Guidelines to Develop Consumers Cyber Resilience Capabilities in the IoE Ecosystem

Eliana Stavrou(✉)

Faculty of Pure and Applied Sciences, Open University of Cyprus, Nicosia, Cyprus
eliana.stavrou@ouc.ac.cy

Abstract. The IoE ecosystem presents ongoing cybersecurity challenges that need to be addressed by all actors to effectively defend against the dynamics of the relevant cyber threat landscape. The consumer IoT market constitutes a key element of the IoE ecosystem that must be protected from cyber criminals. To effectively defend against cybercriminals, consumers must adopt a more active role and become more resilient to attacks. This means that they need to be able to proactively anticipate attacks, defend and effectively respond to a security incident. To this end, it is essential to promote the development of basic technical skills to a level appropriate for consumers. This is an important aspect that should drive the design of specialized cybersecurity curricula in the context of the IoE ecosystem. This research work provides guidelines to curricula designers and trainers as to the thematic areas they should consider in the design and delivery of specialized cybersecurity curricula to build consumers' cyber resilience competencies in the context of the IoE ecosystem. For each thematic area, the key topics to consider in the design of the curricula are specified, highlighting specific skills and knowledge that should be developed. The design of such curricula can contribute in upskilling consumers and improving the cyber resilience level across society.

Keywords: Cyber resilience · Cyber hygiene · Consumer IoT · Cybersecurity education · Societal cyber resilience

1 Introduction

The digital transformation that was observed across the globe as an outcome of the impact caused by the COVID-19 pandemic, has forced citizens to utilize a range of smart products and use technologies without realizing the potential threat they bring in their homes [1]. These smart connected products are often referred to as the Internet of Things (IoT), which is part of a greater concept, that of the Internet of Everything (IoE). IoE is a complete ecosystem that consists of four key elements: things, people, data, and processes, where the Internet forms the foundation of these elements. According to [2], the number of IoT devices worldwide is forecast to almost triple from 8.74 billion in 2020 to more than 25.4 billion IoT devices in 2030. By 2030, it is anticipated that around 60% of all IoT connected devices will concern the consumer sector.

T. Pereira et al. (Eds.): IoECon 2022, LNICST 458, pp. 18–28, 2023.
https://doi.org/10.1007/978-3-031-25222-8_2

IoT products have become part of everyday life as consumers have realized the great benefits of using these products, such as convenience and personalization. The utilization of IoT devices can assist in saving valuable time in an era of fast-paced world, which can be dedicated to other essential aspects of consumers' life such as family and wellbeing.

Although IoT devices have many benefits, it is well known that they constitute crown jewels for cybercriminals who continue to exploit a range of well-known vulnerabilities, such as insecure passwords, insecure ecosystem interfaces, outdated components and unencrypted communications [3]. According to Netscout Systems [4], the average IoT device gets attacked just five minutes after it goes online. Unfortunately, this trend will get worst as more devices get connected and extend the overall IoE attack surface. As indicated in the survey performed by the Consumers International and the Internet Society [5], approximately 50% of the survey's participants reported distrusting their connected devices to protect their privacy and handle their information in a respectful manner. Even though the low trust levels to connected IoT devices, consumers still use them due to the benefits they offer.

The IoE ecosystem presents ongoing cybersecurity challenges that need to be addressed to defend against the dynamics of the cyber threat landscape. To increase the chances to effectively defend against cybercriminals and become more cyber resilient, consumers must adopt a more active role and support the efforts to protect the IoE ecosystem. The plug-and-play nature of the IoT devices, alongside the utilization of a range of IoT-powered applications makes the whole experience transparent to consumers who often do not realize the technologies they use and the relevant risk, or it's magnitude, for their privacy and safety and how this can extend and impact the entire society. It is imperative to upskill consumers on fundamental cybersecurity aspects and make them aware of the situation in cyber space. Currently, cybersecurity awareness raising efforts have not achieved the appropriate level of competencies among consumers [6]. To start building consumers' cyber resilience capabilities, curricula designers should consider building capabilities across the five functional cybersecurity areas (identify, protect, detect, respond, and recover) specified in NIST Cybersecurity Framework [7].

