УДК 004.4 https://doi.org/10.51301/vest.su.2021.i3.24

[1]D. Berdysheva, [1]A. Askhatuly, [2]D. Yedilkhan*
[1]Kazakh national university after al-Farabi, Almaty, Kazakhstan
[2]Astana IT-University, Nur-Sultan, Kazakhstan
*e-mail: yedilkhan@gmail.com

REVIEW ON METHODS OF IMRPOVING INFORMATION SECURITY POSTURE OF THE COMPANY BY INCREASING END USER AWARENESS

Abstract. Employees can potentially expose their organizations to huge amount of cyber risk. This may happen through falling for phishing attacks, careless handling of sensitive data, or poor password management, many data breaches are directly or indirectly caused by user awareness issues. To tackle this, mature companies have implemented security awareness program initiatives. However, without fostering feelings of responsibility and accountability for cybersecurity among employees, these programs will not necessarily make an organization any safer or less vulnerable.

This article provides general review on different ways of establishing robust security culture within companies and building effective security programs. The report also discusses current approaches and challenges of implementing information security awareness programs.

Keywords: information security, human factor in security, cybersecurity awareness.

Building security culture. Establishing an organization wide culture of information security is top priority for the most security leaders and management. It cannot be denied that people represent the most important chain in resiliency program against attacks. Therefore, a security culture highly concentrates on behavioral change.

Study outlines several aspects which are crucial for establishing security culture in the whole organization, such as [1]:

- Leadership and communication – visibility of strong leadership among internal security team helps to build desired image of the function and as a result create a better security culture in the organization. As for communication, it is important to pay attention to tone and demeanor when communicating with other functions.
- Network and collaboration – security function should be well known across the organization.
- Vision of the company should be clearly shared on all levels of the organization and trust to the employees should be maintained, so no hidden agendas take place.
- Existence of an Advisory Board, which contributes to promotion of cybersecurity throughout the organization.
- Employee engagement, where importance of realistic simulation tests over training programs are highlighted. Employees in the Company should be viewed as an asset not weakness.
- Recruitment of security ambassadors – IT help desk is referred to be an important ambassador, since this function receives calls and emails and need to be involved from the very beginning
- Definition of meaningful metrics for security department which will help the business to understand what security is doing, what value the function is creating for enterprise. For example, correlation of the reduction in security incidents with relative costs over time.

Culture is a critical characteristic of establishing a security program that reaches all employees in the organization. It is important to understand that information security is not always something procedural and mechanical, it is people centric. The people aspect is further reviewed in the next sections of this article.

How to increase information security awareness. It cannot be denied how considerable amount of work, in both public and private sectors of various industries and businesses, heavily relies on IT systems. Hence, they must be secured and protected. Although, several techniques and policies exist that can be used to control users’ behavior, they are not always provide positive results. Most probably it can be explained by the fact that people are not aware of risks, the ways to protect information assets and manage the risk properly.

According to the US National Institute of Standards and Technology (NIST) delivering training programs is not sufficient for raising awareness. The key is to raise the awareness of people to properly understand and react to threats adequately [2]. It is important to highlight that while various organizations like governmental bodies and the private sector have made significant investments into technology to ensure information security, people are the main target of the most cyberattacks and often this fact is not taken into consideration. Therefore, the main idea behind any information security policy or program should be the change of people's behavior.

Any security awareness program is driven by the fundamental reasons like regulatory mandates, retaining assets, increasing value, ethical considerations (especially when it comes to management of personal information), protection from threats and risks (for example, financial loss, reputation). Information security and privacy awareness training program can be viewed from the perspective of regulatory, business, and personal benefits. Regulatory benefits include presentation of compliance with external information security, privacy laws and regulations, protection of personal data of employees and customers. Also, awareness program hugely contributes to the above-mentioned establishment of security culture and environment, protects public image of the enterprise.

There are different methods on how to increase the awareness on information security within the organizations, including posters, offline trainings, tests, videos, games, information security awareness content on intranet page, and simulations. The study was performed to examine those methods versus factors affecting cybersecurity awareness, such as [3]:

- knowledge on the vulnerability
- realizing an impact of attack
- recognizing that the attack can take place at any time
- ability to protect information during a real attack
- cyberresilience
- recognizing the importance of information security

The research shows that the most effective training methods for cybersecurity awareness are simulation based and instructor led methods. However, authors suggest using integrated method of simulation and online training for a large organization with a high number of employees. The prototype for evaluation and enhancing information security awareness using integrated approach is depicted in Figure 1 [3].

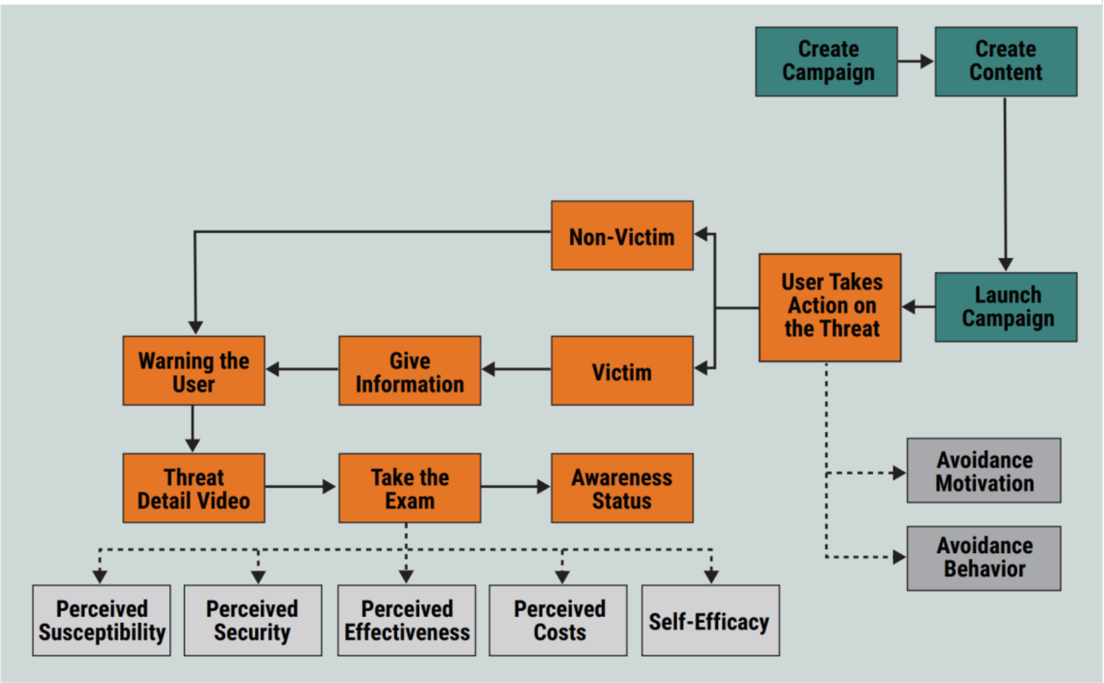

Figure 1. The prototype for evaluation and enhancing information security awareness

Almost all organizations' security programs include delivering training programs to employees to increase their awareness. However, this may not be sufficient for organization to cope with current security challenges and threats, because most such awareness programs are theory based. Therefore, it is important for management to exercise real life cyber incidents – so called cyberdrills.

Human behavior in information security. Various research projects and studies suggest that people are the most vulnerable part of the organization's security system. Currently available literature on the topic of human factor in information security propose raising awareness through trainings and education to ensure protection of sensitive data. Although individuals are provided with the trainings and most organizations establish punishment for violation of security procedures, security of sensitive information is still compromised by human factors such as errors, omissions or intentional actions.[7-9] The information security professionals should accept the fact that failure is inevitable in any human nature. Consequently, security program should be built as ongoing lessons learned process with due consideration about inevitability of failure [10].

Recent reports show that investments in security and information security are mainly concentrated on strengthening infrastructure through purchasing new technologies. For example, study indicated that the substantial amount of investment in data security was dedicated to security of perimeter infrastructure, while data treatment received the smallest amount. However, while investments in technological periphery get bigger, data treatment areas are the most exposed to threats [11-13]. Consequently, there is a need to revise the focus of investments in security from control of access towards control of use, where people and their behavior are important aspect in improving overall security of the organization [14].

Another study has determined that the minimum of five aspects are necessary to shape employees' behavior in relation to information security and control (Figure 2) [15]:

