47-54, 2013
9.Sebastian, Ina M.; Mocker, Martin; Ross, Jeanne W.; Moloney, Kate G.; Beath, Cynthia; Fonstad, Nils O. How Big Old Companies Navigate Digital Transformation, MIS Quarterly Executive, September 2017
10.Shaukat, Kamran; Luo, Suhuai; Varadharajan, Vijay; Hameed, Ibrahim A.; Xu, Min.
A survey on Machine Learning Techniques for Cyber Security in the Last Decade, https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2730527/Hameed%2C+Ibr.pdf?sequence=2
11.Soviany, Sorin; Puşcoci, Sorin; Pescaru, Gheorghiță; Dragomir, Radu. Sisteme de detecție a intruziunilor, https://www.agir.ro/buletine/726.pdf
12.Tripathi, Vaibhav; Dubey, Anmol; Sathvik, Kesari; Subhashini, N. A comparative Study of Machine Learning Algorithms for Anomaly-Based Network Intrusion Detection System , https://link.springer.com/chapter/10.1007/978-981-19-0745-6_2
13.Vey, Karin; Fandel-Meyer, Zipp; Tanja, Jan S.; Schneider, Christian. Learning & Development in Times of Digital Transformation: Facilitating a Culture of Change and Innovation, https://doi.org/10.3991/ijac.v10i1.6334
14.*** Tendințe emergente, Raport ENISA ian. 2019-apr. 2020, https://www.enisa.europa.eu/publications/report-files/ETL-translations/ro/etl2020-emerging-trends-ebook-en-ro.pdf
15. *** The top Growth Opportunities for IoT in 2023, https://www.frost.com/frost-perspectives/the-top-growth-opportunities-for-iot-in-2023/
16.*** https://www.statista.com/statistics/
17.***https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf