The Employer and Employee Reputation in the Ukrainian Cyberspace and Social Internet-Services

Olena Rudnitska[1[0000-0001-8128-9595]], Svitlana Kondakova[1[0000-0003-0626-6849]], Anastasiia Kondakova[2[0000-0003-1302-2244]], Yurii Khlaponin[1[0000-0002-9287-0817]], Victoriia Ternavska[1[0000-0003-2102-619X]] and Yevhen Vasiliu [3 [0000-0002-8582-285X]]

[1] Kyiv National University of Construction and Architecture, Kyiv, Ukraine
[2] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
[3] O.S.Popov Odessa National Academy of Telecommunication, Odessa, Ukraine
y.khlaponin@gmail.com

Abstract. The article deals with the importance of the cyber hygiene in the relationship between the employer and the employee. Attention is paid to such aspects as employee cyber hygiene when working with company-own data and information. An experiment was conducted in a real company. The current state of cyber hygiene employees of the organization was studied and analyzed. The methods of counteracting and protection in case of violation of the rules of cyber hygiene by the employee are offered. The ways of getting additional information about the employee (also the potential one) are described for analyze of the digital identity. Some open state registers are analyzed for information about a person who would be useful in terms of forming a psychological portrait of the employee. Ways to obtain information from an employer company are described. Also attention is paid to the importance of cyber hygiene in shaping the company's image in the market.

Keywords: cyber hygiene, phishing, cyber kill-chain, cyber defense, online reputation, social internet-services.

1 Introduction

When employees access a company's data, they can manage it in an unpredictable way. Therefore, companies have to spend resources on tracking of so-called digital traces from available to them sources such as social networks, government registers, etc. This is how companies try to protect themselves and their clients from the harmful (conscious or not conscious) actions of their employees. It should also be noted that the reputation of some employees is significantly affected the reputation of company. Therefore, it is advisable for companies to track whether their employees comply with the cyber hygiene rules and what an impression the digital profile of a particular employee makes for customer (first and foremost important first persons of the company and those employees, who communicate directly with the customers).

2 Employee`s cyber hygiene when working with company - owned information and data. Counteraction/Protection methods at cyber hygiene violations employees

Cyber hygiene is aimed at protecting devices from viruses and malware as well as to restrict online access to personal data. A well-known approach to targeted Cyber Kill-Chain attacks suggest as the first aimed attack stage "reconnaissance". From how well it is done reconnaissance, that is, the amount and quality of data collected at this stage the success of the attack and its cost depends.

For the first time, the term Cyber Kill-Chain as a part of Intelligence Driven Defense model was used by Lockheed Martin Corporation in order to identify and prevent to cyber-invasion processes [1].

The collecting of information at this stage is been carried out with the help of Social Engineering in addition to the various software and technical methods of exploration. The distribution of phishing messages is one of these methods. Such messages look like messages from reliable source and often contain malicious attachments or links that lead to phishing resources. The goal of these actions is to steal sensitive information (such as credit cards and account information) or to install malware on the victim's computer. Phishing is a widespread type of cyberattack that each user needs to know to provide the protection they need.

With the help of such implementation of similar scenarios, the attacker also tries to gather information about the attacked object to increase the likelihood that the addressee will respond appropriately to the email.

The prevalence of various social networks, as well as the openness of their typical user, gives the attacker the opportunity to obtain information about the potential victim and make a compelling legend for the letter: the text of the cover letter, style of communication. The outcome of such actions often depends on the particular situation: who? when? what is the subject of the letter and what is the "payload" in the particular letter?

So, according to the official website of the Cyber-Police of Ukraine during the famous Petya attack, “one of the ways of spreading this virus was to send phishing (fake) emails on behalf of well-known companies or on behalf of the addressees with whom the correspondence was conducted. These emails contain links for downloading malicious applications (Word documents, PDFs, spreadsheets, and more). Therefore, you should be especially vigilant and not open such applications. We recommend that you receive confirmation of sending files from the recipient to other available communication channels (phone, sms, messenger) [2].

