“Cyber-security effect on organizational internal process: mediating role of technological infrastructure”

AUTHORS	Yanal Kilani
ARTICLE INFO	Yanal Kilani (2020). Cyber-security effect on organizational internal process: mediating role of technological infrastructure. *Problems and Perspectives in Management*, *18*(1), 449-460. doi:10.21511/ppm.18(1).2020.39
DOI	http://dx.doi.org/10.21511/ppm.18(1).2020.39
RELEASED ON	Tuesday, 07 April 2020
RECEIVED ON	Monday, 02 December 2019
ACCEPTED ON	Thursday, 27 February 2020
LICENSE	This work is licensed under a Creative Commons Attribution 4.0 International License
JOURNAL	"Problems and Perspectives in Management"
ISSN PRINT	1727-7051
ISSN ONLINE	1810-5467
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
30	2	9

BUSINESS PERSPECTIVES

LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine

www.businessperspectives.org

Yanal Kilani (Jordan)

CYBER-SECURITY EFFECT ON ORGANIZATIONAL INTERNAL PROCESS: MEDIATING ROLE OF TECHNOLOGICAL INFRASTRUCTURE

Abstract

Adopting the technologies among organizations comes with the continuous worries of protection and hacking. The idea of cyber-security has become over the years the main interest of many organizations, which depend on technologies in its operations, which requires them to pay extra attention to their technological infrastructure. The current study aims at examining the influence of cyber-security forces on organizational internal operations and the role of technological infrastructure in defining and controlling the level of protection that cyber-security has on organizational internal processes. Quantitative approach was adopted, and a questionnaire was utilized to collect the data from a convenient sample of 360 software engineers, network engineers, software testers, web developers, and technical support using a structured survey questionnaire, and analyzed using SPSS version 21. The results confirmed that cyber-security motivators (data growth, technology expansion, access to required resources, operational control, and technical control) indirectly affect solid internal processes that are attributed to the consistency of technological infrastructure in an organization. The variable of 'data growth' appeared to be the most influential motivator on cyber-security strategies, as it scored a mean of 4.2661, which is the highest among all adopted variables and followed by the variable of 'technical control', which scored a mean of 4.1296. Accordingly, the study recommends that organizations should consider IT infrastructure as a main item within their risk management strategies to avoid unpredicted risks and attacks.

Keywords cyber-security, data growth, technology expansion, operational control, technical control

JEL Classification M15, L86

Received on: 2nd of December, 2019
Accepted on: 27th of February, 2020
Published on: 7th of April, 2020

Yanal Kilani, Ph.D., Assistant Professor, Department of Management Information Systems, Isra University, Jordan.

Conflict of interest statement:
Author(s) reported no conflict of interest

INTRODUCTION

Nowadays society runs largely on technology, as it depends on it for commerce, industry, and interaction. This dependency of society on technology has made cyber to be firmly entrenched in people's mindset and language. While the use of the technology or cyber/internet has led to significant advances in many areas, it has exposed individuals and organizations to a host of security risks emanating from cyber-attacks via digital interfaces. Examples of these cyber-attacks include data breaches on personal and corporate devices, the virus that attacks computer infrastructure, and denial-of-service (DoS) attacks on computer networks. Other common forms of cyber acts that can potentially cause harm to an organization include sabotaging of systems to compromise the integrity of the systems and services, copying of customers' data for selling on dark web, and theft of corporate secrets. As emphasized by Agrafiotis, Nurse, Goldsmith, Creese, and Upton (2018), these cyber breaches, attacks, and threats have increasingly become a key concern for many organizations and are now at the center of organizational cyber-risk and security discussion. A report

by Symantec (2016) reinforces this view by showing that 318 data breaches were reported in 2015, exposing 429 million business identities. These cyber-security breaches and threats are believed to bring losses to organizations. For example, the cost of each of these cyber-security breaches was estimated at US$ 221 in the financial sector; US$ 208 in the service industry; US$ 355 in the healthcare industry; and US$ 246 in the education industry (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014).

Renaud et al. (2018) believe that most of these cyber breaches and threats may affect the organizational internal process. Some scholars (e.g., Sun, 2018; Pak Nejad, Javadi, & Mohammadi, 2014) support this view by linking these cyber-security risks and threats to cyber-security forces. For example, in view of Pak Nejad et al. (2014), data growth, technology expansion, and access to required resources can enhance the chances of cyber-risk. For other authors (e.g., Yasin, 2018), the increasing number of cyber threats and their associated costs have pressured many organizations to adopt the technology and use all possible tools and technologies in an attempt to protect its data and information from being hacked or stolen through the different means of technologies like software, programs, and risk management approaches. However, few studies have examined the effects of cyber-security on organizational internal process and the role of technological infrastructure in minimizing these effects. The present study investigates the effect of cyber-security on organizational internal process with technological infrastructure as a mediating variable.

1. LITERATURE REVIEW

Cyber-security was defined by Schatz, Bashroush, and Wall (2017, p. 64) as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber-environment and organization and assets." As it is known, having internet means to have open doors to the world; those open doors do not only bring us information, developments, and enhancements; it also brings us risks, dangers, and pitfalls that can erupt and cause much damage. Vishik, Matsubara, and Plonk (2016) defined cyber-security as "an activity that protects the human and financial resources associated with ICTs, ensures the potential to reduce losses and damages in the event of risks and threats, and allows the situation to be restored as quickly as possible, so that the wheel does not stop."

The idea of cyber-security came in accordance with the concept of cyber-attacks and piracy, which appeared on the internet, resembling itself as a ghost that threatens online data and information, in addition to risking the security of transactions that take place online (Whyte & Mazanec, 2018). Priyadarshini (2018) argued that cyber-security is considered to be an important pillar of information security not only at the organizational level but also at the level of countries, as it includes e-government security.

In general, cyber-security is considered to be one of the most important issues that are attracting the attention of the countries. Nowadays, many countries are putting the concept of cyber-security on its agenda as a reference to the importance of this issue and the in-reversed negative influence that this problem may bring with it (Efthymiopoulos, 2016). Many scholars (Abu-Taieh, Al Faries, Alotaibi, & Aldehim, 2018; Keplinger, 2018; Dewal, Narula, Jain, & Baliyan, 2018) have stated that cyber-security is not only tools and software; it is more of an ideology that organizations embrace to spread the culture of cyber-security among its individuals.

On the other hand, Elamiryan and Bolgov (2018) noted that cyber-crimes can be committed either by people outside the organization who infiltrate the computer system (often through networks) or by people within the organization who have access to the system, but who abuse the system for various reasons. Orkand Consulting stated that losses from computer crime are estimated at US$ 1.5 million for computerized banking companies in the United States. On the other hand, the National Center for Computer Crime Data in Los Angeles estimates that 70% of recorded cyber-crimes occurred from within, i.e., by those working within

http://dx.doi.org/10.21511/ppm.18(1).2020.39

organizations management of information systems in particular.

Protecting the organizational information and supporting its data with the needed cyber-security can, with no doubt, be considered to be an expensive and hectic process.

Over time, the continuous operations on an organization's data begin to increase in accordance with the on-going operating life. The organization begins to collect the data that are related to many aspects of organizational processes. Udo et al. (2018) noted that this expansion of the data in the organizations increases the force towards developing risks in the organizational internal process, specifically if the organization was based on the high end of technological advancement. Narukonda and Rowland (2018) stated that online operating organization and those working on the internet, like online trading and communication, are usually more exposed to cyber-attacks compared to those organizations, which are away from technology.

Pernik (2016) noted that the expansion of technology is the first fore towards increasing hazards and risks of cyber-attacks. He argued that the expansion of technology opens different gates of information, which increases the flow and also jeopardizes the organization into a realm of data leading it to the state of sensitivity technology-wise.

This idea, according to Horowitz et al. (2018), is considered to be one of the most sensitive forces of security issues. The access of different personnel to information should be based on a strict approach that can control those who have access and who do not. On the other hand, Moreira, Molina, Lazaro, Jacob, and Astarloa (2016) noted that free access to data within an organization to its personnel makes these data accessible for the outsider. They meant that if an organization was not well-protected, then it would be easier for external parties to perform any type of attacks on its systems and exposing it to the dangers of hacking and piracy.

The role of operational control is very important in this field. It refers to the group of processes that are manifested in the internal environment of an organization and which, through control, can be managed and handled according to what is needed and required (Poresky, Andreades, Kendrick, & Peterson, 2017). From the perspective of Udo, Bagchi, and Kirs (2018), it was noted that operational control is basically sourced from individuals who have to enjoy a high level of awareness regarding security. This awareness is one of the basic needs among individuals since they are the first and only operator of technological equipment and tools.

Rasekh, Hassanzadeh, Mulchandani, Modi, and Banks (2016), on the other hand, argued that operational control is sourced from plans and strategies that an organization embraces through its operating times. When an organization decides to adopt the technology of different types, it should put into the perspective of its strategies that cyber-attacks and different cyber hazards come with the package. There is no such thing as gaining advantages and being harmed from the disadvantages, based on which the disadvantages of technologies are one of the aspects that can be controlled through the organizational operational process.

The technical control is sourced here through activating all knowledge that employees have in references to cyber-attacks and protection. Not to mention the role of technological infrastructure that also plays a role in defining the nature of operational control and awareness of employees at the security level. Poresky et al. (2017) added that the technical control appears not only at the level of personnel, but also at the level of tools, programs, and software that an organization embraces to protect itself from cyber-attacks and forms a well-built framework that can work as a shield of cyber-security for organization.

A cyber-security system would not be valid alone; at the end, it is nothing more than a program or software that needs other factors to be activated and perform in the best way possible. Craigen et al. (2014), Schatz et al. (2017), and Pak Nejad et al. (2014) noted that there are main components that when gathered can formulate the overall performance of cyber-security systems in the organizations. They noted that there are four main components, which are: technological solutions, processes, methods, and human engagement.

Rasekh et al. (2016) noted that technological infrastructure refers to the set of means and capabilities normally coordinated by a centralized information organization. For example, a telecommunications network operated by a particular enterprise and shared by many commercial and service organizations constitutes a common infrastructure. Laws and customs constitute mechanisms that link the exploitation of both physical and mental compounds to the IT architecture. The common facilities for IT architecture are the embodiment of the architecture and the realization of practical applications.

Also, Rasekh et al. (2016) added that the degree of sophistication that the technological infrastructure of an organization depends on and the idea of infrastructure is very important in any organization that seeks to depend on technology to operate. It plays a very important role in defining the degree of security that this organization enjoys in terms of protection, speed, and final results. A week infrastructure, specifically in technology, cannot be useful for the organization; on the contrary, it can be seen as a threat to organizational core into a weak performance in terms of technology.

Technological infrastructure rules dictate how resources are acquired, managed, or exploited. Working groups may have building and development software with rules that dictate the use of specific physical capabilities such as programming languages (C++, Pascal). In this example, IT standards provide a guideline for determining both the use of mental capabilities in the software development method and the use of specific physical capabilities (programming languages) in the application software development process (Göztepe, Kılıc, & Kayaalp, 2014).

The employees within the field of IT are among the factors that deeply influence the level of cyber-security in an organization. It is normally taken for granted that employees within the field of IT have to be highly trained and experienced in the technology and its tools. This experience would not be valid or useful unless those employees enjoy a high level of awareness regarding the importance of security, protection, and technological hazards that accompany IT-based organizations (Pfleeger, Sasse, & Furnham, 2014).

Considering staff and employees as a force for cyber-security is seen as one of the most important issues that should be addressed by the management. Some aspects of cyber-security require high level of alert from employees in order for the security to be valid within the organization. This requires the employment of highly experienced individuals in the field (Dewal et al., 2018).

Göztepe et al. (2014) noted that the operating software is of great importance. An organization should pay extra attention to the nature and approach of software it uses to guarantee the best and the strongest protection for its technological advancements used in its internal operations. Software is usually supplied with suitable protective programs that enable it to work in a safe environment. The organization should be aware of the importance of protected software before installing it in its system due to the massive fragility that can be brought through uncensored software.

The network is one of the important aspects in the field of cyber-security. A network is mainly the first gate an attacker may take to attack. In that sense, the network on an organization should be built on a strong technological infrastructure that helps it work on the safe level rather than exposing the organization to attacks that may endanger its existence (Diego, 2019).

2. CONCEPTUAL SCHEME AND HYPOTHESES

Stafford, Deitz, and Li (2018) noted to the importance of internal processes in identifying cyber-security and mainly internal audit. Stafford et al. (2018) claimed that internal processes like monitoring, audit, and controlling are among the important factors that shape the way cyber-security is in an organization. On the other hand, one of the leading consulting organizations around the world "Deloitte" mentioned in one of its annual reports that cyber-security is mainly a culture that spread in the organization in the shape of tools, strategies, plans, and approaches. Deloitte (2015) stated that following the security-based internal processes can help in defining the concept of cyber-attacks and piracy in a clearer approach and in building a secure environment. Generally speaking, the more technology

http://dx.doi.org/10.21511/ppm.18(1).2020.39

Source: Yasin et al. (2018), Pak Nejad et al. (2014).

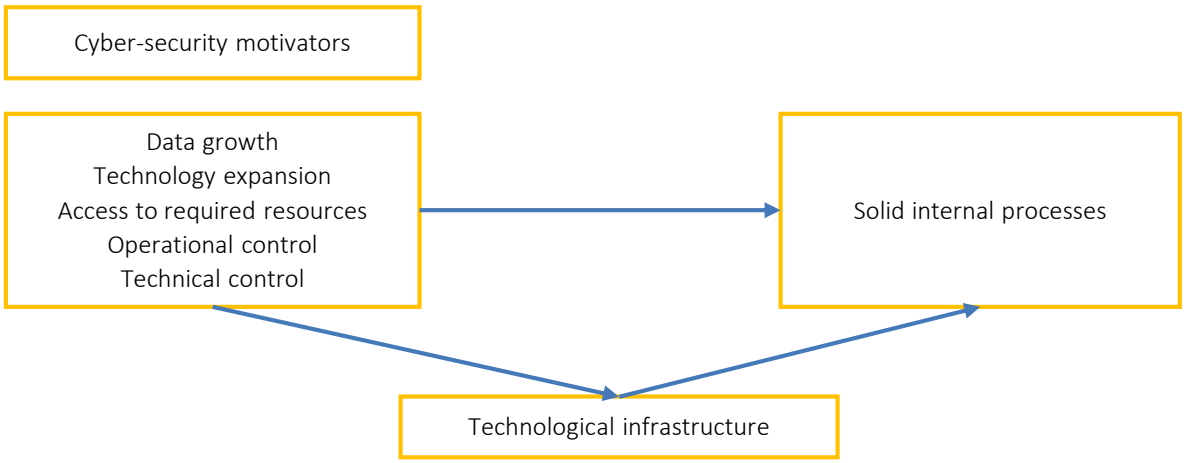

Figure 1. Conceptual framework relating cyber-security motivators to technological infrastructure and internal processes adapted

and internet are used, the more there is a chance to expose the organization for cyber-security issues. Many scholars spoke of such forces and risks, which increase cyber-security risks, such as Yasin, Liu, Li, Wang, and Zowghi (2018) who argued that operational control and technical control and are main motivators for cyber-security risks, while Pak Nejad et al. (2014) argued that data growth, technology expansion and access to required resources can enhance the chances of cyber-risk.

Based on the above argument, the current study seeks to examine the influence of cyber-security forces on internal operational processes within the organization and the role of technological infrastructure in controlling such forces and their implications on internal processes.

Based on the above conceptual framework supported by the existent literature, it was hypothesized that:

1. Cyber-security motivators positively and statistically significantly help create solid internal processes.

2. Cyber-security motivators positively and statistically significantly influence technological infrastructure.

3. Technological infrastructure positively and statistically significantly influences solid internal processes.

4. Technological infrastructure positively and statistically significantly mediates the relationship between cyber-security motivators and solid internal processes.

3. METHODS

3.1. Sample

Data were collected using a convenient sampling technique by selecting a sample of 360 software engineers, network engineers, software testers, web developers, and technical support participants from engineering, electrical and information technology sectors in Jordan.

3.2. Data collection tool

Quantitative data used in the present study were collected using a structured survey questionnaire derived from past studies and modified to reflect the context of the present study. The questionnaire consisted of closed-ended questions scored on the Likert scale ranging from 1 to 5, with 1 representing strongly disagree, 2 representing disagree, 3 representing neutral, 4 representing agree, and 5 representing strongly agree.

The questionnaire encompassed two sections. The first section covered the demographic variables, namely age, gender, experience, and position. The second part of the questionnaire statements was

related to study variables, namely data growth, technology expansion, access to required resources, operational control, and technical control.

A total of 400 questionnaires were distributed using drop and pick method to 400 participants who were software engineers, network engineers, software testers, web developers, and technical support. A total of 360 participants filled the questionnaires and returned them, representing a response rate of 90%.

3.3. Data analysis

Data analysis was undertaken using SPSS version 21. Data were processed into descriptive statistics (mean, standard deviation, mode, and median). Path analysis was undertaken using IBM SPSS Amos 21.0 program.

A reliability test was undertaken using SPSS's Cronbachs' alpha, which measures the internal consistency of a construct. The result showed a value of 0.942 for all items, as well as alpha for each variable is greater than accepted percent 0.60, which is a reasonable value, indicating the tool consistency that enhanced its use for the study.

4. RESULTS

Frequency and percentages were used to describe the following sample characteristics. Table 1 shows that the majority of the sample ranged between 25-30 years and 31-36 years, forming 36.7% and 38.1% of the total sample, respectively, while those within the age range (43+) form 8.1% of the sample.

Table 1. Age

Age		Frequency	Percent	Valid percent
Valid	25-30	132	36.7	36.7
	31-36	137	38.1	38.1
	37-42	62	17.2	17.2
	43+	29	8.1	8.1
	Total	360	100.0	100.0

As can be inferred from Table 2, 57.2% of the sample was male participants, with 42.8% being translating to the frequency of 206, and 154 for male and female participants, respectively, and totaling 360 participants.

Table 2. Gender

Gender		Frequency	Percent	Valid percent
Valid	Male	206	57.2	57.2
	Female	154	42.8	42.8
	Total	360	100.0	100.0

From Table 3, it can be seen that the majority (75%) of study participants held the MA degree, representing a frequency of 272 individuals, with parity 1.9% holding a PhD degree, representing a frequency of 7 individuals.

Table 3. Education

Education		Frequency	Percent	Valid percent
Valid	Diploma	48	13.3	13.3
	BA	35	9.7	9.7
	MA	270	75.0	75.0
	Ph.D.	7	1.9	1.9
	Total	360	100.0	100.0

Based on Table 4, the majority of study participants (58.90%) were software engineers (22.2%), web developers (20%), and offered technical support (16.7%), while 14.7% worked as software testers.

