International Journal of Scientific Research and Management (IJSRM)
||Volume||10||Issue||06||Pages||EC-2022-871-880||2022||
Website: www.ijsrm.in ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v10i6.ec01

Security Challenges for Digital Transformation in Saudi Arabia

Khalid Almdani[1] , Hassan Al saeedi[2], Abdullah Softah[3], Sultan Khogeer[4] ,Khalid H Assiri[5]

[1,2,3,4,5] College of Computer Science and Engineering, University of Jeddah, Kingdome of Saudi Arabia
Jeddah, P.O.23218
Supervised By Dr. Abdulrahman Al Shdadi

Abstract
Saudi organizations are increasingly using digital technologies. Despite widespread efforts to benefit from digitalization, few companies can claim to have seen significant results. Organizational employees have been linked to the success or failure of the digitization process in a growing body of studies. Three hypotheses regarding the security of the digital transition have been suggested in this study. These hypotheses include determining how security has evolved because of the increased use of digital systems, as well as determining the best risk management strategies. A range of public and private Saudi entities will get an electronic survey as part of this study. In summary, we have found that as the digital transformation grows, the security risk increases as well, necessitating the implementation of a robust security system and the most effective risk management measures. Additionally, the business must include employees in the development and implementation of the digital transformation to maintain their loyalty. Additionally, all employees must understand and agree on the digital transformation goals, objectives, and plans. Successful business leaders can build a compelling vision, unite, and engage staff to adopt new methods of doing business

Keywords: Digital government, Digital transformation, e-Government, Cybersecurity.

Introduction

With the rapid advancement of technology and the trend of governments and institutions to digitize all of their services, the Kingdom of Saudi Arabia has been eager to adopt the concept of government digital transformation by replacing traditional processes with digital ones, and developing five-year plans and strategies to ensure the achievement of its goals with quality and efficiency, as it aspires to become an integrated digital government that facilitates the development of five-year plans and strategies. Sakr, T. (2021, October 9).

This digital transportation (DT) in Saudi araba was initiated by Saudi government as a one of the tools used to achieve the Saudi e-government which is aligned with Saudi vision 2030. Thus, the SA government have stablished many of agencies that supervises and control the process of the DT. Sakr, T. (2021, October 9).

The Government Authority (DGA) is the government agency that drives digital transportation in Saudi Araba. On March 9, 2021, equivalent to Rajab 25, 1442 AH, the Digital Government authority was founded by Cabinet Resolution No. (418). It is the competent authority in all matters relating to digital governance and the national point of reference in these matters. Its goal is to coordinate digital government activity inside government agencies in order to produce a proactive and proactive digital government capable of providing high-quality digital services, as well as to accomplish digital government integration across all government agencies. Sakr, T. (2021, October 9).

The term digital government refers to the use of digital technologies as an integral part of government strategies. It relies on a digital government system to support the production of services, content and data and access to them through interaction and integration between government agencies according to a set of principles and dimensions, and in the context of the strategic directions of the digital government, the digital government focuses on providing

information and communication technology, advanced technical systems, platforms and portals to build, improve and enable access Government information and services are effectively facilitated, high quality and secure, by enhancing community participation to support administrative, organizational and operational processes within government sectors and adopting innovative business models and flexible policies and standards that adapt to models of digital transformation and excellence. (Catch-22: Digital Transformation and its impact on, May 20, 2022)

In this article will identify the e-government security challenges in the Kingdom of Saudi Arabia in terms of digital transportation. Data privacy and cybersecurity in terms of digital transportation. As well as the best risk-mitigation practices, synchronized with digital transportation approaches. (Catch-22: Digital Transformation and its impact on, May 20, 2022)

Digital Transformation Challenges

Digital Transformation Development Planning.

The formulation of digital transformation plans, which need fresh and clear strategies for the transition to the digital economy, is one of the most challenging tasks facing the Saudi government. The construction and enhancement of institutions takes a lot of time, money, and effort, thus implementing these digital enterprises is technically expensive.

Lack of Appropriate Internal Skills and Experience.

Having internal skills and experience is very important, as traditional organized processes are slow due to the lack of operating skills, they cannot support digital transformation, and at the same time there are no proven and ready-to-operate business models as a result of the flight of competencies abroad due to high wages in foreign markets compared to Significant decline in the Saudi market. (Saudi Arabia National Portal, May 20, 2022)

Concerns About Data Privacy and Cybersecurity

Because of its reliance on the Internet and computer systems that store sensitive data about residents, the government confronts cyber security issues. There are several issues with cyber security, including:

Hacking crimes: where cybercriminals or hackers launched more complex attacks that target the violation of the main data of institutions, and with each attack costing these institutions millions, and with the increase in the number of those institutions that rely on technology, the number of such attacks will increase more. (Saudi Arabia National Portal, May 20, 2022)

Fraud crimes: Some hackers have created a group of programs that can transmit anonymous digital messages to some important people such as company owners and bank owners, which leads them to install some malware in order to obtain some important data and obtain information. (Saudi Arabia National Portal, May 20, 2022)

This article will focus on the security side in the digital transformation in Saudi Arabia, as well as identify the most significant risk in terms of DT, and the impact of the risk and how to mitigate it.

Literature Review

Digital transformation, often known as "digitalization," is a term that is rarely defined in today's literature. According to our findings, digital transformation is described as a social phenomenon or cultural evolution for individuals, and as the evolution or construction of a business model for enterprises. Indeed, it is considered as a major cultural shift, driven by "digital" generations whose culture and daily routines are heavily influenced by digital technology. Organizations must be able to adapt to this climate, either by altering or establishing a new business model. However, identifying digital Ptransformation as a business model is challenging and inadequate since it may affect other characteristics of an organization, such as culture and organizational structure. (Emily Henriette, 2016). Digital transformation is a dramatic reimagining of how technology may be used to change strategy, revenue streams, operations, and business models, with substantial implications for customers, partners, and workers. Aside from the technology, digital transformation entails transforming three major elements of an organization: customer experience, operational procedures, and business models. It may be extremely basic to define it as a specific project with a commencement phase, an implementation phase, and a maintenance phase. It is a long-term transformation. (S. Shafiee, 2018).

On the part of the human element and its relationship to digital transformation, skills and experiences have a pivotal role in digital transformation. Users are central to the strategy as a result of digital transformation (Henriette et al., 2016). Younger generations have a higher level of digital literacy than older generations. There are also diverse backgrounds and tendencies when it comes to technology. The ability of these various stakeholders to adapt to developing technologies and make effective use of them is critical to the success of a digital strategy. (R. Luis Silva, 2017).

The unfavorable effects that a consumer is concerned about when performing an action are referred to as received risk. When applying for a service or sharing personal information, users are particularly concerned about the perceived risk of e-services. Furthermore, users with weak ICT abilities will be more concerned about the threats they perceive. In addition, one of the most important concerns of users in e-government services is privacy. This will almost certainly reduce their use of e-government services. Furthermore, one of the challenges to e-government use is a lack of awareness. It has been demonstrated that awareness plays an essential role in the acceptance of new technologies, and that a lack of it has a negative impact on potential e-government users. Governments oversee raising citizen awareness and developing proper tactics and plans to do this. (Nawaf Alharbi et al, 2014)

User experience includes not only customers but also internal users such as collaborators and employees (Berman, 2012; Belk, 2013).

Employees posing a threat to the organization's information or assets is one of the challenges identified. Within organizations, the focus is mainly on the employees or the staff itself. People within the company, or employees, are viewed as essential variables in preserving and securing data. Employees in organizations do not follow the organization's information security policies and regulations. Many employees do not take the rules and regulations seriously, and they will always try to avoid the essential procedures because they are too formal, and they will look for the simplest ways to do their tasks. Lack of common sense in completing their work according to the regulations of the organization will open the door to any attacks and mistakes that may occur to the organization's assets (Shamsudin et al., 2019).

As a result, the threat may arise directly or indirectly from both external and internal sources. The threat has an overpowering effect that might lead to the disintegration of organizations. As risks emerge from external aspects or are characterized as an external threat that can be related with a third party breaking the organization's information security, security threats and attacks can humiliate the organization's performance and productivity. Threats from within, on the other hand, could be related to management and employment. (Shamsudin et al., 2019).

Because of the large number of cyber-attacks on critical infrastructure, a lot of cyber-attack research has been done recently. However, there has been a dearth of research on evaluating cyber-attacks from an offensive cybersecurity perspective. (Leandros Maglara, 2021)

Cyber-attacks have been quantified using a quantitative method rather than an abstract one. They started by creating and deriving a comprehensive offensive cybersecurity framework and taxonomy, then conducting a content analysis of public reports of cyber-attacks to uncover specific cyber-attack techniques. (Leandros Maglara, 2021)

In today's digitized economy, when cybersecurity risks are always growing, protecting data, infrastructure, consumers, business partners, clients, and third parties from a breach is one of the most onerous challenges that enterprises face. We are becoming more internationally networked as a result of the financial and practical challenges that technology presents, which raises the danger of cybercrime. As a result, business leaders face new challenges. If a firm does not undertake digital transformation, it risks falling behind, and if it does, there is an inherent and growing risk of cybercrime. (Sheila Pancholi,2019).

The need for cybersecurity and action is increasing as digital transformation progresses. (Sheila Pancholi,2019). Based on survey has been done by RSM they found the following:

- 78% of businesses agree that digital transformation is the only way to thrive in the current and future economy.
- 64% of businesses agree that it is inevitable that digital technologies will

replace lower-skilled jobs.

- 38% agree that the more technology you implement, the more at risk you are of a cyber-attack if adequate controls are not implemented. (Sheila Pancholi, 2019).

Hypotheses

We have asked questions on the key digital transformation difficulties that have been recognized in the literature, based on the literature review in many prior studies and based on the previous literature related to the experiences and skills of users and the cybersecurity impact on digital transformation, hypotheses have been determined as follows:

H1: With implement more information technology in digital transformation will increases the possibility of cyber-attack.

H2: lower skills and changes resistance are failure factors for DT.

H3: The success of digital transformation depends primarily on increasing the technological awareness of internal and external users.

Research Methodology

To provide proof for the main hypothesis of this study, and to fulfill its objectives, a survey method has been implemented for specialist persons in information technology in different organizations in Saudi Arabia. in addition, information has been gathered from cybersecurity agencies in Saudi Arabia for comparison with other information generated from the surveys.

A mixed techniques strategy will be used in the study. To enable a complete investigation of the hypothesis, an intensive study of qualitative information from secondary sources will be joined with an analysis of statistics data from a distinct organization-based survey. A survey is the most appropriate data-gathering strategy for this study since it tries to collect data from the largest available sample size. In order to accommodate all responders, the poll also contained questions in Arabic. To answer to the three study hypotheses, an online survey will be employed. To compare the survey findings to qualitative data from secondary sources, an extensive study of qualitative data from secondary sources will be conducted as well.

Findings from qualitative investigations will be pooled, integrated, and evaluated to make conclusions using this method. This qualitative method works well for generating in-depth and complete information on users' ideas, attitudes, emotions, and experiences. Systematic evaluations of multiple primary qualitative sources will provide data from several research in order to provide fresh and more complete conclusions about cyber security in digital transformation.

Many questions have been designed to proof the suggested hypotheses that have generated based on many of previse studies. All those questions will be published by electronic survey in order to have a big data as match as possible.

Hypothesis 1 will include below questions:

Q1: Do you working in government sector or privet?
Q2: Does your organization adopt a digital transformation?
Q3: Up to which level of the digital transformation plan has been achieved?
Q4: Up to which level your organization has faced a cyber-attack in 2021?
Q5: What action plan has been taken to mitigate the attack's impact?
Q6: Based on your work in information technology, do you see an increase in cyber-attacks as the technical services increase?
Q7: which level do you expect the positive relation between the DT and the Cyber-attacks?
Q8: is there any IT Risk Management framework in your organization?