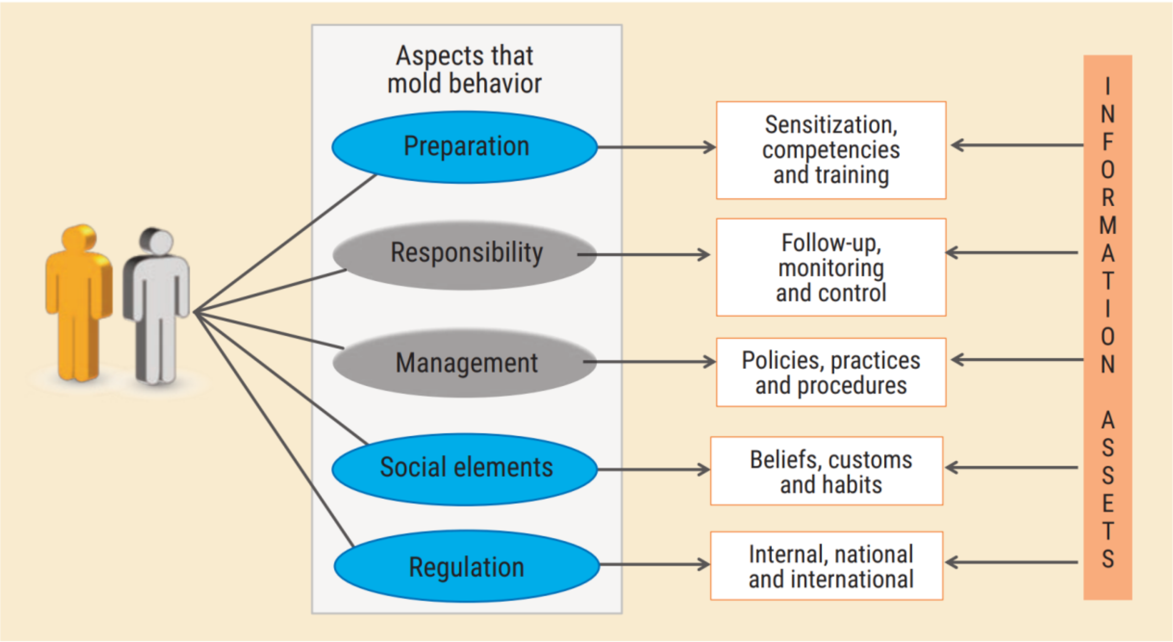
Aspects that mold behavior
Preparation
Responsibility
Management
Social elements
Regulation
Sensitization, competencies and training
Follow-up, monitoring and control
Policies, practices and procedures
Beliefs, customs and habits
Internal, national and international
INFORMATION ASSETS

Figure 2. Aspects that shape information security behavior

- Preparation, which means development of competency of employees in the secure management of data, understanding and implementing practice in the reality of business.

- Responsibility – individual decisions and execution of activities should be assisted by regular follow up, monitoring and control.

- Management – the practice to ensure stability of the organization's security and control activities.

- Social elements – consideration of people’s customs, beliefs, and habits in relation to data treatment provides an essential information for improving data protection.
- Regulation – internal and external requirements to ensure compliance with information security laws, personal data protection laws, and other privacy requirements.

Conclusion. Management of employees’ behavior is critical for establishing information security culture in any organization. In order to transform the way how people act in regard to data security and overcome present challenges, there is a need to move beyond simple safeguarding practices and trainings by recognizing significant attack directions, where vulnerabilities exist, and implementing security management practice that accepts inevitability of failure and takes advantage of each lessons learnt.

REFERENCES

[1] Cybercrime damages $6 trillion by 2021 // Cybercrime Magazine, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016.

[2] PwC 2015 Information Security Breaches Survey // PricewaterhouseCoopers UK.- United Kingdom,2015, https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

[3] Ponemon Institute, 2018 Cost of a Data Breach Study: Global Overview, USA, 2018, https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/

[4] Saurbaugh, M. Moving towards better security for today and tomorrow. ISACA Journal, 2020. № 2. P. 18-21.

[5] National Institute of Standards and Technology (NIST), “Information Technology Security Training Requirements,” Special Publication (SP) 800-16, USA, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

[6] Nachin N., Tangmanee C., Piromsopa K. How to increase cybersecurity awareness. ISACA Journal, 2019. № 2. P. 45-50.

[7] Bada, M.; M. A. Sasse; J. R. C. Nurse; “Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?” *International Conference on Cyber Security for Sustainable Society*, 2015, *https://arxiv.org/abs/1901.02672*

[8] Dreyer, P.; T. Jones; K. Klima; J. Oberholtzer; A.Strong; J. Welburn; Z. Winkelman; “Estimating the Global Cost of Cyber Risk: Methodology and Examples,” Rand Corporation, 2018, https://www.rand.org/pubs/research_reports/RR2299.html

[9] Alhogail, A.; A. Mirza; “Information Security Culture: A Definition and a Literature Review,” World Congress on Computer Applications and Information Systems, Hammamet, Tunisia, 17–19 January 2014

[10] Fuenmayor, R.; H. López-Garay; “The Scene for Interpretive Systemology,” Systems Practice, № 4, iss. 5, 1991, https://doi.org/10.1007/BF01104459

[11] Kuper, P.; “The State of Security,” IEEE Security & Privacy, September/October 2015, https://doi.org/10.1109/MSP.2005.134

[12] Cano, J.; “Administrando la Inseguridad Informática,” Revista Hakin 9, № 23, iss. 4, 2007, https://es.slideshare.net/heynan/hakin9-inseguridad

[13] Kuper, P.; “The State of Security,” IEEE Security &Privacy, № 3, iss. 5, September-October 2005, P. 51-53.

