A CYBERSECURITY AND DIGITAL RISK ASSESSMENT: A FAMILY CASE STUDY

Suha Khalil Assayed

Faculty of Engineering and Information Technology, British University in Dubai, UAE

ABSTRACT

Digitalization is not limited merely to business companies and high-tech industries; it has increasingly changed families' behaviors and attitudes as they are exposed to the digital world using different technological aspects. Therefore, numerous risks can be raised between all members of the family. For example, if IoT devices in a smart home are not embedded with high-security standards, they would be vulnerable to being attacked by hackers. Cyberattacks will not be limited to attacking virtually, but also they could unlock the home's door from the phone, and accordingly, the criminal will enter the home, and they can lose much more than credit cards. In this paper we identified various types of risks, with providing an analysis about the vulnerabilities and protecting families from digital attackers.

KEYWORDS

cybersecurity, risk assessment, family, digital, hacker, cyberattack

1. INTRODUCTION

Digital transformation plays an essential role in improving the quality of life, it impacts the daily lives of people. However, the digitalization is not limited merely to the business' companies and high tech industries; it has increasingly changed families' behaviors and attitudes as they are exposing to the digital world by using different aspects of technologies [1]. Accordingly, numerous risks can be raised between all members of the family. As most families are increasingly, using the mobile devices for the social networking such as Twitter, Instagram, Facebook, and TikTok [2]. In fact, due to the properties of digital of information, digital system as well as digital network, an effective risk management strategy should be implemented between all family members. Using different kind of digital information can raise the digital risk since e-marketing and e-business grow rapidly and many people are addicted purchasing online different items of clothes, electronics, and others. Thus, the companies could use a cookies or other tools which all embedded in these business websites in order to collect different information about customer's behaviors [3]. However, this data could be combined with other data from the social media which might cause a privacy invasion of these customers. On the other hand, some companies might sell this privacy information to other adverting companies. Hence, government should educate families about preventing such risks [4], as some companies such as Google, adopted some techniques into the browser called " Do Not Track" as it can prevent the websites to collect information from the visitors. On the other hand, the properties of digital system, as nowadays, microchips and different hardware such as cameras, mobiles, and other devices could be designed and updated easily by using an affordable resource in terms of human skills as well as financial resources. Therefore, designing such devices might not have embedded with high security standards, and accordingly it would be vulnerable to be attacked by hackers [5]. For instance, some people designed a smart home with using the (IoT) and connecting different

DOI:10.5121/cseij.2023.13204

devices at home by using the Internet and computer systems. For example, the lighting system and the security alerts as well as the main doors could be locked and controlled by mobile app.

Henceforth, cyberattacks will not be limited to attack virtually, but also they could unlock the home's door from the phone and accordingly the criminal will enter the home and they can lose much more than credit cards num. Moreover, since Microsoft Windows are used widely in the world and it's integrated with different software and systems, many hackers attempt to target it by finding out any vulnerabilities into this operating system, therefore Microsoft is releasing yearly a "Microsoft Vulnerabilities Report" for providing an analysis about the vulnerabilities and protecting it by installing the security patches regularly [6]. Indeed, the digital network properties have a vital impact of the digital risk as all the digital functions are connected via the internet which is no central authority of the data besides it's very hard to identify the attribution of users.

1.1. DIGITAL RISK IDENTIFICATION

In order to identify the digital risk, we usually refer to the official government agencies reports, for instance in United States there are a Cybersecurity and Infrastructure Security Agency (CISA) and FBI Internet Crime Complaint Center (IC3), and the European Cyber Security Organization (ECSO) is a centralized entity in Europe for reporting and documenting the digital risks [7]. However, in other countries it could be different departments such as The department of Defense and the department of Homeland Security.

In fact, not all countries as well as companies would report to all incidents and threads. For example, the risk assessment depends on the assets that could be affected by the threats. The assets could be information, privacy data, hardware, laptop, photos, intellectual properties, reputation, and etc.

1.2. QUANTIFYING LIKELIHOOD AND IMPACT

The most popular method that used for quantifying the risk called the Bernoulli's model [8], which believe that individual accept risk on calculating the possible losses as well as calculating based on the utility that gained from the risky action from itself. However, the risk is calculated by having the economic loss in 1 $ (Impact) and multiplying it by the Probability of Loss (P) Risk= Impact * Probability

In general, different risk stakeholders have different values. So the impact should be given in order to be able to calculate the risk.

1.3. RISK TREATMENT OPTIONS

1.3.1. Risk Reduction

Reducing the threat occurs by decreasing the probability of occurring the risk [9], however the risk could be divided in the below-mentioned cases: 1- Before- incident 2- After-incident.

Risk could be reduced before the incident by following the below actions:

- Keeping the systems updated by installing different security patches [10].
- Using a strong password in all the web portals.
- Using Firewall and Safeguard techniques [10].