Hypothesis 2 will include below questions:

From your point of view:
Q1: Do you think the DT change can make a risk in your job carrier.
Q2: Do you think the employee IT skills can make difficulty for DT.
Q3: Do you think that digital transformation is directly related to all employees' skills?
Q4: how far do you expect there is a Positive relation between the DT failure and the Resistance of change?

Hypothesis 3 will include below questions:

Q1: do you have DT awareness plan in your

organization?

Q2: Do you think the organization culture can influence in the DT succuss?

Q3: From your point of view do you think its required to improve the organization culture to have a succuss digital transformation?

Q4: In your opinion, to what extent can organizational culture affect the success of digital transformation?

Q5: Do you think that the organization should publish and clarify the benefits before starting their digital transformation?

Q6: Do you think the employee not understanding information, goals, and strategies make digital transformation difficult?

Count of Timestamp	DT Availability					
	Yes (نعم)					Yes (نعم) Total
Organization Type	High (عالية)	Low (منخفضة)	Medium (متوسطة)	Very high (عالية جدا)	Very Low (منخفضة جدا)	
Government Sector (قطاع حكومي)	16	20	12	5	9	62
Above 30 % less than or equal 50%	2	6	7	1	3	19
Above 70%	3	3	1		2	9
less than 30%	2	4	2	1	2	11
Less than or equal 70 %	9	7	2	3	2	23
Privet Sector (قطاع خاص)	3	4	4	2	4	17
Above 30 % less than or equal 50%	1		1		1	3
Above 70%	2		2	1	2	7
Less than or equal 70 %		4	1	1	1	7
Grand Total	19	24	16	7	13	79

Data And Analysis

The research used a variety of data sources to better understand the implications of security on digital transformation. A survey was conducted with eighteen questions that were answered by several IT personnel from various Saudi Arabian sectors.

First hypothesis is highlighting on the connection between security concerns and digital transformation, as well as their impact on DT delivery. On the other hand, we will collect information from other agencies via the internet, including the impact of cybersecurity on digital transformation, which we will utilize as a foundation for compiling the survey results. For the analytical procedure, we will utilize EXCEL tools for analysis.

An interest analysis method will be used to quantities the data obtained in order to provide a clear picture of the DT's true role.

A survey has been released and distributed with a sample of IT employees. this sample is a set of 92 persons who responded to the survey they are as shown the table 1 from the government sector and private sectors. the government sector covers 68 responses with a percentage of 73.1 % whereas the privet sector covered 25 responses with a percentage of 26.9 % of the participated users.

Row Labels	Count of Timestamp
Government sector (قطاع حكومي)	67
Privet Sector (قطاع خاص)	25
Grand Total	**92**

Table 1: participate users counts

79 of the participating employees have agreed that their organization implements digital transformation as a strategic option. 62 organizations in the public sector agreed they organization is adopting digital transformation whereas 5 of the results are not. In the privet sector as well has 17 organizations agreed to have a digital transformation, and 8 are not applied the DT as show in table 2.

Row Labels	No	Yes	Grand Total
Government sector	5	62	67
Privet Sector	8	17	25
Grand Total	**13**	**79**	**92**

Table 2: Organization adopts a digital transformation

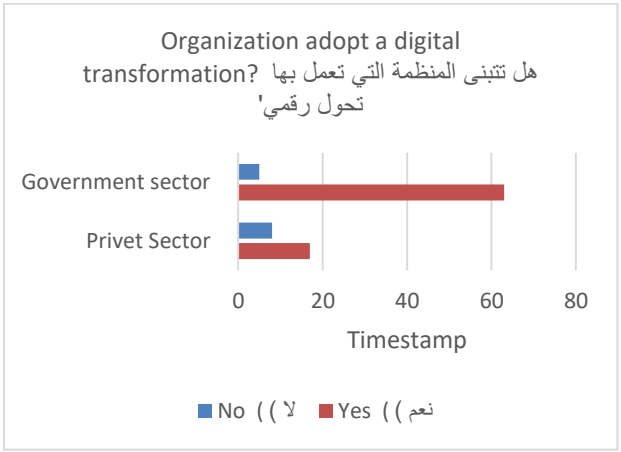

Figure1: Organization adopts a digital transformation

Table3: level of attaches based on the sectors at

SA

Based on the above figure and statistics table information we hare agreed that most of the government organization have adopting the digital transformation following up the Saudi Arabia vision 2030 with view participation from proved sector as shown above.