[14] Sieber, S.; J. Zamora;“The Cybersecurity Challenge in a High Digital Density World”, European Business Review, 18 November 2018, https://www.europeanbusinessreview.com/the-cybersecurity-challenge-in-a-high-digitaldensity-world/

[15] Ahmad, Z.; T. Ong; T. Liew; M. Norhashim;“Security Monitoring and Information Security Assurance Behaviour Among Employees: An Empirical Analysis,” Information & Computer Security, 12 June 2019.

[1]Д.Д. Бердішева, [1]А. Асхатұлы, [2]Д. Еділхан*
[1]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
[2]Астана IT-университеті, Нұр-Сұлтан, Қазақстан
*e-mail: yedilkhan@gmail.com

КОМПАНИЯНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН КҮШЕЙТУ МАҚСАТЫНДА ҚЫЗМЕТКЕРЛЕРДІҢ БІЛІМІН АРТТЫРУ ӘДІСТЕРІНЕ ШОЛУ

Аңдатпа. Қызметкерлер ұйымның ақпараттық қауіпсіздігін қамтамасыз ету жүйесіндегі ең әлсіз буын болып саналады, сол себепті олар мекемені көптеген киберқауіптерге ұшыратуы мүмкін. Көп жағдайда адамдар фишингтік шабуылдардың құрбаны болады, құпия деректерді қолдану ережелерін сақтамайды, немесе әлсіз парольдерді таңдайды. Көптеген сәтті кибершабуылдар тікелей немесе жанама түрде қызметкерлердің ақпараттық қауіпсіздік ережелері жайлы хабарсыздығынан болады. Ақпараттық қауіпсіздікті қорғауды жетік меңгерген мекемелер корпоративтік ресурстарды дұрыс пайдалану ережелері туралы тұтынушылардың білімін арттыруға бағытталған бағдарламаларды жүзеге асыруда. Алайда, қызметкерлердің деректер қауіпсіздігі үшін жауапкершіліктерін дамытпай, бағдарламалар өздерінің стратегиялық мақсаттарына жетуі екіталай.

Мақала ақпараттық қауіпсіздік бағдарламаларын тиімді жүзеге асыру арқылы қауіпсіздік мәдениетін құрудың әртүрлі тәсілдеріне жалпы шолу жасайды. Сондай-ақ, баяндамада ақпараттық қауіпсіздік бағдарламаларын жүзеге асырудың тәсілдері мен проблемалары талқыланады.

Негізгі сөздер: ақпараттық қауіпсіздік, ақпарттық қауіпсіздіктегі адами фактор, ақпараттық қауіпсідік жайлы хабардар болу.

[1]Д.Д. Бердышева, [1]А. Асхатулы, [2]Д. Едилхан*
[1]Казахский национальный университет им. ал-Фараби, Алматы, Казахстан
[2]Астана IT-университет, Нур-Султан, Казахстан
*e-mail: yedilkhan@gmail.com

ОБЗОР МЕТОДИК ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ КОНЕЧНЫХ ПОЛЬЗОВАТЕЛЕЙ В ЦЕЛЯХ УКРЕПЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

Аннотация. Сотрудники являются самым слабым звеном в системе защиты информационной безопасности организации, тем самым подвергая компанию огромным рискам. Люди не редко становятся жертвами фишинговых атак, небрежно обращаются с конфиденциальными данными или используют слабые пароли. Большинство успешных кибератак прямо или косвенно были связаны с пробелами в осведомленности конечных пользователей. Компании имеющие зрелые процессы защиты информационной безопасности реализуют программы по улучшению осведомленности пользователей о правилах пользования корпоративными ресурсами. Однако без культивирования ответственности сотрудников за сохранность данных, эти программы не достигнут своей стратегической цели.

В этой статье представлен общий обзор различных способов создания культуры информационной безопасности компании путем применения эффективных программ. В докладе также обсуждаются текущие подходы и проблемы реализации программ по повышению осведомленности в области информационной безопасности.

Ключевые слова: информационная безопасность, человеческий фактор в информационной безопасности, осведомленность о кибербезопасности.