Table 4. Position

Position		Frequency	Percent	Valid percent
Valid	Software engineers	80	22.2	22.2
	Technical support	60	16.7	16.7
	Software testers	53	14.7	14.7
	Web developers	72	20.0	20.0
	Network engineers	95	26.4	26.4
	Total	360	100.0	100.0

From the descriptive statistics as revealed in Table 5, participants either agree (value 4) or strongly agree (value 5) (i.e., a mean of above 3) to questionnaire statements regarding data growth, technological expansion, access to the required resources, operational control, technical control, solid internal processes, and technological infrastructure. This indicates that they approve (4) or strongly approve the statements relating to data

http://dx.doi.org/10.21511/ppm.18(1).2020.39

Table 5. Descriptive statistics

Question	N	Min	Max	Mean	Std. deviation
Cyber-security forces					
Data growth					
Data growth increases the risks of cyber-attacks	360	1	5	4.28	.828
When data increases in an organization manual controlling would be hard	360	1	5	4.24	.777
There is always a chance for cyber-attacks when the organization grows data in a massive amount	360	1	5	4.25	.741
The larger the organization, the more data it would generate	360	1	5	4.32	.716
Cyber-security is important in organizations that are based on a huge amount of data	360	2	5	4.25	.712
Technology expansion					
The price of technological advancements can be the safety and security of the organization	360	1	5	4.11	.862
Technology expansion should be based on well-built technological infrastructure and strong cyber-security	360	1	5	4.21	.857
Not every technology developed organization is developed security wise	360	1	5	4.16	.749
Technology expansion increases risks and dangers	360	1	5	4.17	.803
Technology expansion should be built with risk management plans and strategies	360	1	5	3.91	.958
Access to required resources					
Not all employees in an organization should have access to sensitive resources	360	1	5	3.90	.910
Access to resources should be entrusted to someone who is worthy	360	1	5	3.92	.905
Open access to resources in an organization can expose the organization to many risks	360	1	5	4.03	.914
Resources should be protected through strong shield of cyber-security	360	1	5	3.88	.876
There is always a chance for cyber-risks when there is no protection on resources in an organization	360	2	5	4.13	.753
Operational control					
Internal operations are of great important in managing cyber-attacks	360	2	5	4.09	.706
Employees should be aware of the sensitivity of data protection	360	1	5	3.99	.781
The control can be done based on fixed internal plans and strategies	360	1	5	4.01	.786
Internal operations are the first jeopardy to data in an organization	360	2	5	4.03	.820
The control must be done on the level of employees within the internal front more than the external front	360	1	5	3.86	.936
Technical control					
The control should be done through experienced employees in technicality	360	2	5	4.09	.750
Technical control of cyber-security should be based on complicated and safe infrastructure	360	1	5	4.15	.773
Every technical move in an organization should be controlled and monitored	360	2	5	4.14	.709
Solid internal processes					
Internal processes should be based on constant monitoring	360	2	5	4.38	.607
Internal processes should be corrective to avoid risks	360	1	5	4.19	.793
Plans and strategies are a basic requirement for internal processes	360	2	5	4.30	.771
Internal processes are the first defense towards cyber-attacks	360	1	5	4.15	.824
Internal processes should be based on integrated requirements and control framework	360	1	5	4.10	.904
Technological infrastructure					
A weak infrastructure is the first step towards cyber-attacks	360	2	5	4.43	.660
Organization with well-built infrastructure are protected against casual risks	360	2.00	5.00	4.2722	.69081
An organization with weak infrastructure is usually weak against cyber-attacks	360	2.00	5.00	4.2583	.69814
The technological infrastructure should be accompanied by experienced staff	360	2.00	5.00	4.1722	.74513
Cyber-security is backup with string and well-built infrastructure	360	1.00	5.00	4.1583	.81759

growth, technological expansion, access to the required resources, operational control, technical control, solid internal processes, and technological infrastructure.

As can be inferred in Table 6, the statements regarding data growth, technology expansion, required resources, operational control, technical control, solid internal processes, and technological infrastructure are approved. This is based on the view that the mean of responses ranged between 3 and 5 as scored on the Likert scale, which indicates an approval (agree) or strong approval (5) of the statements captured in the questionnaire.

Table 6. Descriptive statistics

Variable	N	Minimum	Maximum	Mean	Std. deviation
Data growth	360	2.00	5.00	4.2661	.55149
Technology expansion	360	1.60	5.00	4.1128	.61951
Required resources	360	1.60	5.00	3.9733	.68258
Operational control	360	2.00	5.00	3.9967	.63596
Technical control	360	2.00	5.00	4.1296	.58654
Solid internal processes	360	2.40	5.00	4.2233	.54534
Technological infrastructure	360	2.80	5.00	4.2583	.52102
Valid N (listwise)	360	–	–	–	–

Based on path analysis, the results are found and presented in Table 7.

Table 7. Path analysis

RAMSEA	Chi²	df	*p*-value	GFI	CFI
0.065	5.221	13	0.14	0.981	0.992
GFI		–		≥ 0.90	
CFI		–		≥ 0.90	
RAMSEA		–		≤ 0.08	

To test the structural model fit, the value of X2 = 5.221 is not significant at 0.05, GFI = 0.9920 is an excellent indicator, the CFI = 0.981 is an excellent value, RAMSEA = 0.065 is an acceptable value, which means the structural model is fit.