- Installing Anti-virus software
- Employing a security engineer
- Using an effective backup for all data. On the other hand, the below actions can be taken after the incident:
- Reporting the incident to the government such as the police department.
- Informing the bank immediately for any online suspicious transaction.

1.3.2. Risk Transfer

Transferring the risk is implemented by shifting the risk from one person or organization to third party entity[11]. Usually the risk is transferred when the impacts of the risk is very high with low probability, it’s like paying someone else to accept the risk.

The cybersecurity policy can be purchased by the families in order to protect the following:

- Protecting the financial assets: Especially if any of the parents get hacked while using the credit cards during the online shopping, so the cybersecurity insurance could cover this loss.
- Psychologically damaged for kids for exposing them to unappropriated content or for cyberbullying.
- Reputation risk.

1.3.3. Risk Acceptance

Sometimes, parent and kids can accept the risk if there is a low impact with low probability to occur, for instance the parent could use a mobile app for purchasing from amazon platform even though, two years ago an instance happened with one user as he gets scammed

1.3.4. Risk Avoidance

The risk should be avoided by the family, if the impact and the probability of the risk is very high, for instance, if parents know that one particular website has very high likelihood to be hacked and their banking accounts could be hacked by the scammers, accordingly, they should avoid this risk and not using this website.

2. FAMILY SCENARIOS

2.1. Scenario 1

Purchasing products using range of websites for the cheapest prices

Risk A: Viruses and different malwares that could infect the mobile or the PCs.

Treatment: The risk reduction will be adopted by using the following actions:

- Family should reduce this risk by using a secured website such as starting the link with https, in order to be sure it’s safe and protected.
- Avoid using insecure Wi-Fi.
- Protecting the PCs by installing an updated antivirus software and keeping all software along with the operating system up-to-date.

Risk B: Attacking by Scammer: We might purchase some products and sending money to the provider without receiving any products.

Treatment:

The risk reduction will be adopted by using the following actions:

- Family should reduce this risk by using a secured website such as starting the link with http**s**, in order to be sure it's safe and protected.
- Try to validate the website by navigating the name by using the internet.

Risk C: Stealing our banking credential information by exposing to the username and the password of the Banking system.

Treatment:

This risk could be shared with other parts by adopting the risk transfer, as well as the risk reduction will be adopted by using the following actions:

- Using a protected credit card.
- Getting a temporary card for online shopping use.
- Keep tracking all transaction for any unfamiliar transaction.

Risk D**:** Privacy invasion

Due to the e-commerce is growing very fast, many companies use different platforms for selling their products which they might collect customers' information and accordingly they will be able to sell it to other advertising companies for financially benefits.

Treatment: Risk could be reduced by Avoiding giving any unneeded personal information to any online retailers.

2.2. Scenario2

Teenagers child uses social media to share artwork and political opinion.

Risk A**:** Exposing to the radicalisation and the extremists

Teenagers are living in the digital era, and they depend on using a digital content for processing their daily activities. Therefore, they would be exposed to read and follow inappropriate political content that are related to the radicalisation and the extremists [12]. Moreover, by using the internet, the individuals will be able to communicate easily with wrong people besides they will be able to meet periodically and virtually without being invisible to the formal authorities.

Onyango [13] highlighted the most platforms that are targeted by the extremists groups as the following:

1- Chatrooms:

It can be embedded into different platforms. Accordingly, they can use the chatrooms by violent extremist group.

2- Facebook:

Some extremist groups are avoid using the Facebook, and

Maybe, because it has tools of tracking and can link users with their places in specific times.

3- Twitter: The extremist groups might prefer this social media that others due to the hard of attribution, and accordingly the traceability of the identity will be very hard to be identifies.

4- YouTube: Many individuals use it due to the difficulty to trace the identity of the people, more over they would be able to share comments and contents between others.

5- Videogames: There are many teenagers are addicted into using the videogames, and they increasingly have their own char rooms which can be target it as well by the extremists groups

Treatment:

The family should reduce the exposure to the risk as it might have high probability:

- The awareness: By educating the teenagers about verifying these contents and guiding them to the right websites.
- Using a technical solution to prevent the unsecured contents, some Internet Service providers could suggest some tools for protecting child to be exposed to these extremists' groups.