Therefore, we will analysis the data that we are collected by the survey to prove if the hypotheses have been suggested are correct and measurers it on the different research sectors.

First, the survey has clarified that the relationship between the digital transformation and increasing of the cyber-attacks. Most of the participating on the survey have reflect status of their organization.

So that the result shown on above table3. As you see in the table is explain the organization in both sectors privet and public effective in digital transformation at which level of transformation maturity. The data shows that 16 of the response shows height level of attack at 70 % of transformation level. As well as only 5 persons are show very high attacks, they faced with same level of transformation at the same level at government sector

Table 3 demonstrates a significant rise in the number of replies at the 70% level mark of the government's digital transformation. Only three replies for a high attack for the level above 70% of the DT. In all, 16 of the 92 answers noted that a high-level assault occurred at their business in 2021.

At the very high level, 5 individuals reply, and 12 people respond at the medium level, with 33 people verifying that an assault occurred at various levels of digital transformation. This means that nearly half of the respondents indicate that the DT can increase the number of attacks during the DT period. While the degree of maturity of DT, which we predicted was above 70%, only 9 out of 62 people said they had been attacked, implying that once the system has matured, it can be secured.

While the commercial sector has given just a few replies, the public sector has given only nine responses, all of which agree that there is a high degree of DT progress.

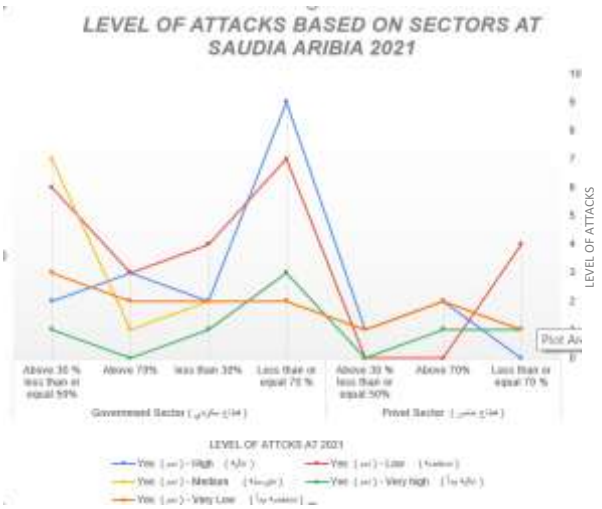

Figure2: Level of attacks based on an organization

Second, the survey takes a different method to determining the relationships between digital transformation and security, therefore we asked the target sample of users' direct questions to obtain their feedback on the research themes. So, in response to the first hypothesis's question 6" do you see an increase in cyber-attacks as the technical services increase?
", The following table4 shows the results we discovered.

The Relationship Between DT And Attacks

Sector	Count
Government Sector (قطاع حكومي)	**67**
No (لا)	9
Yes (نعم)	58
Privet Sector (قطاع خاص)	**25**
No (لا)	2
Yes (نعم)	23
Grand Total	**92**