After several well-known mass attacks (WannaCry, Petya/Nyetya/NePetya) big organizations' security services create instructions and carry out the training of the staff as to the malicious correspondence. Now the attackers have to extract extra efforts to deliver "payload" to Inbox and made the attacker to take the necessary action so as not to arouse suspicion.

The authors of the article conducted an experiment in which the current state of cyber hygiene was investigated and analyzed on the example of employees of the organization. In order to avoid compromise of the company, its name will not be indicated.

To collect the information, a fake site Cybersecure was created at https://cybersecure1.github.io/mobirise/. It was created on a free domain, emphasizing its inability to be official. For Social Engineering, feedback forms have been created that let you know the interests of employees at work, during leisure activities, as well as other personal information. This can be used by an attacker to retrieve user passwords.

It was formed an email, very similar to the official N organization email, from which usually the messages are being delivered were. It is noticed in the message that there is the organization involved in scientific and educational activities in the field of cybersecurity. It is ready to cooperate and, as a result of a similar line of business, wants to become a friendly partner of Organization N. Therefore, it was decided to take into account the view-points of all the staff as to the content of the Cybersecure's website, and to organize joint leisure activities in order to strengthen communication between organizations. Furthermore it was a request to state their wishes about the content of the site, as well as the joint leisure. The persons who answered the first letters the correspondence has being prolonged. In the process of this correspondence the private personal information of the individuals were defined that could give the attacker an opportunity to pick up a password from the email account. Because as to the statistical data users enter the password ignoring the rules of cyber hygiene, taking into account their interests, and not changing theme depending on the resource. Therefore, incorrect authentication takes the second place in the OWASP TOP 10 for many years.

In order to investigate in detail the problem of non-compliance by cyber hygiene workers with the general population of people who are responding to phishing, a sample was investigated - people working in organization N. The above said letters where send to 120 employees. 56 employees, i.e.- 46.6%, followed the links held in it.

The age and the position of the employees were taken into consideration in our statistical study.

Using the methods of one-way ANOVA, the null hypothesis of the absence of influence of the specificity of the department's work on compliance with the rules of cyber hygiene was tested.

The experiment considered four levels of factor A. For this purpose, the above said phishing letters were sent for the staff of 4 departments.

A1 - Law Department;

A2 - Finance Department;

A3 - IT department;

A4 - Customer Service Department.

There were 5 phishing attacks. The value of a random variable corresponds to the percent of department employees who answered each phishing letters. The experimental data are presented in the Table 1.

The total average (in percentage) of company employees who replied phishing

$$\bar{x} = 30{,}17\% \quad Q_{overall} = \sum_{i=1}^{5}\sum_{j=1}^{4}\left(x_{1j} - \bar{x}\right)^2 = 11{,}75.2,$$

$$Q_{factor} = n\sum_{j=1}^{n}\left(\bar{x}_j - \bar{x}\right)^2 = 6{,}580.7,$$

$$Q_{res} = Q_{overall} - Q_{factor} = 5{,}144.5.$$

F test statistic $\mathrm{F_{exp}} = \frac{\mathrm{m}}{(\mathrm{m}-1)(\mathrm{n}-1)}\frac{\mathrm{Q_{factor}}}{\mathrm{Q_{res}}}$=0.53

Table 1. Experimental data

Test number	Department			
	A1	A2	A3	A4
1.Click on the link	15%	15%	8%	26.35%
2.Contact details, messages	56%	51%	2%	80%
3.Leisure suggestions	48%	49%	2%	80%
4.vacation schedule	36%	30%	-	68%
5.Information about children	10%	15%	-	12%
	33%	32%	2.4%	53.27%

According to the Upper critical values of the F distribution for $\mathrm{k_1} = \mathrm{m} - 1 = 3$, numerator degrees of freedom and $\mathrm{k_2} = \mathrm{m(n-1)} = 16$ denominator degrees of freedom and 5% significance level $\mathrm{F_{cr}}(0.05; 3; 16) = 3.24$.