This research work targets to highlight the urgency to educate consumers, beyond awareness raising, and build their cyber resilience competencies so they demonstrate a responsible behavior as actors in the IoE ecosystem. In the context of this work, guidelines to curricula designers and trainers are provided, as to the thematic areas they need to consider when developing and delivering specialized cybersecurity curricula for consumers in the context of the IoE.

Section 2 presents existing work. Section 3 discusses societal cyber resilience competencies in the context of IoE and Sect. 4 presents the thematic areas to consider in the design of specialized curricula to build consumers' cyber resilience skills and knowledge in the context of the IoE ecosystem. Finally, Sect. 5 concludes this research work.

2 Literature Review

For the past decade, the cybersecurity community's efforts converged towards raising awareness across society on fundamental cybersecurity aspects. A key aspect of all these efforts was to build a societal cyber hygiene culture [8, 9] and defend against

the dynamics of the cyber threat landscape. The most recent example of COVID-19 pandemic, demonstrated how fast the cyber threat landscape [10] can be transformed and expand its attack surface across society. The pandemic forced citizens to adapt their lifestyle and habits to cope with lock downs, work from home, socialize and maintain their wellbeing. Inevitable, the rapid digital transformation that occurred across society to address the pandemic's impact, also forced the adoption of more connected devices in consumers' homes. According to [11], the average UK consumer utilizes more than nine connected devices. Another study [12] highlights how COVID-19 impacted consumers, highlighting that consumers are utilizing more connected devices than at the start of the pandemic. The average U.S. household now utilizes 25 connected devices. This means that the attack surface is expanded as consumers connect more products to create smarter homes.

The rising use of IoT consumer devices in recent years, attracted the attention of cybercriminals, especially due to the poor security protection that many of these devices offer [1, 13]. OWASP Top 10 IoT 2018 list [3] is highlighting ten IoT-related vulnerabilities, including insecure passwords, insecure ecosystem interfaces and outdated components. Cybercriminals demonstrated their ability to build massive botnets from compromised IoT devices and launch Distributed Denial of Service (DDoS) attacks or distribute malware [10]. A recent example is Mirai malware [14], that targeted primarily IoT consumer devices, such as IP cameras and routers, and turned them into remotely controlled bots utilized in DDoS attacks against major internet platforms and services.

The necessity of developing a cyber hygiene culture [8, 9] is stronger than ever. This includes being aware of best cybersecurity practices and apply them to stay secure in cyberspace. To this end, the cybersecurity community has been delivering cybersecurity education courses and awareness raising activities across society. These activities have been developed taking into consideration different cybersecurity curricula guidelines and frameworks, such as the CSE2017 [15] and the CyBOK [16]. The focus of these guidelines has been primarily to highlight the knowledge that needs to be developed across different areas in cybersecurity. This approach has been reflected in the design of many cybersecurity education and awareness raising activities delivered across society.

Cybersecurity awareness raising campaigns often include the 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. 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., [14–16].

Even though the cyber awareness raising efforts, these have not been very effective to reach a satisfactory societal cyber resilience level. This is due to different factors as indicated by existing studies, e.g., [17, 18]. Users often prefer convenience over security, and they demonstrate an online behavior that in several cases is associated with bad cyber practices. The studies have also shown that people often do not demonstrate a cyber hygiene behavior simply because they are not aware of the situation, they lack understanding of the relevant concepts, or they do not know how to apply a security measure [19].