Table 4: relation calculation based on users' feedback

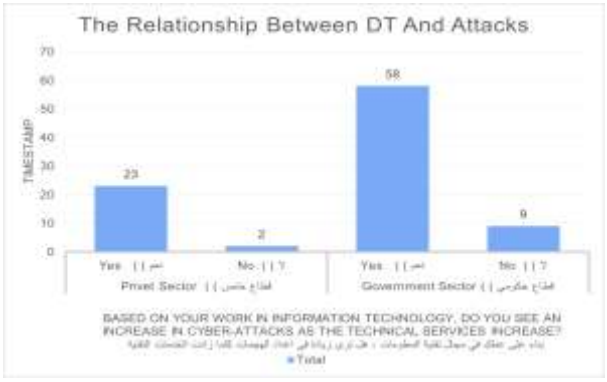

Figure3: level of relation of attack and digital transformation

As a consequence, 58 of the 67 respondents in the government sectors believe that security assaults have a direct influence on digital transformation, while just 9 of the sample have been rejected. In addition, 23 people out of 25 agree that the private sector has an influence on digital transformation. As a result and based on the preliminary study and input from IT employees on the questions presented to assess the impact of security on the DT, we are completely certain of the impact.

According to another survey and Arab News, Saudi Arabia has been a major target of assaults. In the first two months of 2021, there were 7 million assaults. Whereas, according to a study, attacks levels rose from 3.6 to 5.6 between 2012 and 2016. Which is making a significant difference as a result of the technological revolution that has occurred concurrently with the digital transformation.

We asked the survey participants for their input on how to reduce the danger of cyber-attacks. As seen in Table 5, a 31 people agreed that risk should be avoided. Abstaining from any potentially damaging activity is part of risk avoidance. A risk avoidance approach aims to reduce the number of vulnerabilities that can be exploited. Policy and procedure, training and education, and technical installations can all help to limit and manage risk. 30 people responded to the poll, indicating that risk mitigation is used in their company. In the private sector, 17 people agreed that these businesses' risk management strategy is avoidance.

Row Labels	Count
Government Sector (قطاع حكومي)	**67**
Risk Accept	4
Risk Avoid	31
Risk Mitigate	30
Risk Transfer	2
Privet Sector (قطاع خاص)	**25**
Risk Accept	2
Risk Avoid	17
Risk Mitigate	6
Grand Total	**92**

Table 5: Risk Management Approaches.

Finally, and based on the preliminary results of both the survey and the internet report, we find that as the use of digital systems grows in SA, so does the number of attacks. As a result, organizations are constantly under attack, but with a mature system and solid defense in place, we can protect our systems.

The second hypothesis is that one of the reasons for the failure of digital transformation is change resistance and low personnel capabilities. As a result, we issued a survey to 92 individuals in various Saudi Arabian private and governmental institutions. We're trying to figure out how much the Saudi organization's resistance and inadequate staff skills are worth, and how much they may stymie the country's digital transformation.

We discovered the following after analyzing the data obtained from the survey:

- 27 of the 92 samples believe that there is a strong association between the DT and employee resistance changes,
- 31 feel there is a high level of failure factor relationship,
- whereas 27 says there is a medium level of failure factor relationship.

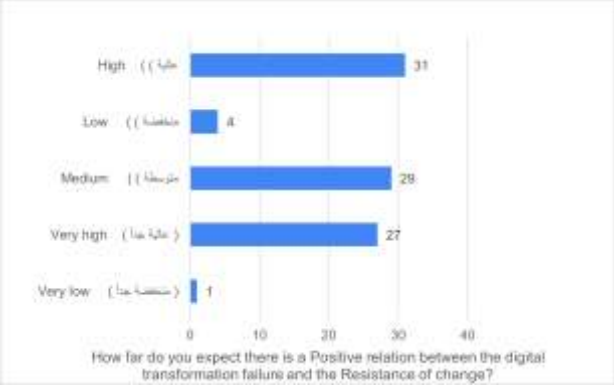

Figure4: Relation between DT and Skiles & resistance

Question	Yes	NO
Do you think the digital transformation change can make a risk in your job carrier?	18.3 %	81.7 %
Do you think the IT employee's skills weakness can make difficulty for Digital Transformation?	89.2 %	10.8 %
Do you think that digital transformation is directly	90.3 %	9.7 %

related to employees' skills?		

Table 6: relation calculation based on users' feedback

As shown in the above table and the results of the survey feedback, when asked if digital transformation poses a risk to their careers, 81.7 percent of IT personnel said no, while 18.3 percent said yes. As a result, some employees are wary about digital transformation, which will be a roadblock for their job stability, especially if upper management shares their concerns.

