Back to Basics: Towards Building Societal Resilience Against a Cyber Pandemic

Eliana STAVROU
Computing Department, Applied Cybersecurity Research Laboratory
University of Central Lancashire Cyprus
Larnaca, Cyprus

ABSTRACT[1]

Cybersecurity experts have long been discussing the potential of a cyber pandemic leading to a massive disruption of ICT operations with a devastating societal impact. Even though society has not faced yet the full potential of a cyber pandemic, the recent COVID-19 pandemic demonstrated how a cyber pandemic can look like at its initial stages. Unfortunately, citizens proofed to be unprepared to handle the COVID-19 threat landscape and how fast cyber-attacks escalated at a global scale targeting individuals, corporations, and governments, all at once. This clearly demonstrates that society, at a global scale, is not adequately prepared to defend against a cyber pandemic, despite all the efforts of the cybersecurity community. Cybersecurity awareness and training efforts have been delivered as part of a national or corporate cybersecurity strategy, aiming to promote a cyber hygiene and enhance protection against cyber-attacks on an individual, a corporate, or a national level. The current level of citizens' cybersecurity awareness is not yet the desired and actions need to be taken to upscale it. Thus, it is time to take a step back to identify what is missing from current awareness efforts and reconsider how people learn. This knowledge can drive the redesign of the national and corporate cybersecurity awareness activities, effectively building citizens' cyber skills and knowledge, and leading to the development of robust cyber resilient societies, capable of defending and withstanding a future cyber pandemic.

Keywords: Cybersecurity Culture, Cyber Situational Awareness, Cybersecurity Education, Cyber pandemic, Citizens cybersecurity skills, Cybersecurity Hygiene and Cyber Resilience.

1. INTRODUCTION

The cybersecurity community has warned of a potential cyber pandemic [1] that can cause a massive disruption of ICT operations worldwide, having a global devastating impact across society. In the case that such a cyber pandemic occurs, society as a whole needs to be well prepared to be able to minimize any potential impact. This means that citizens should be capable to identify a potential cyber threat and demonstrate a cyber hygiene behavior to minimize the risk of a data breach. Establishing such a common cyber front across society will assist in building societal resilience [2][3] against a dynamic cyber threat landscape.

Even though society has not faced yet the full potential of a cyber pandemic, the recent COVID-19 pandemic demonstrated how a cyber pandemic can look like at its initial stages. Given the worldwide crisis that was triggered due to the COVID-19, malicious people found ground [4][5] to exploit people across society and across ages (from young people to elders). Phishing was among the top threats that society had to face during this period. Phishing emails have spiked by over 600% during COVID-19 [6], and the widespread themes [7] of phishing increased exponentially the chances for someone falling for the lure. Medical supply sales, fact sheet information about COVID-19, shipping notifications, work from home tooling, etc., are some of the lures that have been utilized in phishing campaigns. As the pandemic progresses, the threat of phishing is expected to persist and new scams will arise, e.g., related to the cure, etc.

Unfortunately, citizens proofed to be unprepared to handle the COVID-19 cyber threat landscape [4] and how fast cyber-attacks escalated at a global level, targeting individuals, corporations, and governments, all at once. This clearly demonstrates that the global society is not adequately prepared to defend against a cyber pandemic. Even though the cyber community is promoting a range of cyber awareness activities, these have not been so effective to develop a cyber hygiene culture [8][9] among citizens. Developing such a culture means that the necessary skills and knowledge will be cultivated to assist citizens in understanding the risks that may arise from their actions in cyberspace, as well as identifying and addressing effectively cyber threats by applying best practices. This approach can assist society to build cyber resilience [2][3] against a cyber pandemic and minimize any potential impact on an individual, a corporate, or a national level.

Currently, the level of citizens' cybersecurity awareness is not yet the desired, thus, actions need to be taken to upscale it. Given the knowledge we gained related to COVID-19, how fast it was escalated and how it affected every aspect of society, and in anticipation of a cyber pandemic, it is essential to realize that actions need to be taken to reinforce existing cyber awareness efforts. It is time to take a step back, investigate what gaps exist in current efforts and take corrective measures. Key aspect of the investigations should focus on the actual learning process. We need to reconsider how people learn to identify what elements might be missing from current efforts and redesign our cybersecurity awareness strategy and relevant activities. The aim will be to build an effective cybersecurity culture among citizens' communities, contributing to a global cyber resilient society, capable of defending and withstanding a future cyber pandemic.