To address the dynamics in the cyber threat landscape, consumers need to become more resilient to attacks, which means they need to be able to proactively anticipate attacks, defend and effectively respond to a security incident. The need to build societal cyber resilience competencies has been highlighted in many studies, e.g. [6, 20–23]. When considering consumers, it is obvious that the expectations should not be the same as when dealing with professionals, but nonetheless it is essential to build some basic technical competencies to the level appropriate for consumers. This is an important aspect that should drive the design of specialized cybersecurity curricula in the context of the IoE ecosystem.

3 Societal Cyber Resilience Competencies

According to the National Institute of Standards and Technology (NIST), cyber resiliency is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." Currently, cybersecurity awareness raising efforts focused on developing fundamental knowledge on cybersecurity aspects. This approach may have increased to some level the understanding of consumers of the importance of cybersecurity but has not been that effective in convincing people to change their behavior and adopt a responsible cyber hygiene behavior. This might be because cybersecurity awareness raising efforts have not focused on developing the practical skills of consumers so they can actually apply best cybersecurity practices [6]. Thus, we need to rewire the approach we take when designing and developing cybersecurity awareness raising activities and integrate more practical aspects, such as demonstrations and hands-on activities, to promote the development of critical thinking skills. By adopting a what-if-how philosophy, consumers can start building the necessary skills and knowledge to effectively address a cyber threat. Currently, consumers capabilities are not developed to an adequate level, and this is evident from the recent cyber statistics related to COVID-19, that demonstrated that incidents have exponentially increased, leading to data breaches across the society.

To effectively deal with the dynamics of the cyber threat landscape, efforts have focus on building a cybersecurity capacity. As per ENISA guidelines, many countries have specified their national cybersecurity strategy, including objectives to build a cybersecurity culture and relevant capabilities across society [24], considering children, young adults, seniors, the workforce, etc. In this context, authorities tasked with the supervision and implementation of the national cybersecurity strategies, should consider the necessity to upskill consumers and build relevant knowledge and skills to utilize IoT devices in a secure manner. The effort to build an IoT-focused cybersecurity culture should start from a young age, as young people will constitute the future citizens as soon as they enter adulthood. The necessity to develop a minimum exposure to cybersecurity across a global community, starting from a young age, is also highlighted in [25]. To develop a strong educated global community against IoT cyber threats, it is equally important to design appropriate curricula in higher education and adult education so that young people and adults can be educated on the cyber threats that are relevant to IoT and build skills to address them effectively. Therefore, national authorities should coordinate efforts to bring appropriate stakeholders together to collectively work on building

appropriate capabilities. Depending on the audience, their skills and learning objectives, the appropriate learning material and pedagogies need to be developed. It is envisioned that this work can serve as a basis to guide curricula designers as to the thematic areas they need to first consider and initiate further investigations to support the development of a cybersecurity capacity.

To start building consumers' cyber resilience, curricula designers should consider building consumers' competencies across the NIST Cybersecurity Framework areas [7]: identify, protect, detect, respond, and recover. Thematic areas should be specified within the context of the NIST Cybersecurity Framework to build capabilities across all the functional cybersecurity areas. In the context of the identify area, efforts should focus on building consumers' understanding of the fundamentals related to the IoT ecosystem, identify its components and their value on a personal and societal level. At the same time, consumers need to realize the dynamics of the cyber threat landscape, how specific cyberattacks can be delivered and the impact that might arise on a personal and societal level if an attack is successful. To this end, a key aspect is to highlight the adversaries' mindset and the techniques they utilize so that citizens are aware of the situation, realize the adversarial capabilities and how realistic a compromisation can be. In terms of protection, knowledge and skills should be developed related to choosing and applying best practices and solutions so consumers can proactively address cyber threats and minimize the risk of getting compromised. The next area covers detection aspects. Appropriate capabilities need to be developed so that consumers can identify signs of infection which can trigger them to apply response and recovery actions to limit the impact from a potential cyber incident. Such actions may entail communicating the incident to appropriate authorities, reconfiguring tools, using other mitigation actions to effectively manage the security incident, etc. Table 1 presents the thematic areas that are derived taking into consideration the NIST Cybersecurity Framework and the IoT-related cyber threat landscape [3, 10]. The proposed thematic areas (TA) are specified across 8 topics: TA1 IoE Fundamentals, TA2 Cyber threats, TA3 Social Engineering Attacks, TA4 Authentication Controls, TA5 Software Patches & Updates, TA6 Malware Defenses, TA7 Secure Communications & Data Security, and TA8 Incident Handling and Response. Section 4 discusses in detail the proposed thematic areas.

Figure 1 lists the thematic areas included in Table 1, the relevant high-level learning objectives that should be pursued in the context of the five cybersecurity areas (identify, protect, detect, respond, and recover) and maps them to the Bloom's taxonomy. As indicated in Fig. 1, the first three layers (remember, understand, apply) of Bloom's taxonomy can promote consumers' situational awareness. Situational awareness capabilities should be perceived as the fundamental capabilities needed towards societal cyber resilience. Once consumers acquire such capabilities, then the next step is to cultivate their critical thinking skills in the context of the other layers (analyze, evaluate, create) of the Bloom's taxonomy. By developing this skillset, consumers can take an active role in the management of cyber incidents, and a sustainable cyber hygiene behavior can be promoted.

Table 1. Thematic areas mapped to NIST Cybersecurity Framework areas

NIST Cybersecurity framework functional areas	Thematic Areas (TA)
Identify	TA1 IoE Fundamentals TA2 Cyber Threats TA3 Social engineering attacks
Protect	TA4 Authentication Controls TA5 Software Patches & Updates TA6 Malware Defenses TA7 Secure Communications & Data Security
Detect	TA 8 Incident Handling and Response
Respond	
Recover	

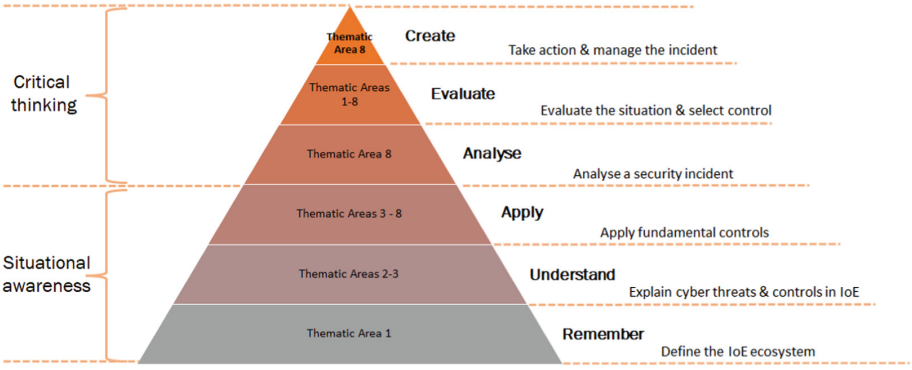

Fig. 1. Pursued high-level learning objectives versus Bloom's taxonomy

4 IoE Curricula Design Guidelines

This section provides guidelines to curricula designers and trainers as to the thematic areas they should consider in the design and delivery of specialized cybersecurity curricula to build consumers' cyber resilience competencies in the context of the IoE ecosystem. For each thematic area, the key topics to consider in the design of the curricula are specified, highlighting specific skills and knowledge that should be developed in the context of the NIST Cybersecurity Framework and taking into consideration the IoT-related cyber threat landscape [3, 10].

4.1 Thematic Area 1: IoE Fundamentals

The aim of this thematic area is to introduce to consumers the IoE ecosystem, present its characteristics and how it fits in the context of ubiquitous decentralization. Understanding

the decentralized nature of this environment should be a key element of this thematic area as it is the first step to realize the cybersecurity challenges linked to this ecosystem. The IoE ecosystem extends the traditional (centralized) security perimeter which now is distributed across the IoE ecosystem. Therefore, protection needs to be applied across the different components that constitute the IoE ecosystem. An important element of the IoE ecosystem is the IoT. Consumers have a significant role in the IoE ecosystem as end-users of IoT products, e.g., in the context of smart homes. Efforts should be placed on raising awareness across consumers regarding the risks that exist in this environment so they can realize how their privacy can be compromised and take informed decisions when utilizing IoT solutions, including applying best practices to enhance their security.