To test the structural model fit, the value of X2 = 5.221 is not significant at 0.05, GFI = 0.992 is an excellent indicator, the CFI = 0.981 is an excellent value, RAMSEA = 0.065 is an acceptable value, which means the structural model is fit. Table 8 shows that the study hypotheses were supported.

The results of the analysis presented in Table 7 show that C.R. values are significant at 0.05 level, which means:

- cyber-security motivators positively and statistically significantly help create solid internal processes;
- cyber-security motivators positively and statistically significantly influence technological infrastructure;
- technological infrastructure positively and statistically significantly influences solid internal processes.

Also, it was found that standardized indirect effect of technological infrastructure was significant at level 0.05, which means technological infrastructure mediates the relationship between cyber-security motivators and solid internal processes, as shown in Figure 2.

Table 8. Amos results

Variable	Direction	Variable	Estimate	S.E.	C.R.	*P***
Technological infrastructure	←	Cyber-security motivators	.690	.070	9.857	***
Solid internal processes	←	Cyber-security motivators	.774	.073	10.568	***
Solid internal processes	←	Technological infrastructure	.267	.046	5.826	***

Table 9. Estimates for direct and indirect impact

Standardized direct effects		P	Standardized indirect effects	Standardized total effects
Cyber-security motivators → technological infrastructure	0.548	⋯,⋅**	–	0.548
Technological infrastructure → solid internal processes	0.255	0.001**	–	0.255
Cyber-security motivators → solid internal processes	0.588	⋯,⋅**	0.14	0.728

Note: ** significant at 0.05 level.

http://dx.doi.org/10.21511/ppm.18(1).2020.39

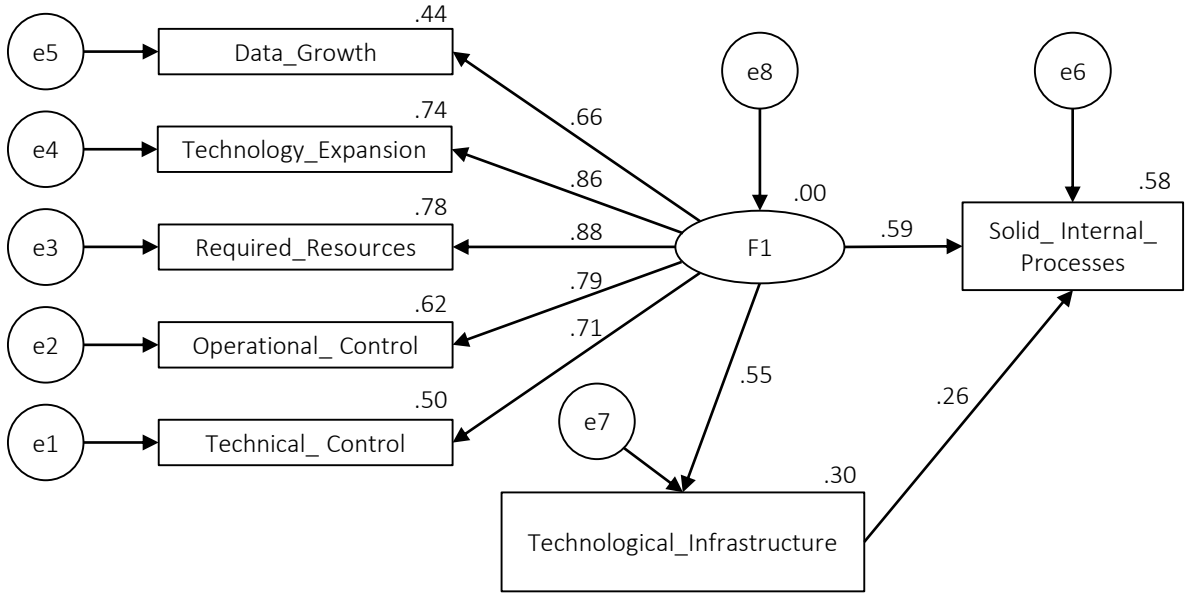

Figure 2. Chart for path analysis results

5. DISCUSSION

As was seen from previous section, which presented the results of analyzing the collected research data, it appeared that all presented hypotheses were accepted. The relationship between cyber-security motivators and solid internal processes is basically nourished and supported through the well-built technological infrastructure. The analysis showed that, based on the respondents' answers, technological infrastructure is one of the most important aspects that helps create a valid theatre for supporting a good level of cyber-security. From the analysis, it was seen that data growth is the most influential cyber-security motivator for solid internal processes, as it scored a mean of 4.2661, which indicate that the more data there is, the more intensive cyber-security should be, as the organization would be more exposed to hazardous attacks within the network. In the 2nd tank of influence came technical control, scoring a mean of 4.1296, which also appeared to be influential in managing the technical issues and plans for the cyber-security strategies, leading to a better fit of the organization and its internal processes.

The study results came to be intact with many studies that focused on the aforementioned variables like Haq (2019) who focused on the data expansion and growth and its role in increasing the exposure of the organization to attacks and dangers within the network. Also, Miron and Muita (2014) focused on the fact that many cyber-security motivators may appear as a hazard for the organizational internal process. Those motivators may vary from the widely famous motivators to the least known ones, which the organization might not be familiar with. However, the authors supported the fact that a well-built technological infrastructure may play a role in increasing the level of security within the organization and decrease levels of exposure towards many types of motivators. This was supported by the current study and appeared through the tested hypotheses, which pointed out the nature of the relationship between cyber-security, internal process, and the delegation of technological infrastructure. The results also supported a study by Stafford et al. (2018) in which the authors adapted to the relationship that gathers between technological infrastructure and cyber-security, arguing that the strength of technological infrastructure defines the strength of protection against cyber-security attacks. On the other hand, Yasin et al. (2018) saw the data growth and expansion, in addition to the technical support, as the first step towards building a cyber-security protective bubble to the organization. This was revealed according to what the authors said regarding the influence of data growth on the organizational internal processes, which highly depends on technology. Besides, the study results matched with Udo et al. (2018), Narukonda and Rowland (2018)

when they argued that in the current time, there are rarely an organization that can work excluded from internet and technology, which complicates its journey to achieve the set goals and, at the same time, collects the data that are massive and may expose the organization to different types of risks and hazards based on the availability of such data to other parties.

CONCLUSION

Based on the present study, cyber-security motivators positively and statistically significantly help create solid internal processes; cyber-security motivators positively and statistically significantly influence technological infrastructure; and technological infrastructure positively and statistically significantly influences solid internal processes.

Based on the results and conclusion, the current study recommended the following: increase the awareness of staff within an organization regarding the importance of infrastructure and the need to work on building it on a solid base. Continuous maintenance and monitoring of technical support is the main issue in managing any gaps that may appear and utilized by attackers and cyber creepers. Before adopting new technology, the organization should examine and test their current technology to find out the suitability of adopting new technology and, at the same time, avoid any possible risks for the organization.

AUTHOR CONTRIBUTIONS

Conceptualization: Yanal Kilani.
Data curation: Yanal Kilani.
Formal analysis: Yanal Kilani.
Funding acquisition: Yanal Kilani.
Investigation: Yanal Kilani.
Methodology: Yanal Kilani.
Project administration: Yanal Kilani.
Resources: Yanal Kilani.
Software: Yanal Kilani.
Supervision: Yanal Kilani.
Validation: Yanal Kilani.
Writing – original draft: Yanal Kilani.
Writing – review & editing: Yanal Kilani.

REFERENCES

1. Abu-Taieh, E. M., Al Faries, A. A., Alotaibi, S. T., & Aldehim, G. (2018). Cyber Security Body of Knowledge and Curricula Development. In *Reimagining New Approaches in Teacher Professional Development*. IntechOpen. https://doi.org/10.5772/intechopen.77975
2. Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), 1-15. https://doi.org/10.1093/cybsec/tyy006
3. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cyber-security. *Technology Innovation Management Review, 4*(10), 13-21. Retrieved from https://timreview.ca/article/835
4. Dewal, P., Narula, G. S., Jain, V., & Baliyan, A. (2018). Security Attacks in Wireless Sensor Networks: A Survey. In *Cyber Security* (pp. 47-58). Springer, Singapore. https://doi.org/10.1007/978-981-10-8536-9_6
5. Diego, A. B. B. O. (2019). *The Analysis of Cyber Security the Extended Cartesian Method Approach With Innovative Study Models*. Scientific Research Publishing, Inc. USA. https://books.google.com.ua/books/about/THE_ANALYSIS_OF_CYBER_SECURITY_THE_EXTEN.html?id=XouUDwAAQBAJ&redir_esc=y

http://dx.doi.org/10.21511/ppm.18(1).2020.39

6. Efthymiopoulos, M. P. (2016). Cyber-security in smart cities: the case of Dubai. *Journal of Innovation and Entrepreneurship, 5*(1). https://doi.org/10.1186/s13731-016-0036-x

7. Elamiryan, R., & Bolgov, R. (2018). Comparative Analysis of Cybersecurity Systems in Russia and Armenia: Legal and Political Frameworks. In *International Conference on Digital Transformation and Global Society* (pp. 195-209). Springer, Cham. https://www.springerprofessional.de/en/comparative-analysis-of-cyber-security-systems-in-russia-and-arme/16262586

8. Göztepe, K., Kılıc, R., & Kayaalp, A. (2014). Cyber Defence in Depth: Designing Cyber Security Agency Organization for Turkey. *Journal of Naval Science and Engineering, 10*(1), 1-24. https://www.researchgate.net/publication/274733863_Cyber_Defense_In_Depth_Designing_Cyber_Security_Agency_Organization_For_Turkey

9. Haq, Q. A. U. (2019). Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan. *International Journal of Computer Network and Information Security, 11*(1), 62-69. https://doi.org/10.5815/ijcnis.2019.01.06

10. Horowitz, B., Beling, P., Fleming, C., Adams, S., Carter, B., Sherburne, T., Elks, C., Bakirtzis, G., Shull, F., & Mead, N. R. (2018). *Cyber security requirements methodology* (No. SERC-2018-TR-110). Stevens Institute of Technology Hoboken United States. https://apps.dtic.mil/sti/citations/AD1057439

11. Keplinger, K. (2018). Is quantum computing becoming relevant to cyber-security? *Network Security, 9,* 16-19. https://doi.org/10.1016/S1353-4858(18)30090-4

12. Miron, W., & Muita, K. (2014). Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review, 4*(10). Retrieved from https://timreview.ca/article/837

13. Moreira, N., Molina, E., Lazaro, J., Jacob, E., & Astarloa, A. (2016). Cyber-security in substation automation systems. *Renewable and Sustainable Energy Reviews, 54,* 1552-1562. https://doi.org/10.1016/j.rser.2015.10.124

14. Narukonda, K., & Rowland, P. (2018). *The Perceptions of Cyber Security in High School Girls*. MWAIS2018.

15. Pak Nejad, M., Javadi, R., & Mohammadi, J. (2014). Influence of security information management in cyber environment on electronic banking efficiency. *European Online Journal of Natural and Social Sciences: Proceedings, 2*(3(s)), 2240-2248. Retrieved from http://european-science.com/eojnss_proc/article/view/3941

16. Pernik, P., Wojtkowiak, J., & Verschoor-Kirss, A. (2016). *National Cyber Security Organisation: United States*. NATO Cooperative Cyber Defence Centre of Excellence: Tallinn. Retrieved from https://ccdcoe.org/library/publications/national-cyber-security-organisation-united-states/

17. Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management, 11*(4), 489-510. https://doi.org/10.1515/jhsem-2014-0035

18. Poresky, C., Andreades, C., Kendrick, J., & Peterson, P. (2017). *Cyber Security in Nuclear Power Plants: Insights for Advanced Nuclear Technologies*. Department of Nuclear Engineering, University of California, Berkeley, Publication UCBTH-17-004. https://doi.org/10.13140/RG.2.2.34430.69449

19. Priyadarshini, I. (2018). Cyber Security Risks in Robotics. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* (pp. 1235-1250). IGI Global. Retrieved from https://www.igi-global.com/chapter/cyber-security-risks-in-robotics/203558

20. Rasekh, A., Hassanzadeh, A., Mulchandani, S., Modi, S., & Banks, M. K. (2016). Smart water networks and cyber security. *Journal of Water Resources Planning and Management, 142*(7). https://doi.org/10.1061/(ASCE)WR.1943-5452.0000646

21. Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., & Orgeron, C. (2018). Is the responsibilization of the cyber security risk reasonable and judicious? *Computers & Security, 78,* 198-211. https://doi.org/10.1016/j.cose.2018.06.006

22. Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law, 12*(2), 53-74. https://doi.org/10.15394/jdfsl.2017.1476

23. Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security, 22*(1), 42-75. https://doi.org/10.1108/IMCS-08-2012-0045

24. Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal, 33*(4), 410-424. https://doi.org/10.1108/MAJ-07-2017-1596

25. Sun, C. C., Hahn, A., & Liu, C. C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems, 99,* 45-56. https://doi.org/10.1016/j.ijepes.2017.12.020

26. Symantec (2016). *Internet Security Threat Report* (6 p.). Retrieved from https://www.nu.nl/files/nutech/Rapport-Symantec2016.pdf

27. Udo, G., Bagchi, K., & Kirs, P. (2018). Analysis of the Growth of Security Breaches: A Multi-Growth Model Approach. *Issues in Information Systems, 19*(4),

176-186. Retrieved from https://iacis.org/iis/2018/4_iis_2018_176-186.pdf

28. Vishik, C., Matsubara, M., & Plonk, A. (2016). Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms. In *NATO CCD COE Publications, Tallinn* (pp. 221-242). Retrieved from https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch11.pdf

29. Whyte, C., & Mazanec, B. (2018). *Understanding Cyber Warfare: Politics, Policy and Strategy*. Routledge. Retrieved from https://www.routledge.com/Understanding-Cyber-Warfare-Politics-Policy-and-Strategy-1st-Edition/Whyte-Mazanec/p/book/9781138640627

30. Yasin, A., Liu, L., Li, T., Wang, J., & Zowghi, D. (2018). Design and Preliminary Evaluation of a Cyber-security Requirements Education Game (SREG). *Information and Software Technology, 95,* 179-200. https://doi.org/10.1016/j.infsof.2017.12.002

http://dx.doi.org/10.21511/ppm.18(1).2020.39