That is, the null hypothesis was confirmed that the variability of group averages is not affected by the specificity of the departments under study. The factors of work experience in the organization and the level of salary were similarly considered. Only in the latter case was the null hypothesis refuted.

For each of the phishing attacks, a two-dimensional statistical distribution of the sample is constructed, which uses the criterion of employees' age and level of position.

Table 2. Age / position dependence

age, X position, Y	20-30	30-40	40-50	50-60	60-70	n_Y
1.Ordinary employee	6	11	12	7	1	37
2.Head of department	1	4	1	1	0	7
3.Employee of Financial \ Legal Departments	0	1	3	5	1	10
4IT specialist	1	1	0	0	0	2
n_X	8	17	16	13	2	$n = 56$

Mean values of the sample mean $\bar{x} = 42$age, position level $\bar{y} = 1{,}5$ mean square deviation -$\sigma_x^* = 11{,}4, \sigma_y^* = 1{,}04$. Selective correlation coefficient $r^* = 0{,}45$. Selective equations of straight regression lines

$$\bar{y}_x = 1{,}5 + 0{,}45\frac{1{,}04}{11{,}4}(x - 42) \text{ (} \bar{y}_x = 0{,}04x - 0{,}22 \text{ after simplification}$$

$$\bar{x}_y = 42 + 0{,}45\frac{11{,}4}{1{,}04}(y - 1{,}5) \text{ (} \bar{x}_y = 4{,}9y + 34{,}6 \text{ after simplification}$$

built on Fig. 1

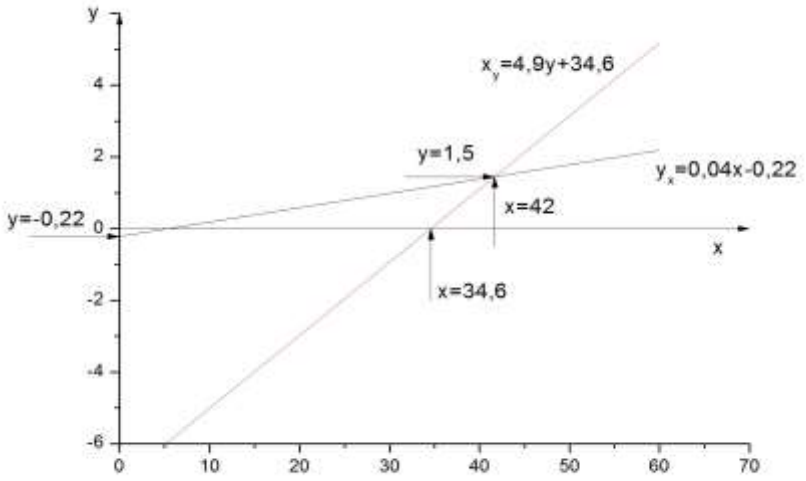

Fig.1. Given dependence

According to the statistics obtained criterion $T_{exp} = 3{,}7$.. The observational value exceeds $t_{cr}(0{,}05; 56 - 2) = 2$, that found in the table of Student's critical distribution points at a significance level of 5%, so we accept the competing hypothesis of correlation of age and level of position in the sample of employees responding to phishing. The correlation coefficient on the aggregate belongs to the interval

$$r \in \left(0{,}45 - 3\frac{1 - 0{,}45^2}{\sqrt{56}}, 0{,}45 + 3\frac{1 - 0{,}45^2}{\sqrt{56}}\right)$$

or $r \in (0{,}13; 0{,}77)$.

Given that the sample volume exceeds 50, the critical limit for normal distribution at the same significance level of 5% is assumed to be 3.

