ISSN 2411-958X (Print)
ISSN 2411-4138 (Online)
European Journal of Interdisciplinary Studies
January - April 2021
Volume 7, Issue 1

Cybersecurity Awareness in Albania

Elvana Moci
Phd Candidate, University of Tirana,
Faculty of Economy

Abstract

The risk of a cyber-attack exist for every business. When a Manager of C level is in front of a cyber-attack or data breach, they begin to worry more about their vulnerabilities in the technology they use rather then about their employees. Creating a risk-aware culture in their workplace is the best way for managers of any level to fight this threat. Cyber security awareness is the way how to start this culture at work. The goal of this study is to measure the cyber security awareness of professionals in businesses in Albania, i.e. to verify specialists or managers have knowledge and understanding of basic cyber security threats. The survey consisted of 16 single and multiple-choice questions divided into three parts. The results categorized the respondents and measured the level of cyber security awareness. The results show an unsatisfactory level of knowledge regarding information security in Albania. The main conclusion drawn from the survey is that the quality of cyber security training among professionals should be improved and frequency of the trainings should be increased. With the pandemic situation caused from the Covid- 19 virus , many worker are working from home. This increase the chances that cyberattack. This is why cybersecurity awareness and training it is needed for the companies to avoid as much as possible the risk of cyberattack.

Keywords: Cybersecurity, Cybercrime, cyber awareness, Covid 19

Introduction

By definition the cyber security awareness is the combination of knowing and doing something to protect a business's information assets. When an enterprise's employees are cyber security aware, it means they understand what cyber threats are, the potential impact a cyber-attack will have on their business and the steps required to reduce risk and prevent cyber-crime infiltrating their online workspace. Creating a culture around cyber security awareness in the workplace doesn't mean that you'll be completely removing the risk of stealing the data or cyber-crime to your business. Malware has increased rapidly, and it is12 expect to see the evolution and growth of cyber-threats and malware to proliferate.

Your organization's cyber security is only as strong as your weakest employee, and a data breach is more likely to come from human negligence rather than a criminal hack. When you strive to create a risk aware culture within the workplace, you're preventing your employees from becoming unknowingly complicit in cyber-crime activity.

According to the 2018 Data Security Incident Response Report, phishing accounted for 34% of data breaches in 2017...One form of phishing, known as spear-phishing, is becoming increasingly difficult for employees to detect, posing a huge risk to organizations all over the world.

Spear-phishing is a malicious email-spoofing attack that aims to gain entry to software via malicious malware that's downloaded through an attachment. The perpetrators target specific organizations or individuals with the goal of gaining unauthorized access to sensitive information. If the person opens the attachment on the email, malware is then downloaded onto the user's computer. This gives hackers an entry into the organization's software, from which they can then move laterally in search of sensitive and valuable information. It is unusual for spear-phishing attempts to be initiated by random hackers with no end goal - they are more likely to be conducted by hackers who are out for financial gain, industry secrets and sensitive information.

With the pandemic of Covid 19 people are working more from home. This increase the risk of cyber attacks and cybercrimes.

People working from home should be aware on how to detect and react to phishing frauds, and other types of cyber-attacks. If they act immediately and thoroughly, then cybercrime damage costs can be contained and kept at the current level. If the carelessness due to lack of awareness will continue, it may cause heavy loss globally

As Warren Buffet says the cybercrime is the number one problem with mankind, and cyberattacks a bigger threat to humanity than nuclear weapons.

Methodology

The survey was created to test cyber security awareness in Albania in the private sector. The survey, set up as a cross-sectional study, was conducted in the second half of 2019. This survey was based on the cyber security recommendations from the European Union Agency for Network and Information Security. The same survey was applied in Poland in the healthcare sector.

The survey consisted of 16 questions where 3 were multiple choice questions. The questionnaire had 3 parts : the first part was information part where the respondents answered about the usage of electronic system , the second part contained questions about the knowledge releated to cyber security at work, and the third part with multiple choice answers contained scenarios on cyber attacs to valuate through scenarios the basic skills and knowledge of the respndents.

The survey was given to different employees in a company to cover different managerial level and seniority at work . In total were delivered 1000 questionnaires to 856 companies. The companies were SME companies as they make the majority of the companies in Albania. From 1000 we received only 421 valid completed surveys , whereas 579 were not valid or we didn't receive feedback.

There were :

Table 1 : The questionare and the answers per each group of questions

Part1	Electronic system usage at a business site	Yes	No
1	Did you have cyber security training at work?	244	177

2	Do electronic systems at your work facilitate your job?	358	63
3	Do you think that the electronic circulation of documents at your work is adequately protected	205	216
4	Do you use a mobile device (smartphone or tablet) to read electronic records	34	387
5	Can you copy financial records to a non-secured portable storage	204	217
Part2	Cyber security knowledge and skills:		
6	Do you know the legal consequences related to the public disclosure of a custmer's financial data?	301	120
7	Can you securely send a customers data records by email?	156	265
8	Are you aware of the existence of simple online tools that allow you to impersonate any email address?	78	343
9	Can you electronically sign documents?	289	132
12	Does a pdf file containing the scan of a printed and signed document have more legal value than a pdf document without an electronic signature (Albania)?	346	75
13	Is the software on your computer continuously updated?	103	318
Part3	Basic cyberattack scenarios:		
14	If you find a pen drive in a cafe, will you connect it to your computer at work? ...: (2 correct answers)	287	134
15	You received an email in your work inbox with information from the system administrator asking you to click on a link, log in, and confirm your password to conduct administrative tasks in the system. What will you do? ...: (3 correct answers)	259	162
16	You received medical documentation (in the form of a.pdf file) as an email attachment regarding a Customer . Can you trust that the documentation received is authentic? How can you check it? (multiple choice, 2 correct answers)	214	207

Table 2. Analysis of returned questionnaires

Classification	**Invite**	**Nr**	**Percentage**	**Percentage by classification**
Management	C level Managers	320	32%	69%
	Mid Level Managers	370	37%	
NonManagement	Officers	310	31%	31%
	Not Completed or Not valid			
Management	C level Managers	198	34%	64%
	Mid Level Managers	172	30%	
NonManagement	Officers	209	36%	36%
	Completed			
Management	C level Managers	122	29%	76%
	Mid Level Managers	198	47%	
NonManagement	Officers	101	24%	24%

Table 3. Results of correct answers of respondents to questions measured in terms of percentage

Part1	Electronic system usage at a business site	C level Managers	Mid Level Managers	Officers
1	Did you have cyber security training at work?	98%	88%	99%
2	Do electronic systems at your work facilitate your job?	100%	100%	99%

3	Do you think that the electronic circulation of documents at your work is adequately protected	80%	80%	35%
4	Do you use a mobile device (smartphone or tablet) to read electronic records	100%	100%	25%
5	Can you copy financial records to a non-secured portable storage	61%	34%	51%
Part2	Cyber security knowledge and skills:			
6	Do you know the legal consequences related to the public disclosure of a custmer's financial data?	82%	78%	25%
7	Can you securely send a customers data records by email?	61%	80%	15%
8	Are you aware of the existence of simple online tools that allow you to impersonate any email address?	44%	88%	55%
9	Can you electronically sign documents?	92%	94%	25%
12	Does a pdf file containing the scan of a printed and signed document have more legal value than a pdf document without an electronic signature (Albania)?	80%	53%	66%
13	Is the software on your computer continuously updated?	22%	84%	27%
Part3	Basic cyberattack scenarios:			
14	If you find a pen drive in a cafe, will you connect it to your computer at work? …: (2 correct answers)	55%	94%	34%
15	You received an email in your work inbox with information from the system administrator asking you to click on a link, log in, and confirm your password to conduct administrative tasks in the system. What will you do? …: (3 correct answers)	69%	96%	49%
16	You received medical documentation (in the form of a.pdf file) as an email attachment regarding a Customer . Can you trust that the documentation received is authentic? How can you check it? (multiple choice, 2 correct answers)	70%	90%	81%

To determine the general knowledge regarding cyber security awareness in SME in Albania, each answer within the group of respondents was calculated as independently to question in the survey. The percentages shown in Table 3 indicate the number of respondents with knowledge regarding cyber security. Each correct response within the group of respondents was divided into three parts: electronic systems use at the healthcare site (Part I), cyber security knowledge and skills (Part II), and basic cyberattack scenarios (Part III).