4.2 Thematic Area 2: IoE Cyber Threats

A variety of cyber threats are related to IoE and need to be addressed by different actors, e.g., consumers, professionals, policy makers, etc., by applying appropriate technologies and controls. Consumers cannot defend what they do not know or do not understand. Therefore, it is critical to highlight this aspect in IoE cybersecurity awareness raising and training modules that aim to educate consumers. An approach to take is to focus on promoting a good level of understanding on fundamental concepts in cybersecurity, such as what constitutes a threat actor, a threat, a vulnerability, a risk and what the impact might be from a successful compromisation. Taking this a step further, it is vital for consumers to understand the adversaries' mindset and what is the typical attack strategy they implement to discover and exploit a vulnerability. Understanding how easily a vulnerability can be discovered and exploited, and the magnitude of a potential impact on a personal and societal level, can enhance the concept that cybersecurity is an aspect that concerns the entire society, not only professionals, and actions need to be taken by all, including consumers.

4.3 Thematic Area 3: Social Engineering Attacks

Even though the efforts of the cybersecurity community to increase awareness on social engineering attacks, a great percentage of consumers still falls for the phish. As IoE evolves and consumers are presented with new smart solutions, they need to be equipped with the necessary knowledge and skills to identify the different forms of social engineering, e.g., phishing, vishing, etc., and defend accordingly by applying critical thinking and taking smart decisions. The fact that adversaries often profile their targets to increase the success of a social engineering attack, is not usually evident to consumers. Thus, it is important to highlight this aspect in cyber raising awareness sessions and to build knowledge and skills to consumers to evaluate how personal and other IoE-related data can be glued together to profile someone and perform a social engineering attack. Moreover, to build societal resilience, consumers need to be able to anticipate social engineering attacks in the context of smart environments, especially in the case of smart homes. By having the ability to anticipate potential social engineering attacks, consumers might have better chances to identify and address such an attack.

4.4 Thematic Area 4: Authentication Controls

Weak authentication is a common vulnerability [1, 3] that adversaries are exploiting to gain unauthorised access to systems. The bad password construction strategies that consumers are using are well known to the adversaries. Unfortunately, consumers often do not realize that the strategies they are using lead to weak passwords. Having a false sense of security is a great obstacle to overcome and convince consumers to change their habits. To address this obstacle, one approach to consider is to demonstrate to consumers how password cracking is performed, and how the adversaries' chances to succeed increase by using bad password construction strategies or by profiling a target. In thematic area 3, the topic of profiling a user is covered. Profiling can be useful in different aspects of compromising authentication controls, such as identifying answers to authentication questions. The extent to which profiling can be utilized is usually not evident to consumers. By demonstrating how profiling can be useful to an adversary, consumers can become more reflective when sharing information and using sensor data. This thematic area should also cover other essential topics such as authentication management and develop citizens' capabilities to utilize a password manager.

4.5 Thematic Area 5: Software Patches and Updates

Use of outdated IoT components is among OWASP IoT Top 10 list [3] of vulnerabilities. Adversaries have in their arsenal a variety of tools which can utilize to scan for vulnerable devices and identify unpatched and/or outdated systems with known vulnerabilities. In the IoE ecosystem, there are different devices, e.g., smart phones, tablets, networking appliances, sensors, etc., that consumers need to keep up to date to limit the risk of exploitation. Although cybersecurity raising awareness activities highlight the need to keep systems up to date, they touch this aspect superficially rather than developing consumers' skills to be able to perform this task. Although updating components is not always straightforward and it depends on the device capabilities [13], it is essential to equip citizens with appropriate knowledge and skills to configure automatic updates where possible, and also perform manual updates where automating this task might not be supported.