3. Risk Assessment Matrix

According to the previous risk analysis, we can summarize the family risks strategy in the below table:

Risk Name	Probability	Impact	Risk Strategy	Actions taken to prevent/reduce the risk
Risk #1: Viruses and different malwares that could infect the mobile or the PCs.	High Probability	If the impact is limited to slow the programs or to halt some applications so it could be considered it's low-medium negative impacts	High probability with low impact the risk strategy is " Reducing the Risk"	Family should reduce this risk by using a secured website such as starting the link with http**s**, in order to be sure it's safe and protected. Avoid using insecure Wi-Fi. Protecting the PCs by installing an updated antivirus software and keeping all software along with the operating system up-to-date.
Risk #2: Attacking by Scammer: We might purchase some products and sending money to the provider without receiving any products	If the website is unknown then the probability will be very high	The impact will depend on the amount of money that used/ the value of the product	The probability is very high and if the impact is very high then the risk strategy should be a "Avoiding the Risk"	- Family should reduce this risk by using a secured website such as starting the link with http**s**, in order to be sure it's safe and protected. - Try to validate the website by navigating the name by using the internet.
Risk #3: Stealing our banking credential information by exposing to the username and the password of the Banking system.	This risk will be high probability to be happened if the website is unsecured and the online retailer is unknown.	The impact could be very high as it could affect the banking system.	The probability is very high and the impact could be as well very high so the risk should be avoided.	- Using a protected credit card. - Getting a temporary card for online shopping use. - Keep tracking all transaction for any unfamiliar transaction.
Risk # 4: Privacy invasion	Many advertising websites use the cookies and other tools to	The impacts varies from low- medium	The Risk should be reduced	**-** Risk could be reduced by Avoiding giving any unneeded personal information to any online retailers.

	collect information about the customers, so the probability could be high			
Risk #5: Exposing the teenagers to the radicalisation and the extremists	High probability, as the radicalisation and extremists contents are available in the websites and it's easy to be reached by teenagers.	Impacts could be very high	The risk should be avoided.	The awareness: By educating the teenagers about verifying these contents and guiding them to the right websites. Using a technical solutions to prevent the unsecured contents, some Internet Service providers could suggest some tools for protecting child to be exposed to these extremists groups.

4. CONCLUSIONS

Due to the properties of digital of information, an effective risk assessment strategy should be implemented between all family members. Using different kind of digital information can raise the digital risk since e-marketing and e-business grow rapidly and it has increasingly changed families' behaviors and attitudes. Accordingly, numerous risks can be raised between all members of the family. For example, smart homes should be embedded with high security standards to avoid hackers from taking control of some IoT devices. Moreover, many families prefer to purchase products using insecure websites, which can make them vulnerable to the hackers. Therefore, the risk assessment matrix can offer a clear representation of the risk analysis, probabilities and impact, which can protect the family from unexpected risk.

REFERENCES

[1] Neugebauer, R. (Ed.). (2019). *Digital transformation*. Springer Berlin Heidelberg.

[2] Ubaedillah, U., Pratiwi, D. I., Huda, S. T., & Kurniawan, D. A. (2021). An exploratory study of English teachers: The use of social media for teaching English on distance learning. *IJELTAL (Indonesian Journal of English Language Teaching and Applied Linguistics)*, *5*(2), 361-372.

[3] Bhatia, V. (2019). Impact of fashion interest, materialism and internet addiction on e-compulsive buying behaviour of apparel. *Journal of Global Fashion Marketing*, *10*(1), 66-80.

[4] Sun, Y., Luo, B., Wang, S., & Fang, W. (2021). What you see is meaningful: Does green advertising change the intentions of consumers to purchase eco- labeled products?. *Business Strategy and the Environment*, *30*(1), 694-704.

[5] Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. *Journal of Computer Networks and Communications*, *2019*, 1-14.

[6] Demetrio, L., Coull, S. E., Biggio, B., Lagorio, G., Armando, A., & Roli, F. (2021). Adversarial exemples: A survey and experimental evaluation of practical attacks on machine learning for windows malware detection. *ACM Transactions on Privacy and Security (TOPS)*, *24*(4), 1-31.

[7] Hinchman, D. B. (2022). Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity. Report to Congressional Requesters. GAO-23-105480. *US Government Accountability Office*.

[8] Monroe, T., Beruvides, M., & Tercero-Gómez, V. (2020). Quantifying Risk Perception: The Entropy Decision Risk Model Utility (EDRM-U). *Systems*, *8*(4), 51.

[9] Rana, J. S., & Pitroda, J. R. (2021). Risk analysis and mitigation technique in Indian transportation industries: A review. *Reliability: Theory & Applications*, *16*(SI 1 (60)), 132-142.

[10] Asaad, R. R., & Saeed, V. A. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. *Applied computing Journal*, 227-244.

[11] Pataci, H., & Ravichandran, T. (2022). INFORMATION SECURITY RISK AND BOUNDARY CHANGING BEHAVIOR.

[12] Firth, J., Torous, J., Stubbs, B., Firth, J. A., Steiner, G. Z., Smith, L., ... & Sarris, J. (2019). The "online brain": how the Internet may be changing our cognition. *World Psychiatry*, *18*(2), 119-129.

[13] Onyango, W. (2021). Digital Media as the Next Frontier for Fighting Violent Extremism among Youth?. *Securitizing Youth: Young People's Roles in the Global Peace and Security Agenda*, 191.