In order to minimize the likelihood of phishing attacks, after analyzing the results obtained, the company has developed a set of measures aimed at increasing the level of cyber hygiene in various departments, such as the Code of Conduct for Employees Suspicious of Attack and training on the basics of cyber hygiene. All employees of the company must not only know and follow the rules, but also understand what they will do in the event of an attack.

3 Ways to get additional employee information (including potential) for analyzing his or her digital identity

There are methods of forming a psychological portrait of a person on the basis of "traces" left in social networks. The set of psychological methods and techniques for assessing and predicting human behavior based on the analysis of the most informative features, characteristics of appearance, non-verbal and verbal behavior is called profiling. “Initially, the term “profiling” was used in the context of compiling a searchable psychological portrait (profile) of an unknown person following the crime scene. The methodology of criminal profiling involves handling criminal proceedings and interpreting evidence. The result of the work of the profiler is a criminal profile - a legally significant document that describes the identity and behavior of the offender and the victim in the key to the crime or series of crimes. The modern paradigm of profiling has several origins: the study of criminologists, forensic specialists, psychiatrists and criminal psychologists» [3].

Due to the complexity of obtaining adequate psychological portraits, this method is not common in the selection of candidates. It should also be kept in mind that there is a possibility of conscious (or unconscious) constructing one's digital identity. International cybersecurity experts say it is estimated that 80% of people in the digital world will have their "avatar" by 2023. Therefore, it is important for the employer to have impartial information about their employees.

Thanks to the public registers opened in Ukraine, a mechanism for getting up-to-date information about a person or a company has appeared. This mechanism can be used by both attackers to collect data and to protect against intruders. For example, when hiring a new employee, such data can protect the company from hiring fraudulent individuals and to track potential conflicts of interest.

To verify the digital identity of a potential employee, it is advisable to use the following resources:

1. State Migration Service of Ukraine https://dmsu.gov.ua/diyalnist/opendata.html

2. Investigative records of the Ministry of Internal Affairs https://wanted.mvs.gov.ua/

• Persons hiding from power https://wanted.mvs.gov.ua/searchperson/

• Verification of the legitimacy of a criminal record certificate https://wanted.mvs.gov.ua/test/

• Search for Ukrainian citizen's passport among the stolen and lost https://wanted.mvs.gov.ua/passport/

3. Free query Ministry of Justice of Ukraine https://usr.minjust.gov.ua/en/freesearch - free search of information in the Unified State Register of Legal Entities, Individual Entrepreneurs and Public Formations.

4. The Unified Register of Debtors https://erb.minjust.gov.ua/#/search-debtors, here you can find, for example, alimony debt and more

5. Automated enforcement system https://asvpweb.minjust.gov.ua/#/search-debtors Search is possible by type of debtor or type of collector

6. Judicial power of Ukraine https://court.gov.ua/

Unified State Register of Judgments https://court.gov.ua/reyestri-ta-sistemi/

Status of court proceedings https://court.gov.ua/fair/

7. OpenDatabot https://opendatabot.ua/ - service of monitoring the registration data of Ukrainian companies and the court registry for protection against raider seizures and control of counterparties.

8. Open data portal https://data.gov.ua/

9. State Fiscal Service of Ukraine http://sfs.gov.ua/. Here you can find out more about your business partner http://sfs.gov.ua/businesspartner

10. Peacemaker https://myrotvorets.center/ - Center for Investigating Signs of Crimes against Ukraine's National Security, Peace, Human Security and International Law.

Social networks. Although information from social networks is an important tool, it should be understood that it may not be the only basis for decision making. This is primarily due to the fact that deliberate discredit (or vice versa) is not excluded. Therefore, this information requires due diligence. Social networking examples: Facebook https://www.facebook.com/, LinkedIn https://www.linkedin.com/

4 Ways to get information about a potential employer

As a company runs the risk of collaborating with people with a negative reputation, the job seeker should check the company's reputation beforehand to avoid the negative effects of possible cooperation.

Checking the employer

To check the employer in Ukraine, it is advisable to use the YouControl system [4] - online company verification service [12].

This system uses only official sources of information from 60 registers. The following is not a complete list of information that can be obtained from this resource.

Financial scoring. It predicts the likelihood of a bankruptcy risk approaching the company and also compares the financial position of the company with other competitors. Such information may be useful, for example, when choosing a company to collaborate with or deciding whether to extend a contract [13].

The MarketScore index gives you an opportunity to find out the place of the company in the industry and the dynamics of its growth compared to its competitors.

This information is useful, for example, when you need to select a potential client or contractor or compare a counterparty with other companies in the market.

Company affiliation to the Financial Industry Group (FIG). With this tool, you can verify a company as a member of a group with reputational problems and check for plagiarism in the name, as well as identify the key persons of the group of companies.

Legal personality: Can this contractor provide and receive services. The counterparty can be in the status of "company started bankruptcy procedure", "there are bankruptcy information", "there are documents of bankruptcy of VSU" - this means that the company has started bankruptcy procedure, ie it does not have money to pay its obligations to other counterparties. The counterparty may also be in a "discontinued" status, which means that the company is closed and no longer operates. It is not worth and impossible to work with.

Company lifetime: Does the counterparty have experience?

Information about executives. The manager is the main authorized person in the company. First of all, make sure it has no restrictions. Otherwise, after the conclusion of the agreement, say 800 thousand hryvnia, you can later find out that its powers are limited to 250 thousand decisions. In this case, the contract may be declared invalid. In addition to possible restrictions, the Dossier must be checked to see if a manager in the OOS or Crimea area is registered.

Share capital: is it enough to pay the debt.

The main financial performance of the company: profitability, debt and profit. This is enough to make a first impression of the success of the company, as well as to compare these facts with the information that the contractor himself gave you.

Is the company on the sanction lists? Here is information about personal sanctions against a company or individual.

Payday debt. If the counterparty does not fulfill its obligations to its own employees, how much responsibility will it treat the arrangements with you? Also, if employees of the company do not receive their salaries on time, can they be sure of the quality of their work?

Presence of open criminal proceedings.

Availability of courts with counterparties for non-provision of services. By checking your counterparty for good faith in fulfilling your obligations, you increase the chances of avoiding fraudulent contracts that can put your company at any time.

Presence of open enforcement proceedings on wage arrears. This risk factor may affect the quality of contractor performance of the assignments you have. Usually, it is from social given.

Future lawsuits: how responsibly the company fulfills the contractual obligations; the status of the counterparty in which he or she appears in court cases: defendant, plaintiff or 3rd person; what are the court cases in the company: administrative, criminal, etc .; whether the counterparty relates to a group of companies with fictitious features.

Licenses and permits available

Tax: Company fiscal information and debt information.

Cooperation with countries under sanctions.

Additionally, you can use the same resources that are listed in a potential employee's checklist to verify your company's reputation. In this case, you should also check the company management separately.

5 The value of cyber hygiene in shaping the company's image in the market

Attacking Iran's nuclear program using the Stuxnet malware has become possible, including due to a breach of cyber-hygiene rules by one of its employees. The use was made of "the possibility of distribution in an isolated environment (without Internet access) using flash drives (flash-net) or its own p2p network" [5]. In this example, the importance of employees' compliance with cyber hygiene becomes apparent. Less obvious is the need to keep cyber hygiene employees on social media. Usually, it is from social networks that the stage of finding information about a company and its employees is the attackers. Such actions often result in attacks on the company that have significant consequences for the company.

According to Deloite experts, in addition to the obvious effects of cyberattacks such as "regulatory penalties, costs associated with public response, costs of reporting events and enhanced safeguards", there are also obvious consequences that "may have long-term effects and hidden costs, including loss of reputation, disruption to the organization, loss of confidential information or other assets of strategic importance" [6, 10-12].

In addition, in the McAfee report, Russia has been named the world leader in cybercrime. "Our research has confirmed that Russia is a leader in cybercrime, manifesting itself in the skills of its hacker community and its ill-treatment of Western law enforcement," writes CSIS Senior Vice President James Lewis. Among other world cybercrime centers, the expert listed North Korea, Brazil, India and Vietnam [7-11].

6 Conclusions

An online reputation can both improve and stop business. Information wars have become a symbol of today. Attacking competitors, or simply attackers, can cause less damage to companies than financial crises, because in addition to destroyed documents and damaged equipment, they can cause much more damage to businesses.

Cybersecurity experts say that cyber hygiene cannot be forgotten because the contingent "adversary" is constantly evolving, becoming more sophisticated and better equipped. The level of knowledge of digital hygiene and cybersecurity currently available to employees of various companies (both public and private) does not meet the threats and challenges of today.

Our research has confirmed that, regardless of their core profession or position, company employees must be trained in cyber hygiene. Violation of cyber hygiene rules harms both the person who violates them and the company that the person works for. In order to prevent financial and reputational risks, the employer should be interested in training employees in this area first. Such cyber security awareness programs should primarily address the practical side of security, and each employee should understand their responsibilities and responsibility for providing security. It is good practice for employees to notify responsible persons that they have received a

phishing email, especially if it is noticeable that they have carefully worked on the mailing. In this case, even if the infection or leak has taken place, you can still quickly respond to the attack and take countermeasures.

References

1. ICS, Web-resource: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
2. Recommendations, Web-resource: https://cyberpolice.gov.ua/article/prosti-rekomendacziyi-dlya-zaxystu-vid-virusu-petya-1885/
3. Davydova Olga, Profiling in negotiations with persons received. collection of materials of the round table: psychological principles of supporting official activities of political enforcement offices, Kryvyi Rih (2017)
4. YouControl, Web-resource: https://youcontrol.com.ua
5. Cybersecurity, Web-resource: https://s3r.ru/wp-content/uploads/2013/12/Kiber_Bezop_---1_2013_28.pdf
6. Web-resource: https://www2.deloitte.com/en/pages/risk/articles/beneath-the-surface-of-a-cyberattack.html
7. New Global Cybersecurity Report Reveals Cybercrime Takes Almost $ 600 Billion Toll on Global Economy
8. Yu. Danik, R. Hryschuk, S. Gnatyuk, Synergistic effects of information and cybernetic interaction in civil aviation, Aviation, Vol. 20, №3, pp. 137-144, 2016.
9. A. Tikhomirov, N. Kinash, S. Gnatyuk, A. Trufanov, O. Berestneva et al, Network Society: Aggregate Topological Models, Communications in Computer and Information Science. Verlag: Springer International Publ, Vol. 487, pp. 415-421, 2014.
10. S. Gnatyuk, V. Sydorenko, M. Aleksander, Unified data model for defining state critical information infrastructure in civil aviation, Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, May 24-27, 2018, pp. 37-42.
11. Gnatyuk S., Akhmetova J., Sydorenko V., Polishchuk Yu., Petryk V. Quantitative Evaluation Method for Mass Media Manipulative Influence on Public Opinion, CEUR Workshop Proceedings, Vol. 2362, pp. 71-83, 2019.
12. S. Gnatyuk, M. Aleksander, P. Vorona, Yu. Polishchuk, J. Akhmetova, Network-centric Approach to Destructive Manipulative Influence Evaluation in Social Media, CEUR Workshop Proceedings, Vol. 2392, pp. 273-285, 2019.
13. A. Peleschyshyn, T. Klynina, S. Gnatyuk, Legal Mechanism of Counteracting Information Aggression in Social Networks: from Theory to Practice, CEUR Workshop Proceedings, 2019, Vol. 2392, pp. 111-121.