4.6 Thematic Area 6: Malware Defenses

Malware is a common attack vector that adversaries are utilizing to compromise the operation of systems, exfiltrate sensitive information or perform other malicious activities. Consumers should gain a good understanding of the different types of malware, e.g., botnets, ransomware, crypto-miner, keyloggers, etc., what their purpose is and how these can be delivered to them. To protect against malware, consumers should at least know how to use an anti-malware solution which they need to keep up to date. Furthermore, appropriate skills should be developed to be able to configure devices, e.g., smartphone, tablet, etc., to conduct an automated or manual anti-malware scan.

4.7 Thematic Area 7: Secure Communications and Data Security

An essential security property is confidentiality. Confidentiality ensures that the data are kept secret from third parties that are not authorized to access them. Data confidentiality must be protected either while data are in transit, meaning they are communicated between actors and/or devices in the IoE ecosystem, or they are at rest. Consumers should be educated on the available encryption standards and tools to use to secure communications and protect data stored on the IoE devices. Building such knowledge can support consumers in making informed decisions when having to select appropriate security configurations and protect their data. Moreover, given that wireless and cellular networks are a core component of the IoE ecosystem, consumers should develop capabilities to configure, for example, wireless access points, wireless routers, and mobile devices to use the strongest encryption standards possible.

Data at rest should also be protected. Thus, citizens should be able to use encryption tools and/or configure IoE devices and platforms to encrypt sensitive information stored on them.

4.8 Thematic Area 8: Incident Handling and Response

Building citizens' knowledge and skills on incident handling and response can tremendously support the efforts to promote societal cyber resilience. By having consumers reporting potential cyber incidents, authorities can take early actions to launch specialized awareness raising campaigns, issue guidelines, etc., and proactively prepare consumers for malicious activities that might be rising. As a first step, it is essential to guide consumers to maintain contact information of appropriate security authorities which they can contact to report an incident. Beyond that, it is a necessity to build capabilities so that consumers can identify abnormal behavior of an IoE device. To this end, curriculum designers should consider what abnormal behavior entails at a level that consumers can understand and identify. It should not be assumed that consumers have deep technical knowledge and capabilities to perform deep investigations regarding an incident. At the very least, consumers should be able to interpret results from tools such as anti-malware tools and be aware of the situation.

Once the fundamental capabilities are developed across the thematic areas presented in this work, then the next step is to specify more advanced topics to deepen consumers' knowledge and skills.

5 Conclusions

The IoE brings together people, processes, data, and things to create smarter environments across different sectors. In the context of consumer IoE ecosystem, connected devices in households provide new capabilities, richer experiences and offer a better quality of services and life to citizens. Even though the benefits, connected devices pose a great risk to consumers if a cyber hygiene behavior is not adopted. Consumers constitute a key actor in the IoE ecosystem. Efforts should be made to educate consumers, beyond cybersecurity awareness raising, to build their cyber resilience competencies.

Such competencies will allow consumers to protect their connected devices and data and handle a potential incident to a reasonable level. It is time to start specifying the fundamental technical skills that consumers need to acquire and design specialized curricula to develop them. The aim of this research work was to identify the thematic areas in which cyber resilience competencies should be developed and provide initial directions to curricula designers and trainers as to the key topics they need to consider when designing and delivering specialized curricula in the context of the IoE ecosystem. Future work will extend the current contributions, providing further guidelines, specifying the learning objectives and the pedagogy to materialize a relevant cybersecurity curriculum and upskill consumers, aiming to increase societal cyber resilience in the context of the IoE ecosystem.