[1] I would like to express my sincere gratitude to Professor Irene Polycarpou for her comprehensive peer-editing of this document

2. CYBERSECURITY AWARENESS EFFORTS

The cybersecurity community has been delivering a range of cybersecurity activities and promoting awareness material across society. The main objective of all these efforts has been to educate people on cyber threats and on following good cyber hygiene practices, so that society can defend against the cyber threat landscape that has been proved to be very versatile given the right circumstances. A recent example is the COVID-19 pandemic that empowered the cyber threat landscape [4] to expand its attack surface across society.

Cybersecurity awareness is delivered through different means. On a national level, many countries have formulated their own national cybersecurity strategy [10], including the delivery of cybersecurity awareness campaigns, targeting citizens of all ages. Organizations also started constructing more actively their own internal awareness campaigns to educate their employees and create a corporate cybersecurity culture [11]. Typical means utilized in a cybersecurity awareness campaign include delivery of presentations, promotion of infographics, posters, guides, and tips on how to stay secure in cyberspace, e.g., [12]. An overall observation is that these resources are often passively delivered to the target audience. An example of a more active approach is the delivery of workshops where the audience has a more engaging role and can practice on cyber concepts to advance its knowledge and skills. Also, phishing simulation [11][13] is a mean that is getting a lot of attention lately, due to the COVID-19 cyber threat landscape. Many organizations have realized that phishing is a threat that needs to be actively addressed, thus they are performing phishing simulations to evaluate their current level of security and to educate employees to recognize phishing attempts. More engaging activities are also delivered by national authorities, academia, and private sector, focusing on younger people. Such activities include participation in cyber competitions, boot camps, and cyber computer games, e.g., [14][15][16].

Cyber awareness efforts vary in terms of the means utilized and the target audience at various countries [17]. It should be evident to all parties involved that efforts should be continuous. At countries where the level of cyber awareness is low, it should be upscaled to support the creation of a global cybersecurity culture that will keep up with the current cyber threat landscape.

3. COVID-19 CYBER THREAT LANDSCAPE

The biggest concern so far related to existing cyber awareness efforts is whether these efforts have been effective to cultivate a cyber hygiene culture. Unfortunately, the indication is not positive, and this can be demonstrated through the recent cyber threat landscape [4] that was the result of the COVID-19 pandemic. Studies [5][7] demonstrate that attackers were focusing on societal vulnerabilities and on people's need to find information about the pandemic. Numbers have been increased tremendously in a very short period given that teleworking has become the norm, supporting most aspects of personal and business activities. In February 2020, a spike on pandemic-related scams was observed, going over 600% [6]. In April 2020, Google announced that it blocked 18 million daily malware and phishing emails [18]. As per [19], approximately 50% of employees have reported that they fell for a phishing scam. Email phishing attacks were the most common source of data breaches during the pandemic, targeting people working from home and people seeking information about the pandemic. The cost from security incidents has been overwhelming. In the UK only, the cost reached 11 million pounds as of July 8th, 2020 [20]. Similar trends have been observed so far and they are not expected to decrease anytime soon, while people keep using the same (often bad) cyber practices. Unfortunately, statistics indicate that the problem persists, and that people are still vulnerable, despite the awareness efforts of the cybersecurity community. Therefore, the focus of the cybersecurity community should be placed on investigating what is missing from current efforts and how an effective cyber hygiene culture [8][9] can be cultivated among citizens.

4. CYBERSECURITY AWARENESS EFFORTS – WHY DO THEY FAIL

A key element to consider while investigating how to build societal resilience against a cyber pandemic is to realize the reasons that current awareness efforts have not been very effective. Investigations should address two audiences: end users of awareness activities and experts involved in designing a cybersecurity awareness strategy.

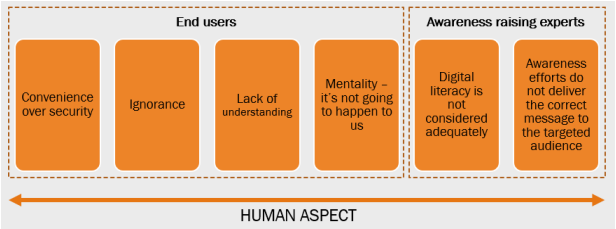

Figure 1: Factors affecting cybersecurity awareness efforts

In terms of end users, there are different factors that have been identified by existing studies, e.g., [21][22]. Users often prefer convenience over security, and they demonstrate an online behavior that in several cases is associated with bad cyber practices. Current awareness efforts failed to motivate people to change their online behavior to a satisfactory level. This is a limiting factor towards building a cybersecurity culture and societal cyber resilience. The studies have also shown that people often do not demonstrate a cyber hygiene behavior simply because they are ignorant, they lack understanding of the relevant concepts or they do not know how to apply a security measure [23]. This is often linked to the communication message delivered by awareness activities. If the message is not relevant to the target audience, if it does not consider the current knowledge and skills and fill in the blanks, then it will not be effective and certainly it will not support people to advance their knowledge and understanding of the cyber threat landscape and actions to be taken. This further hinders attempts to build societal cyber resilience. Another factor that contributes to the failure of developing a cybersecurity culture is that people frequently have a false sense of security as their mentality is that "it is not going to happen to us", so, in essence, they do not have any motivation to change their behavior. Unfortunately, awareness efforts have not been very effective eradicating this notion of false security. This indicates that awareness activities are not conveying an appropriate story to citizens; a story that will clearly demonstrate that everybody is at risk, convince people that

security should be a concern for all and show them how they could deal with an incident.

The other audience that needs to be considered involves those responsible to design and develop an awareness strategy and relevant activities. If someone investigates the approach taken in current awareness activities, he/she will observe that a passive delivery of material is mostly performed [24], where similar awareness content is pushed towards different audiences, e.g., general public, executives, staff, youngers, etc. This flat approach of the awareness activities across all audiences, results into prohibiting the delivery of the correct communication message to the targeted audience as the same message is distributed across all audiences [25][26]. If the communication message is not relevant to the needs of the target audience, then people will not realize the importance of demonstrating a cyber hygiene behavior and they will not be motivated to change their online behavior and habits.

It is imperative to realize that a cybersecurity awareness strategy and activities should reflect the digital literacy of the target audience, its business, and/or personal aspirations, as well as the cyber threat landscape that is relevant to the target audience's business and personal culture [27]. Given that the human aspect is a central point for the success of a cybersecurity awareness strategy, it is essential to revisit the design approach taken so far, identify what is missing, and address it, aiming to build a robust cybersecurity culture and societal cyber resilience.

5. BUILDING BLOCKS FOR AN EFFECTIVE CYBERSECURITY CULTURE

The main goal of a cyber security culture should be to build societal resilience against cyber-attacks. This means that society, at a global scale, will be prepared to handle cybersecurity incidents and address the threat of compromization. To achieve this goal, we need to educate citizens [28] about cyber threats and cyber hygiene practices and develop their skills to be able to apply best practices, addressing effectively a potential cyber threat. To demonstrate a continuous cyber resilience though, people need to develop a sustainable cyber hygiene behavior. To achieve a culture change and promote a sustainable behavior, we need to consider two key objectives (Figure 2): promote cyber situational awareness and cultivate critical thinking in a cyber context.

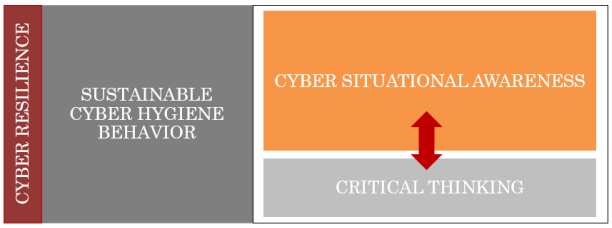

Figure 2: Building blocks for a cybersecurity culture

Cyber situational awareness

A core element that needs to be considered when building a cybersecurity culture is cyber situational awareness [24][29], which refers to the knowledge that people have about a given cyber situation. The specification provided in [30] regarding situational awareness identifies all qualities that should be projected and developed through a cybersecurity culture. According to [30], "situational awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future". In cyber space, being aware of a cyber situation means for people to realize the elements that exist in their environment, understand their importance, identify the relevant cyber threats that may put them at risk, and predict the impact that can occur if an incident is elaborated. Developing abilities such as perception, comprehension, and projection, should constitute a key objective of any cybersecurity culture, as these characteristics can assist in sustaining a cyber hygiene behavior among citizens.

Critical thinking in a cyber context

Cultivating critical thinking skills in a cyber context is essential, as this can support the objectives of situational awareness, especially with regards to comprehending the dynamic nature of the cyber threat landscape and applying mitigation actions. More specifically, critical thinking [31][32][33] is a necessity, if we want citizens to be able to recognize cyber risks, predict and identify how cyber threats can transform given different circumstances (latest example COVID-19), and make wise decisions as to the actions that need to be applied. By developing citizens' critical thinking in a cyber context, societal cyber resilience can be developed and sustained.

Given the key role that situational awareness can play in the efforts of the cybersecurity community to build societal cyber resilience, the focus should shift from developing a cybersecurity culture to promoting a cyber situational awareness culture.

6. TOWARDS A CYBER SITUATIONAL AWARENESS CULTURE

As discussed previously, awareness efforts have not been as effective as expected. It is thus imperative to reinforce these efforts to achieve an effective and long-lasting cyber situational awareness culture. To do so, we first need to identify what is missing from the awareness approach considered so far and then redesign how an awareness strategy can support the development of the building blocks identified in section 5. Given that the main goal is to develop the appropriate knowledge and skills for citizens to be able to handle a cybersecurity incident, investigations should focus on how people learn, optimizing the learning process in a cyber situational awareness context. The investigations can provide new insights and result to new directions for the design and development of a cyber situational awareness culture across society.

How people learn – Bloom's taxonomy

To revisit how people learn and to achieve a culture change, a learning framework should be utilized to guide the change. One of the most widely used learning frameworks which models the human cognitive process is the Bloom's taxonomy. Bloom's taxonomy is a classification of the different learning objectives, knowledge, and skills that educators should consider when specifying educational objectives across different disciplines. Moreover, the taxonomy indicates what students need to do to demonstrate their learning or competence. The original

taxonomy was published in 1956 [34]. Figure 3 presents the revised taxonomy that was published in 2001 [35], which includes 6 taxonomy levels of learning objectives. As it can be observed, Bloom's taxonomy follows a bottom-up approach, where higher levels of learning are depended on previous knowledge and skills attained at previous levels. This approach fits very well in the overall concept of building a cyber situational awareness culture where people should be aware of fundamental cyber topics that will guide their behavior in cyberspace, considering the current cyber threat landscape. It is expected that once people have a good understanding of the cyber concepts, then they can be educated on how to apply cyber hygiene techniques, from simple to advance actions, depending on their background, business obligations, personal aspirations, and culture.

To be able to optimize the learning process in a cyber context, it is essential to first have a good understanding of how Bloom's taxonomy fits into the development of a cyber situational awareness culture. As depicted in Figure 3, each learning layer of Bloom's taxonomy is associated with specific learning objectives. The key learning objectives per layer (bottom to top) are listed below:

1) Remember – recall facts and basic concepts
2) Understand – explain ideas or concepts
3) Apply – use information in new situations
4) Analyze – draw connections among ideas
5) Evaluate – justify a stand or decision
6) Create – produce new or original work

As discussed in section 5, the building blocks for an effective cyber culture are cyber situational awareness and critical thinking skills. Through critical thinking, situational awareness can be established. The reverse also applies, as through situational awareness people can build their thinking process, improve their perception regarding cyber threats, enhance their knowledge, critically evaluate new cyber incidents they may face, and select the appropriate course of actions. Therefore, each building block should be perceived as complementary for the development of the other. Developing situational awareness and critical thinking skills should happen progressively across all layers of Bloom's learning framework. Bottom layers should be considered to build lower order thinking skills and basic awareness levels, while as we move upward in the taxonomy, higher order cognitive skills and advanced awareness can be developed.

For example, we can consider that bottom layers (e.g., Remember, Understand) can assist people to acknowledge and realize the problem and understand the fundamentals in terms of a cyber hygiene. Building the appropriate knowledge and perception is the first stage of a cyber situational awareness culture. The second stage has to do with building an elaborated comprehension of cyber hygiene components and actions. This can be achieved initially through the third layer (Apply) of Bloom's taxonomy. This is the layer where people should have the opportunity to apply their knowledge and evaluate whether they have understood the cyber concepts and whether they know how to put them in practice. This is the stage where people can start becoming reflective and more critical about their skills and abilities, potentially identifying areas of knowledge that need to be enhanced. Critical thinking can then be reinforced and developed further in the following three layers (Analyze – Evaluate – Create), where people should be exposed to real case situations, analyze how a cybersecurity incident has been elaborated, critically evaluate actions taken comparable to cyber hygiene fundamentals, and then reinforce the knowledge that has been obtained at the bottom layers of the taxonomy. The main goal is to be able to critically apply this knowledge in different situations and to effectively manage a cybersecurity incident.

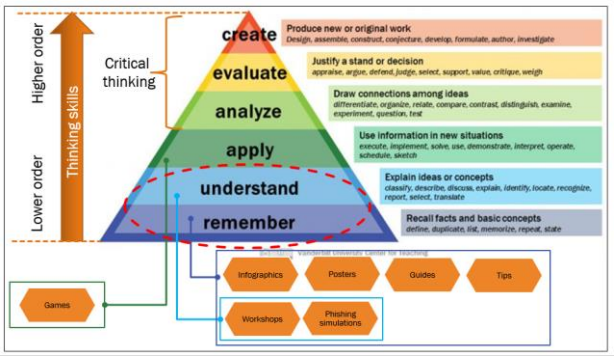

Figure 3: Cybersecurity awareness efforts focus (image adopted from [36])

Awareness efforts – current focus

To be able to identify the gap that currently exists in awareness efforts, it is essential to examine where the focus of these efforts is. In section 2, the typical means that are utilized in an awareness strategy have been discussed. Means such as infographics, posters, guides, and tips, achieve the learning objectives mostly applicable in the bottom two layers of Bloom's taxonomy (Remember and Understand) and help people to learn about the basic concepts and recall information. More interactive means like workshops, phishing simulations, and computer games support learning objectives of higher layers of Bloom's taxonomy (e.g., Apply, Analyze) and can assist people to comprehend the concepts, develop their practical skills, and evaluate actions to be taken towards a cyber hygiene. These interactive means are not widespread utilized across society, but rather target specific communities, such as younger people and employees. Despite the utilization of these interactive means, an adequate level of cyber situational awareness has not been achieved among these target audiences. This is evident from the high figure numbers that are listed in terms of data breaches across the industry [19][37]. This observation should trigger more investigations into whether these target audiences master the fundamentals that should have been obtained through the previous layers of the Bloom's taxonomy. If they do not have an appropriate level of awareness and a fundamental understanding of cyber concepts, then they will not be able to engage with activities that target to build upon the fundamental knowledge that is assumed to have been obtained.

It is evident that most of the efforts are covering learning objectives obtained from the bottom learning layers of Bloom's taxonomy, yet our expectation is that people should demonstrate critical thinking when it comes to a cyber incident and being able to evaluate the incident and apply a solution. This is currently a limiting factor, as existing cybersecurity efforts are not providing adequate stimulations to people to be able to move from the lower taxonomy learning layers to the higher layers and meet the relevant learning objectives. The target should be to infuse to people, beyond the basics, the knowledge to apply technologies, develop their critical

thinking, and be able to manage a cybersecurity incident.

Awareness efforts – what is missing

It is imperative to identify what learning layers need to be reinforced to cultivate higher order cognitive skills and cyber situational awareness levels. Currently, there are a lot of activities covering the learning objectives at the bottom two layers of Bloom's taxonomy, educating people on basic concepts. One question that needs to be answered is whether people have sufficient understanding of the fundamentals and consequently, the next step will be to evaluate [38][39][40] whether they can translate theory to practical concepts (Figure 4). It is essential to evaluate people's overall understanding and skills, identify the current awareness level that has been established, and then adjust the delivered awareness activities and content according to the evaluation results. This approach will assist in bridging the gap, in terms of knowledge and skills that might not be present in certain user communities, and advance them to an appropriate awareness level towards developing a sustainable cyber hygiene behavior and societal resilience. Moreover, this approach can provide insights as to whether citizens realize what is happening in cyberspace and what are the relevant risks. Quantifying the level of people's understanding can assist in designing activities that will deliver the appropriate communication message and content, motivating people changing their habits and adopting best practices in cyberspace. Such an evaluation component is often missing from current cyber awareness strategies.

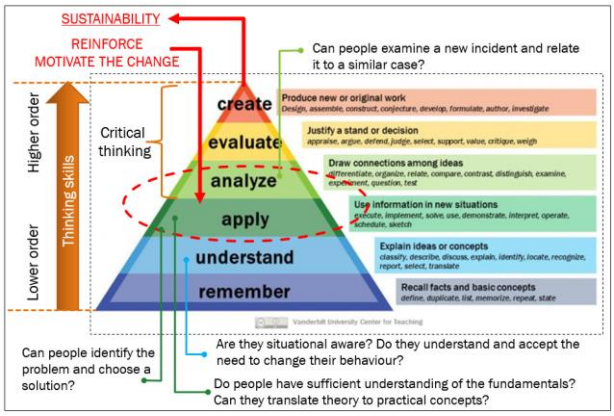

Figure 4: What is missing from cybersecurity awareness efforts (image adopted from [36])

Issues also appear at the third learning layer of Bloom's taxonomy. There is not enough evidence that given a cyber incident people can identify the problem and apply a solution. This is a great issue, as societal resilience cannot be achieved, if people cannot take actions to address a cyber incident. A mutual understanding by all parties involved in the design and development of awareness activities is required, that if we do not teach people with a what-if-how philosophy, we should not expect them to know how they should proceed to effectively address a cyber threat. Unfortunately, this lack of knowledge is evident from the recent cyber statistics related to COVID-19, that demonstrated that incidents have exponentially increased, leading to data breaches on an individual and corporate level.

The problem propagates at the higher layer of Bloom's taxonomy where it is expected that people will be able to analyze and evaluate a cyber incident. Apart from the fact that people's understanding of fundamentals might be absent or limited, awareness activities are not placing enough focus on the dynamic nature of the cyber threat landscape. Therefore, most awareness efforts are not aligned with how the cyber threat landscape transforms. This means that knowledge and skills are not upscaled to the level appropriate for people to address a new incident and take actions accordingly. Awareness activities should improve people's knowledge regarding the dynamics of the threat landscape and make evident how the threat landscape relates to their existing knowledge, so they can critically apply a solution.

The issues identified highlight the fact that awareness efforts need to be improved to motivate and sustain a positive change in online behaviors and increase people's awareness level. To achieve this, a solution is to reinforce (Figure 4) the third (Apply) and fourth (Analyze) learning layer of Bloom's taxonomy.

Awareness efforts – back to basics & design directions

As discussed, the current level of citizens' cybersecurity awareness is not yet the desired. To develop a good understanding of cyber fundamentals, build critical thinking skills, and be able to address a cyber incident, requires a solid foundation that begins from the lower learning layers of Bloom's taxonomy. Thus, the need to go back to basics. The target should be to ensure that once people understand the fundamentals, they have: 1) the skills to choose and apply solutions, b) a solid understanding of the cyber threat landscape and the impact that might arise, if they do not apply best practices.

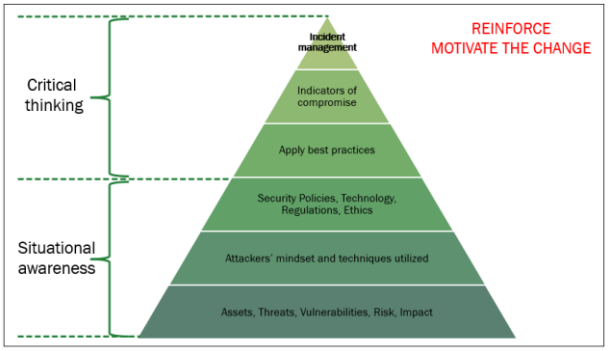

Figure 5: Back to basics - design directions

If we succeed in reinforcing the middle learning layers and motivate the change in behavior, then we can develop citizens with critical thinking skills, ones that will be able to understand the semantics of a cybersecurity incident and take decisions accordingly. This can lead to a sustainable cyber situational awareness culture.

The key point here that needs to be considered is how we can achieve cyber situational awareness as a foundation for critical thinking (Figure 5). We can achieve this, if we make sure that citizens can identify the assets that need to be protected, identify the relevant threats, vulnerabilities, and impact. It is imperative for people to understand the attacker's mindset and techniques utilized, so they can realize the need for taking specific cyber hygiene actions. This entails obtaining a good knowledge background on measures that can be applied, being aware of regulations, and understand their responsibility to follow cyber hygiene practices. To truly defend against an evolving cyber threat landscape, we need to have a unified

front across society that is cyber situational aware, has embraced the responsibility of building and maintaining secure societies, and has now the fundamental background to build critical thinking skills. This means that given a situation, citizens should be able to apply critical thinking, select the appropriate best cyber hygiene practices, identify indicators of a potential compromization, and take further actions to manage and resolve an incident.

The focus of a cyber situational awareness culture should be cultivating citizens' situational awareness, promoting the understanding of people in cyber space, and developing their practical skills. Given the gap that has been identified in current efforts, the focus from this point forward should be to reinforce the comprehension of people across urgent topics in cybersecurity, including enhancing/developing relevant practical skills. The strategy to be considered should follow a bottom-up approach, similar to Bloom's taxonomy. At the bottom layer, the key elements to consider include the selection of the topics to cover in awareness activities and the means to deliver them. To do so, a good understanding across different aspects is needed. For example, consider how people learn, what the current threats that people should be aware of are, what the mindset of cyber criminals is, how people behave in cyberspace and what factors may affect their decision-making, how do we motivate the change, how can national policies support the change, etc. To cover all these aspects, an interdisciplinary team needs to be considered working at this layer to assist in creating a robust cyber situational awareness culture.

Moreover, to motivate the change and promote a cyber hygiene behavior, it is essential to be aware of the current understanding that people have related to cybersecurity aspects and their ability to apply cyber hygiene practices. Such an understanding can assist the experts to prioritize the topics covered in awareness and training activities and maximize the situation awareness that can be achieved. Contextualizing situational awareness to the needs of the target audience and covering topics that are relevant to the audience's business and/or personal aspirations, alongside covering the current threat landscape, can assist in developing a culture of cyber hygiene practices.

7. CONCLUSIONS

It is often stated that humans are the weakest link in cybersecurity. This is a notion that needs to change, and we need to start viewing humans as our strongest asset. Given the dynamics of the cyber threat landscape, which was reinforced during the COVID-19 pandemic, it is imperative to build societal resilience against a potential cyber pandemic. This can be accomplished by infusing a culture of cyber hygiene across society and developing citizens that can demonstrate critical thinking when coming across a cyber incident, applying the appropriate cyber hygiene best practices, and effectively addressing the incident. If this approach is applied consistently across society, then the society has better chances to withstand a potential cyber pandemic. It should be evident to all that to be successful, a sustainable cyber behavior should be cultivated to promote societal resilience. Current cybersecurity awareness activities have not been very effective to develop a sustainable cyber culture. It is time to return to basics, revisit how people learn, and reinforce the approach taken when designing awareness activities. To achieve and sustain a cyber hygiene culture and motivate people to change their online behavior and practices, cyber situational awareness concepts should be taken into consideration. A learning framework can assist in identifying the learning layers that need to be reinforced, integrating cyber situational awareness aspects where needed, and establishing a cyber situational awareness culture across society.

8. REFERENCES

[1] J. Voas and P. Laplante, Cyberpandemics, in Computer, vol. 53, no. 6, pp. 13-15, June 2020, doi: 10.1109/MC.2020.2984253

[2] G. Baldini et al., Cybersecurity - Our digital anchor, EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19957-1 (online), 978-92-76-19958-8 (print), doi:10.2760/352218 (online),10.2760/967437 (print), JRC121051

[3] A. McCormac, D. Calic, M. Butavicius, K. Parsons, M. Pattinson and M. Lillie, Understanding the Relationships between Resilience, Work Stress and Information Security Awareness, Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017), Adelaide, Australia, November 28-30, 2017

[4] ENISA, ENISA Threat Landscape 2020 - The year in Review, October 2020, Accessed on: December 10, 2020. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-the-year-in-review

[5] European Commission, Joint communication to the European parliament, the European council, the council, the European economic and social committee and the committee of the regions. Tackling COVID-19 disinformation -Getting the facts right, June 2020. Accessed on: December 10, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0008&from=EN

[6] P. Muncaster, COVID19 Drives Phishing Emails Up 667% in Under a Month, March 26, 2020, Accessed on: December 10, 2020. [Online]. Available: https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/

[7] COVID-19 Cyber Threat Coalition (CTC), 2020-04-20 Weekly Threat Advisory, April 2020, Accessed on: December 10, 2020. [Online]. Available: https://www.cyberthreatcoalition.org/advisories/2020-04-20-weekly-threat-advisory

[8] K. Maennel, S. Mäses and O. Maennel, Cyber Hygiene: The Big Picture, 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings. 10.1007/978-3-030-03638-6_18

[9] A. Vishwanath, L. Seng Neo, P. Goh, S. Lee, M. Khader, G. Ong and J. Chin, Cyber hygiene: The concept, its measure, and its initial tests, Decision Support Systems, vol. 128, 2020, 113160, ISSN 0167-9236

[10] ENISA, National Cyber Security Strategies - Interactive Map, Accessed on: December 10, 2020. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

[11] M. Alshaikh, Developing Cybersecurity Culture to Influence Employees Behavior: A Practice Perspective, Computers & Security, 2020, doi: 10.1016/j.cose.2020.102003
[12] ENISA, European Cybersecurity Month, Deployment Report, January 19, 2020, Accessed on: December 10, 2020. [Online]. Available: https://www.enisa.europa.eu/publications/ecsm-deployment-report-2019
[13] H. Aldawood and G. Skinner, Educating and raising awareness on cyber security social engineering: A literature review, in IEEE International Conference on Teaching, Assessment, and Learning for Engineering, Wollongong, NSW, Australia, 2018
[14] European Cyber Security Challenge (ECSC). Accessed on: December 10, 2020. [Online]. Available: https://europeancybersecuritychallenge.eu/
[15] UK National Cyber Security Centre, CyberFirst. Accessed on: December 10, 2020. [Online]. Available: https://www.ncsc.gov.uk/cyberfirst/overview
[16] Google, Interland, Be Internet Awesome. Accessed on: December 10, 2020. [Online]. Available: https://beinternetawesome.withgoogle.com/en_us
[17] European Economic and Social Committee, Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks – Study, March 2018, Accessed on: December 10, 2020. [Online]. Available: https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf
[18] N. Kumaran and S. Lugani, Protecting businesses against cyber threats during COVID-19 and beyond, April 16, 2020, Accessed on: December 14, 2020. [Online]. Available: https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond
[19] Panda Security, 43 COVID-19 Cybersecurity Statistics, August 26, 2020, Accessed on: December 14, 2020. [Online]. Available: https://www.pandasecurity.com/en/mediacenter/news/covid-cybersecurity-statistics/
[20] Action Fraud, National Fraud & Cyber Crime Reporting Centre, COVID-19 related scams - news and resources, March 26, 2020, Accessed on: December 14, 2020. [Online]. Available: https://www.actionfraud.police.uk/covid19
[21] M. Bada, A. Sasse and J.R.C Nurse, Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In proceedings of the International Conference on Cyber Security for Sustainable Society (CSSS, 2015) Coventry, UK, 2015, pp. 118-131
[22] S. Goel, K. Williams and E. Dincelli, Got Phished? Internet Security and Human Vulnerability, Journal of the Association for Information Systems, vol. 18, pp. 22-44, doi: 10.17705/1jais.00447
[23] ENISA, Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, April 16, 2019, Accessed on: December 14, 2020. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity
[24] CyberSec4Europe, Deliverable D9.6: SME Cybersecurity Awareness Program, February 1, 2019, Accessed on: December 14, 2020. [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2020/04/D9.6-SME-cybersecurity-awareness-program-1-V-1.0-Submitted-1.pdf
[25] O. Beris, A. Beautement and M.A. Sasse, Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the Risk Perceptions and Emotions That Drive Security Behaviors. Proceedings of the 2015 New Security Paradigms Workshop, 2015, pp. 73-84
[26] Information Security Forum (ISF), From Promoting Awareness to Embedding Behaviours, Secure by choice not by chance, February 2014
[27] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin and H. N. Basim, Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems, February 2020, doi: 10.1080/08874417.2020.1712269
[28] A. R. Neigel, V. L. Claypoole, G. E. Waldfogle, S. Acharya, G. M. Hancock, Holistic cyber hygiene education: Accounting for the human factors, Computers & Security, vol 92, 2020, 101731, ISSN 0167-4048
[29] J. Brynielsson, U. Franke and S. Varga, Cyber Situational Awareness Testing, Combatting Cybercrime and Cyberterrorism - Challenges, Trends and Priorities Springer International Publishing, 2016, pp. 209-233
[30] MR. Endsley MR, Toward a theory of situation awareness in dynamic systems, Human Factors, 1995, 37(1), pp. 32–64
[31] H. Santos, T. Pereira, I. Mendes: Challenges and reflections in designing cyber security curriculum in 2017 IEEE World Engineering Education Conference (EDUNINE), March 2017, pp. 47-51
[32] D. Mouheb, S. Abbas, M. Merabti, Cybersecurity Curriculum Design: A Survey, in: Z. Pan, A. Cheok, W. Müller, M. Zhang, A. El Rhalibi, K. Kifayat (eds) Transactions on Edutainment XV. Lecture Notes in Computer Science, vol. 11345, 2019. Springer, Berlin, Heidelberg, doi: 10.1007/978-3-662-59351-6_9
[33] B. Lorenz and K. Kikkas, Pedagogical Challenges and Ethical Considerations in Developing Critical Thinking in Cybersecurity, 2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT), Tartu, Estonia, 2020, pp. 262-263, doi: 10.1109/ICALT49669.2020.00085
[34] B. S. Bloom, M. D. Engelhart, E.J. Furst, W.H. Hill and D.R. Krathwohl, Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain. New York: David McKay Company, 1956
[35] L.W. Anderson, D.R. Krathwohl, P.W. Airasian, K.A Cruikshank, R.E. Mayer, P.R Pintrich, J. Raths and M.C. Wittrock, A taxonomy for learning, teaching, and assessing: A revision of Bloom's Taxonomy of Educational Objectives, 2001, New York: Longman
[36] Vanderbilt University Center for Teaching, Accessed on: December 14, 2020. [Online]. Available: https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/
[37] ENISA, ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis, October 20, 2020, Accessed on: December 14, 2020. [Online]. Available: https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis
[38] J. Esparza, N. Caporusso and A. Walters, Addressing Human Factors in the Design of Cyber Hygiene Self-assessment Tools. In: I. Corradini, E. Nardelli, T. Ahram (eds) Advances in Human Factors in Cybersecurity. AHFE 2020. Advances in Intelligent Systems and Computing, vol.

1219, 2020, Springer, doi: 10.1007/978-3-030-52581-1_12
[39] E. Albrechtsen and J. Hovden, Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study, Computers & Security, vol. 29, issue 4, 2010, pp. 432-445, ISSN 0167-4048, doi: 10.1016/j.cose.2009.12.005
[40] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac and T. Zwaans, The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies, Computers & Security, vol. 66, 2017, pp. 40-51, ISSN 0167-4048, doi: 10.1016/j.cose.2017.01.004