How to Improve Awareness

5

5.1 INTRODUCTION

The results of the reported investigations in this book suggest that to improve the security of people in cyberspace, knowledge and awareness plays a vital role in enhancing security. We need to understand that simply having knowledge is not enough. As the famous Chinese proverb from Confucius puts it: "The essence of knowledge is, having it, to apply it." Consequently, the knowledge given to people must be applied so that they can benefit from it in their cyber lives. Our survey results indicate that even when people know about cyber risks, they are still not always taking practical actions to protect themselves. In this chapter, we will review the literature on awareness and training programmes and then discuss some potential solutions.

A significant number of security breaches are due to users' lack of knowledge or unsafe behaviours such as sharing passwords and opening unknown emails and attachments. These activities potentially open up the organization or individuals to threats from hackers and to the loss of assets of individuals and organizations.

Although organizations and enterprises invest and rely more on technology for security solutions (e.g., firewalls, antivirus software, and intrusion detection systems) and to defend organizational assets, the importance of considering the role of users in the security equation has grown. On the one hand, users/employees need to understand security issues, while on the other hand, they must follow the security policies of each organization, which become crucial to comply with information security (IS) laws and regulations.

Despite the role of users, there are huge investments in defensive technologies, but little investment in human awareness.

The first step in improving awareness is to measure it among each targeted group. The aim of awareness measurements is to use a reliable methodology to measure awareness in cybersecurity. Combinations of three different methods are used to measure awareness mostly among employees of a company. Questionnaires and surveys are used to measure knowledge (what you know), attitude (what you think), and behaviour (what you do) [23].

Model-driven techniques and survey-based research are also used to investigate behaviour modelling in the security context such as information-sharing and security policy compliance [69] as well as computer security behaviour while interacting with email attachments [70].

Egelman and Peer [71,72] developed the Security Behavior Intentions Scale (SeBIS), to measure the intention of security rules that end users employ while interacting with a wide variety of security controls and interfaces.

To improve the awareness of employees, many vendors have gradually formed several programmes. However, there are not many studies investigating the effectiveness of their outcomes. Most of the existing studies focus on three areas: awareness (measurements, security training, content for security training), delivery methods, and programme effectiveness measurements. In the following section, we will review each area.

5.2 TRAINING AND EDUCATION

Looking at all types of training offered, we classify them in the following four groups: formal education, professional training, employee training, and people training.

5.2.1 Formal Educational Programmes

Different formal education programmes are offered as a degree or specialized courses to train future professionals. Even though the number of educational programmes to educate information technology (IT) professionals is not enough to match the demand, they are gradually growing in numbers and continue to evolve and improve. Most cybersecurity educational programmes require at least a bachelor's degree in a related field to get started. The content of each programme mainly includes specific technical areas such as the following:

- Legal issues in information assurance
- Network programming
- Secure electronic commerce
- Discrete structures
- Computer forensics
- Audits and regulations
- Cryptology
- Computer security
- Database security
- Database design.

These types of educational programmes are not the focus of this book since their objectives are to educate and train IT professional.

5.2.2 Training Programme for IT Professionals in the Industry

A second group of educational programmes includes the hundreds of training workshops, certificate programmes and tutorials of all kinds offered by private companies, training institutions and individuals on a variety of technological tools, technical topics, and solutions. These types of educational programmes are also not the focus of this book since their objective is to educate the professional workforce.

5.2.3 Employee Training

With the growing number of companies that have become victim to cyber-attacks, the protection of information systems and information assets from cybersecurity threats has become critical. Despite this fact, most companies do not provide training but are still more reliant upon technology to resolve their cybersecurity issues. Thus, employees often lack cybersecurity knowledge and skill sets and are identified as susceptible threat vectors by cyber-attackers and are, therefore, being targeted with continually evolving threats [73].

Despite considerable investment in organizational security, the majority of the approaches and protection methods focus heavily on external attacks and technological defences and have not minimized the number of security incidents [74]. However, Abawajy [75] points out that the organization is only as secure as its weakest link. Stanton et al. [76] stated that even the best technology efforts intended to address IS would fail unless the organization's employees take the proper courses of action when approached with a threat.

Although technology-oriented safeguards such as firewalls and intrusion detection systems are found in a large number of organizations, the focus on human factors in security including awareness and training initiatives has historically lagged behind [77]. Previous studies in IS literature have confirmed awareness techniques to be effective in increasing employee security-related knowledge and promoting security-conscious decision-making. However, the benefit of an educated general business community is limitless [78]. Technology alone cannot solve a problem that is controlled by individuals.

5.2.3.1 Security Education, Training, and Awareness programmes

A Security Education, Training and Awareness (SETA) programme is designed to reduce the number of security breaches that occur through a lack of employee security awareness. These programmes mainly explain the employee's role in the area of IS. A SETA programme is generally offered as part of the employee orientation programme. The main content of a SETA is to explain each organization's security policies.

5.2.3.2 Cybersecurity countermeasures awareness

Cybersecurity countermeasures awareness (CCA) is the state where individuals are aware of their cybersecurity mission within the organization. In general, a CCA programme

includes SETA programmes, computer monitoring, and various security countermeasures to make people aware of their cybersecurity mission within the organization.

5.2.3.3 Cybersecurity skill

This programme aims to improve an individual's technical knowledge, ability, and experience surrounding the hardware and software required to execute IS in protecting IT against damage, unauthorized use, modification, and/or exploitation.

5.3 SECURITY TRAINING CONTENT

While training programmes and initiatives exist within many organizations, there appears to be limited empirical research to determine which topics should be covered, what the most useful delivery methods are, and to what degree these factors play a part in the IS practice of employees [79].

A study of 252 global organizations found nine principal cyber-attack vectors, most of which focused on the human factor in IS including viruses, malware, web-based attacks, phishing and social engineering, malicious code, denial of services, and stolen devices [80].

Comparative research among the different training programmes concluded that there are no statistically significant mean differences on employees' CCA and cybersecurity skills (CyS) between the two SETA programme types (typical and socio-technical) [81].

5.4 DELIVERY METHODS

The training delivery methods to improve awareness among employees or IT professionals are the subjects of several studies. Even though there are no conclusive reports that illustrate what approach would be the best, there is some indication of what would work better and these are worthy subjects to the discussion. Overall, the following training delivery techniques can be identified:

- Face-to-face training or classroom
- Online training
- Online instructor-led training
- Games
- Competitions
- Mass media: posters, emails, podcast newsletter, etc.

Abawajy (2012) reviewed the literature and investigated the user preferences of cybersecurity awareness delivery methods. Although people often express interest in a classroom-based delivery method, this is relatively expensive and provides a "static

solution for a fluid problem" [82]. Also, many users find it to be boring and ineffective [83]. In general, the success of classroom training depends upon the ability of the instructor to engage the audience. It might also tend to fail because it is based on rote memorization and does not require users to think about and apply IS concepts [84].

Sharing experiences and knowledge between the employees of an organization facilitated by participation makes classroom training more effective [85]. However, this approach assumes that participants are knowledgeable about the subjects being discussed.

Despite the extensive use of online training sessions in many companies, there is no conclusive evidence that online standardized courses are effective enough to create a successful security culture in an organization.

The use of games to train people has been growing. Games are good tools to motivate people to focus their attention on specific issues. However, no evidence has been found on how effective they are. "Serious games" (defined as games with a purpose other than pure entertainment) are used in training IT professionals to explore solutions or issues, but these are not effective in educating ordinary individuals.

5.5 TRAINING AND AWARENESS PROGRAMME EFFECTIVENESS

No matter what type of training is used to improve cybersecurity awareness, it is more important to measure its success in not only educating employees of their knowledge of cybersecurity, but also to see if and how they integrate this awareness into their everyday practice and behaviour. It is also essential to measure the effect of awareness training on the actual behaviour of the trainees.

Egelman et al. developed the SeBIS [86], a 16-item, scale-based instrument to measure the intention of security rules that end users employ while interacting with a wide variety of security controls and interfaces [87].

Some studies are conducted to measure programme effectiveness. For example, Parsons et al. [88] have developed a survey instrument (Human Aspects of Information Security Questionnaire – HAIS-Q) including a 63-item measure that assesses seven focus areas: password management, email use, Internet use, social media use, mobile devices, information handling, and incident reporting. Each focus area is further divided into three specific subareas resulting in 21 areas of interest, each of which is measured via a separate knowledge, attitude, and behaviour.

5.6 END USERS' TRAINING AND AWARENESS

In regard to end users, there have been field studies done to understand novice users' views about security practices and awareness [89]. An early field study on security-related employee behaviours, such as backup and file access practices, indicates

knowledge and informal heuristics as better determinants of behaviour than enforced security policies. Such qualitative investigations (interviews and field observations) enable an in-depth exploration of a narrow work domain, context, or demographics, but results from these may not be applicable to the larger population.

There is no specific training on how to train individuals to protect themselves in cyberspace aside from what exists in mainstream press and media.

5.7 A NEW APPROACH TO AWARENESS PROGRAMMES: ISSUES AND CHALLENGES

5.7.1 Cost of Security Awareness Training Programmes

According to www.infosecurity-magazine.com [90], the cost of security education for large enterprises is $290,033 per year, and about 94% of chief information officers surveyed have pushed for increased investment in user education following the recent headlines regarding phishing and ransomware. Almost all of them (99%) see users as the last line of defence against hackers, which means that user education, policies, and procedures are essential to ensuring that employees understand their role.

From the research point of view, no reliable and systematic study has been found that indicates how much this investment improves security. No data seems to be available in estimating the cost to develop security awareness for the general population. However, according to 2018 Identity Fraud: Fraud Enters a New Era of Complexity from Javelin Strategy & Research [91], in 2017 there were 16.7 million victims of identity fraud, a record high that followed a previous record the year before. Criminals are engaging in complex identity fraud schemes that are leaving record numbers of victims in their wake. The amount stolen hit $16.8 billion in 2017 as 30% of U.S. consumers were notified of a data breach, an increase of 12% from 2016. For the first time, more social security numbers were exposed than credit card numbers.

Numerous surveys and research studies have shown that ransomware is another area of growing concern for businesses, governments, and personal threats. While there is no precise data about how much this costs individuals, it has been reported that each occurrence yields an average of $1,077 for criminals [92].

Knowing that the cost of cyber-attacks is exponentially growing for the population, if we add the costs of all identity thefts, ransomware, and all enterprise costs of data breaches due to human error, we see that these costs far surpass the amount of money being invested in raising awareness in the overall population.

5.7.2 Changing People's Behaviour

In order to improve people's awareness of cybersecurity (not just their knowledge but also how to implement better behaviours into their everyday lives), one must

come up with structural solutions that address people at an early age. Much like other behaviours ensuring safety and security (such as locking their cars or homes or keeping their valuables in a safe box at home or in a bank), people should also learn to lock their online home/account effectively or safeguard their digital assets. If people use a good lock for their home or business or place cameras all over the place, why shouldn't they learn to do the same for their digital assets and to monitor their online activities?

To effectively improve awareness and change behaviour, the population needs to be educated very early, continuously, and consistently. After all, it is unlikely that issues in cybersecurity will be resolved soon. Thus, it is in the interest of the greater community to include measures of cybersecurity in the educational system from middle school and up. Because children are using computers at a very early age these days, it is that much more important that they be aware of their cybersecurity as early as possible.

Including cybersecurity in the formal education system would also be the more cost-saving approach for society considering all the costs associated with training employees and individuals following instances of identity theft, ransomware, and so on.

5.7.3 Cybersecurity 101: A Solution

To improve cybersecurity awareness and prepare students for professional life, it would be extremely effective to include a basic course on cybersecurity in all university education curricula. After all, most universities require students to take many introductory-level courses such as English or Chemistry 101, so why wouldn't we offer cybersecurity awareness in all disciplines of an education curriculum? This approach would be the most effective way to fundamentally help students be prepared to protect themselves, and the organizations that they will work for, in the future. Instructors could then prepare and update their content based on the evolving and constantly changing protection methods to keep students updated about cyberspace and how to practise safe behaviour. This approach would also help educational institutions to protect universities from cyber-attacks. The content of this type of education could include, but would not have to be limited to, the following areas:

1. Trust
2. Authentication
3. Privacy
4. Ransomware
5. Identity theft
6. Phishing
7. Application access
8. Social media
9. Social engineering
10. Surveillance
11. Mobile device protection

The content could include the awareness and practice of each topic. As a result, people could learn about each area and also the ways they could implement their knowledge.

5.7.4 Cybersecurity Games: Another Solution

With the expansion of online and video games and their massive popularity among the younger population, creating scenario-based gaming is another effective way to improve overall awareness among the population. After all, many people (especially younger people) spend a great deal of time playing video games. There are several games available for IT professionals and cybersecurity that can create more dynamic learning tools. There are also games targeting the younger population, the majority of which are available for free [93].

However, large audience computer games dealing with cybersecurity issues running on main gaming platforms are not yet available on the market. After all, if there are hundreds of wargames available on all gaming platforms that show how to pilot an airplane, why not create cybersecurity games? Studies have shown that games can not only be effective training tools but also be effective for encouraging behavioural change [94].

The author has created a few card games, board games, and even online games that are used in his classes and training programmes, and he has been pleasantly surprised by their effectiveness and the degree to which students are not only having fun but also engaging with the topic. This approach could also expand to cybersecurity awareness among employees. Many people use games like Solitaire or other sorts of card games on their computers, so why not let employees play a fun game that would let them learn cyber awareness and safe behaviour? This would surely be better than just asking them to listen to static online trainings. Couldn't this be a better approach and more cost-effective? Couldn't this be an area for private enterprises to invest in or for the National Science Foundation to promote research and development?

5.7.5 Cybersecurity Culture

The numerous cybersecurity threats will not be solved in the near future simply by technological solutions. The speed at which technologies evolve in finding solutions is not as fast as the complexity of cyber-attacks. The number of Internet-enabled devices in homes, cars, and cities makes keeping up with security and protection more challenging. The events in the last U.S. election and interferences in mass communication by what is now labelled as "fake news" make trust between what is real and fake a challenging issue for citizens. The example of Cambridge Analytica [4], a political data firm that gained access to the private information of more than 50 million Facebook users and then offered tools that could identify the personalities of American voters and influence their behaviour, is a good illustration of how much citizen privacy is at stake. It also shows the importance of the judgement of people in what they choose to share.

5.8 CONCLUSION

In conclusion, in order to elevate awareness, cybersecurity needs to become a "security culture" both at work and at an individual level. Cybersecurity is not a one-time solution, and it should not be reduced to just strong passwords or a few protective approaches. It needs to become an individual responsibility. Knowing about security is vital. By addressing security concerns and risks, students and all individuals can better protect themselves against risks at work and at home.