References

1. Malan, J., Eager, J., Lale-Demoz, E., Cacciaguerra, G., Brady, M.: Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things (IoT) Landscape. Centre for Strategy & Evaluation (2020)
2. Holst, A.: 'IoT connected devices worldwide 2019–2030', *Statista*. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. Accessed 13 Dec 2021
3. OWASP, OWASP Internet of Things Project. https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main. Accessed 14 Dec 14 2021
4. NETSCOUT, Threat Intelligence Report - Dawn of the Terrorbit Era. Accessed 13 Dec 2021. https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat%20Intelligence%20Report%202H%202018.pdf
5. Internet Society, The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things, *Internet Society*. https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/. Accessed 13 Dec 2021
6. Stavrou, E.: Back to basics: towards building societal resilience against a cyber pandemic. J. Systemics, Cybern. Inf. **18**(7), 73–80 (2020)
7. NIST, NIST Cybersecurity Framework, *NIST*, February 05, 2018. https://www.nist.gov/cyberframework/framework. Accessed 30 May 2022
8. Maennel, K., Mäses, S., Maennel, O.: Cyber hygiene: the big picture. In: Gruschka, N. (ed.) NordSec 2018. LNCS, vol. 11252, pp. 291–305. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03638-6_18
9. Vishwanath, A., et al.: Cyber hygiene: The concept, its measure, and its initial tests. Decis. Support Syst. **128**, 113160 (2020). https://doi.org/10.1016/j.dss.2019.113160
10. ENISA, ENISA Threat Landscape 2021, *ENISA*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021. Accessed 14 Dec 2021
11. Vailshery, L., Sujay.: Average number of connected devices in UK households 2020. *Statista*. https://www.statista.com/statistics/1107269/average-number-connected-devices-uk-house/. Accessed 14 Dec 2021
12. Deloitte, How the pandemic has stress-tested the crowded digital home. https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey.html. Accessed 13 Dec 2021
13. ENISA, Guidelines for Securing the Internet of Things, *ENISA*. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things. Accessed 14 Dec 2021
14. Wikipedia, 'Mirai (malware)', *Wikipedia*. December. 14, 2021. https://en.wikipedia.org/w/index.php?title=Mirai(malware)&oldid=1060214070. Accessed 14 Dec 2021

15. Joint Task Force on Cybersecurity E, Cybersecurity Curricula 2017. New York NY, USA: ACM 2018 https://doi.org/10.1145/3422808
16. 'CyBOK', *The Cyber Security Body Of Knowledge*. https://www.cybok.org/. Accessed 30 May 2022
17. Bada, M., Sasse, A.M., Nurse, J.R.C.: 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), pp. 118–131 Coventry, UK (2015)
18. Goel, S., Williams, K., Dincelli, E.: Got phished? internet security and human vulnerability. J. Assoc. Inf. Syst. **18**, 22–44 (2017). https://doi.org/10.17705/1jais.00447
19. ENISA, Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, April 16, 2019. https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity. Accessed 14 Dec 2021
20. European Commission, Joint Research Centre, Baldini, G., Barrero, J., Draper, G., et al.: Cybersecurity, our digital anchor : a European perspective. In: Dewar, M., et al. (eds.) Publications Office (2020). https://data.europa.eu/doi/10.2760/352218. Accessed 14 Dec 14 2021
21. McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., Lillie, M.: The effect of resilience and job stress on information security awareness. Inf. Comput. Secur. **26**(3), 277–289 (2018). https://doi.org/10.1108/ICS-03-2018-0032
22. European Court of Auditors, Challenges to effective EU cybersecurity policy (2019). https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf. Accessed 14 Dec 2021
23. European Economic and Social Committee, 'Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks'. https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf. Accessed 14 Dec 2021
24. ENISA, Raising awareness of cybersecurity: a key element of national cybersecurity strategies. Publications Office, LU (2021). https://data.europa.eu/doi/10.2824/363629. Accessed May 30 2022
25. Parrish, A., et al.: Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In: Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education, New York, NY, USA, Jul. 2018, pp. 36–54 (2018). https://doi.org/10.1145/3293881.3295778