Furthermore, we asked if the employee's skills influence DT progress and how the match is linked with employees' skills, and the answer was that 89.2 percent of respondents agreed that they make the DT difficult to process, and 90.3 percent of respondents agreed that the digital transformation and employee's skills have a strong link.

As a result, we can summarize the talents and resistance of workers who have a strong relationship with the DT based on this information. Employees must be included in the planning process, and the planner must have an awareness strategy "as described in the third hypothesis" to ensure support from all levels of shareholders.

The **third hypothesis** looked at organizational culture and digital transformation awareness, and a survey was sent out to Saudi national organizations in both the private and governmental sectors to see how employees affect digital transformation development.

As a consequence, we asked employees a series of questions to extract their opinions on the company's culture and how it influences digital transformation. When asked whether "is there digital transformation awareness strategy in their firms," we observed that 61.3 percent had plans in place, while 38.7% did not. According to 93.5 percent of respondents, is important to the success of digital transformation efforts.

We had 100% agreement from all voters that improving the organization's culture is essential and recommended for a successful digital transformation. Which reflects the employees' viewpoint?

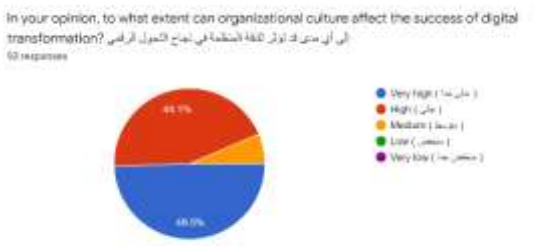

Figure5: Organization culture effect level

Based on the findings of the survey, to what extent can the organization's culture influence digital transformation. The digital revolution has an influence on the organization's culture, according to 49.5 percent of voters. 44.1 percent of them, on the other hand, said that digital transformation had had a significant impact on them. That is to say, the culture of the company is a critical aspect that might influence the digital transformation's development and achievement of objectives.

According to 97.8% of study respondents, before initiating its digital transformation, the organization should disclose and clarify the advantages of the transition. This is a sort of shareholder involvement in the planning stage that may help to lessen opposition to organizational changes. Employees will become a success factor for digital transformation rather than a failure factor if the organization includes them in the process, shares their ideas, and includes them in the process. Finally, 95.7 percent of respondents feel that a lack of understanding of the digital transformation process will intensify the process. As a result, personnel at all levels must understand the digital transformation's goals and objectives in order to receive the appropriate support in order to achieve the desired results.

Conclusion

While many businesses seek digital transformation, putting it in place is a difficult task. Understanding the technology and accepting its execution seldom yields positive outcomes. Instead, leaders must understand that digitizing their organizations typically necessitates a major rethinking of many organizational procedures, as well as the necessity to genuinely drive this difficult shift.

Some critical areas must be addressed, according to organizational and leadership theory, if organizations are to achieve the intended outcomes through digital transformation. Setting

clear goals and objectives for digital transformation is the first step. Leaders must choose what they want to accomplish through digitalization, where they want to do it, and how they want to do it. A detailed structure and mapping of the process should be built based on this knowledge. Leaders must be digitally savvy and create a digital imperative with a clear goal and ways for everyone to participate.

Successful organizations are able to unite organizational members around common goals and ideas, encourage individuals to take action, and plan activities by being active and rewarding them. Accepting the challenges and roadblocks that digital transformation brings is also critical. Successful leaders do not see them as a source of failure; rather, they see them as an additional source of knowledge, and they like incorporating them.

Recommendations

Employee resistance to change is the most critical factor influencing digital transformation. Employees' capacity to adapt to new technologies and services will aid digital transformation success. Employees must handle this problem and conquer the difficulty by regularly adjusting to new technology and services. Expert employees are more aware of the benefits of digital transformation as a result of their experience.

To have a successful digital transformation we have to implement a satiable security strategy to protract the organization systems level of the level can guarantee the digital transformation can be moved to achieve its objectives without interruption.

References

1. Henriette, Emily; Feki, Mondher; and Boughzala, Imed, "Digital Transformation Challenges" (2016).MCIS 2016 Proceedings. 33.
2. Belk, R. (2013), Extended Self in a Digital World, Journal of Consumer Research, 40 : 3, 477-500.
3. Berman, S. (2012), Digital transformation: opportunities to create new business models, Strategy & Leadership, 40 : 2, 16-24.
4. Rodrigues, L. S. (2017, November 1). Challenges of digital transformation in Higher Education Institutions: A brief discussion. Proceedings of 30th IBIMA Conference. Retrieved May 20, 2022, from http://hdl.handle.net/10400.22/15234
5. Alharbi, N., Papadaki, M. and Dowland, P., 2014. Security factors influencing end users' adoption of E-Government. Journal of Internet Technology and Secured Transactions (JITST), 3(4), pp.320-328.
6. Shamsudin, N.N.A., Yatin, S.F.M., Mohd, N.F., Nazim, A.W.T., Sopiee, M.A.M. and Natasya, F., 2019. Information Security Behaviors among Employees.
7. Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1).
8. Mohamed, Bushra & Elamin, Bushra. (2013). Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future. Journal of Information & Knowledge Management. 3.
9. Catch-22: Digital Transformation and its impact on ... - RSM global. (n.d.). Retrieved May 20, 2022, from https://www.rsm.global/ireland/sites/default/files/media/catch-22_digital_transformation_and_cybersecurity_final.pdf
10. Alhubaishy, A., Aljuhani, A. The challenges of instructors' and students' attitudes in digital transformation: A case study of Saudi Universities. Educ Inf Technol 26, 4647–4662 (2021).
11. Afandi, W. (2017). THE ROLE OF STRATEGIC LEADERSHIP IN DIGITAL TRANSFORMATION PROCESS. International Journal of Research and Reviews in Applied Sciences, 33(2), 19–22.
12. Quadri, Aman & Khan, Muhammad. (2019). CYBERSECURITY CHALLENGES OF THE KINGDOM OF SAUDI ARABIA.
13. Sakr, T. (2021, October 9). Digital transformation in Saudi Arabia ...strict steps towards "paperless government". Leaders. Retrieved May 20, 2022, from https://wp.me/p9QH6r-3BJ
14. Saudi Arabia National Portal. التحول الرقمي في المملكة العربية السعودية. (n.d.). Retrieved May 20, 2022, from https://www.my.gov.sa/wps/portal/snp/aboutksa/digitaltransformation

Author's Information

Author's[1]: Khalid Almdani
Highest Qualification: MS Degree in Information Technology (IT)
Department: College of Computer Science and Engineering
Corse/Year: Electronic Government 2022
Affiliation: University of Jeddah, KSA, PO 23218
Email ID: abuaiman1@gmail.com

Author's[2]: Hassan Al saeedi
Highest Qualification: MS Degree in Information Technology (IT)
Department: College of Computer Science and Engineering
Corse/Year : Electronic Government 2022
Affiliation: University of Jeddah, KSA, PO 23218
Email ID: h.alsaeedi7770@gmail.com

Author's[3]: Abdullah Softah
Highest Qualification: MS Degree in Information Technology (IT)
Department: College of Computer Science and Engineering
Corse/Year: Electronic Government 2022
Affiliation: University of Jeddah, KSA, PO 23218
Email ID: Softah15@hotmail.com

Author's[4]: Sultan Khogeer
Highest Qualification: MS Degree in Information Technology (IT)
Department: College of Computer Science and Engineering
Corse/Year: Electronic Government 2022
Affiliation: University of Jeddah, KSA, PO 23218
Email ID: Sultan.khogeer@hotmail.com

Author's[5]: Khalid Hamdan Assiri
Highest Qualification: MS Degree in Information Technology (IT)
Department: College of Computer Science and Engineering
Corse/Year: Electronic Government 2022
Affiliation: University of Jeddah, KSA, PO 23218
Email ID: khalid.assiri@gmail.com