Table 4: Averages of the Correct answer per different management or non-management levels

		C level Managers	Mid Level Managers	Officers
Part1	Electronic system usage at a business site	88%	81%	62%
Part2	Cyber security knowledge and skills:	64%	80%	35%
Part3	Basic cyberattack scenarios:	64%	94%	54%
	Total Averages	***72%***	***85%***	***51%***

From the percentages of the correct answers we can see that the C Level Managers and the Mid-Level Managers has better knowledge. They answered respectively 88% of the C Level Managers that responded to the question ere correct answers for the Electronic System Usage at the Business site and 81 % of the Mid-Level Managers who responded to the questionnaire

responded correctly for this part of the questions. The Non mangers they have for the first part of the questionnaire 62 % correct answers. This means that the Management knows better than the non-management the Usage of the Electronic system usage.

Analyzing the part 2 of the questionnaire which had the purpose to check the cyber security skill and knowledge of the managers and non-managers of the businesses in Albania SMS- s , we can see from the results that the Mid-level managers had better knowledge and skills for the cyber security and the Non managers were the less skilled.

To the questioners were asked basic scenarios on the cyber-attack again to see the skills and how they would react on a scenario that involved a cyber-attack event. The results show gain that the Mid-level managers has better knowledge, they are more prepared to potentials events of an attack. The C Level Managers had again better knowledge and can react better to a cyber-security attack rather than the non-managers of the companies.

Checking the total of averages of the 3 parts of the questioner results that the Mid-level Managers of the companies in Albania have better knowledge to the cyber-attack and are more aware of the cybersecurity.

Conclusions

Colleagues need to understand the role they play in strengthening a business's cyber security. In most cases, it needs to be taken back to the very basics. Cyber-crime shows no signs of slowing down, and a cyber-attack has the potential to incapacitate an organization. Training the employees and making them aware is not only your best defense - it also shows you're paving your way to a more GDPR compliant future. It is crucial for businesses to implement the most basic cyber security measures, and cyber security awareness for employees is one of them.

The results of the questionnaire conducted in Albania shows that the non managers of the companies have a lack of knowledge and law cyber security awareness. The manager level showed to have better skills and knowledge rather then the non management roles. The results of the survey is not divided by industries in order to see in which industry its more relevant this gap. This analysis will be part of future investigations.

As we are in the area of the Digitalization , the cyber security awareness is very important to the protection of the assets. If managers want to keep their data safe, it is needed to educate their staff and create a workplace culture surrounding cyber security awareness. Hackers will always try and find a vulnerability, and when they do you need to make sure you have the resources , capability and knowledge to discover and respond to their activities as quickly as possible. Implementing a security information and event management (SIEM) solution will aggregate logs from applications, operating systems, and network infrastructure appliances across the enterprise . It's clear that the weakest point in cyber security is the human factor, and if the employees are unable to make an informed and educated decision about something as simple as what network to connect to or which email attachment to open, the businesses are at risk of a potential cyber-attack . That's why investing in cybersecurity training and awareness is a key element to reduce the risk.

References

[1] L. Fabisiak t.Hyla "Measuring cyber security awareness within groups of medical professionals in Poland" - Proceedings of the 53rd Hawaii International Conference on System Sciences , P 3880

[2] T. Ahmad Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity , 2020

[3] Online : https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[4] Online : https://www.ogl.co.uk/the-importance-of-cyber-security-awareness

[5] Online : https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf