Understanding the Last Line of Defense: Human Response to Cybersecurity Events

Summer Rebensky, Meredith Carroll(✉), Andrew Nakushian, Maria Chaparro, and Tricia Prior

Florida Institute of Technology, Melbourne, FL 32901, USA
mcarroll@fit.edu

Abstract. Cybersecurity in consumer, corporate, and military settings, continues to be a growing concern in the modern and technologically driven world. As Wiederhold (2014) puts it, "the human factor remains the security's weakest link in cyberspace." A literature review related to human response to cybersecurity events reveals three phases involved in the cybersecurity response process, including: (1) Susceptibility, the phase preceding an event, which primarily encompasses behaviors that impact vulnerability to a cybersecurity event; (2) Detection of the event when it occurs; and (3) Response to the event after it occurs. In order for an individual to effectively protect themselves and their organizations from cybersecurity breaches, they must understand and be sensitive to the susceptibility of their devices, and when a potential breach occurs, must exhibit rapid and effective response. The goal of this effort was to examine the human factors surrounding non-expert response to a cybersecurity vulnerability or event and create a framework based on the literature. Recommendations for what steps can be taken to better prepare individuals to respond to cyber events is provided.

Keywords: Cybersecurity · Internet of Things (IoT) · Human factors · Information security · Decision making

1 Introduction

Cybersecurity is increasingly becoming a threat across a range of different industries. In a report by the United States Government Accountability Office (GAO), 23 of the 24 major federal agencies noted information security as a major problem that needed more management, with 19 of those agencies noting their weakness in information security procedures. The number of cybersecurity incidents for federal agencies has increased from 5,503 in 2006 to 77,183 in 2015 [1]. In 2016, the U.S. Navy experienced a breach of 134,386 sailor names and social security numbers from the compromise of only one laptop [2]. These threats are not limited to the government and military, as three billion users were affected by the Yahoo! Inc. hack in 2016 and 143 million by the Equifax Inc. hack in 2017 [3].

Prevention of breaches in cybersecurity has typically focused on providing technical solutions such as hardening networks and improving computer systems that detect

A. Moallem (Ed.): HCII 2021, LNCS 12788, pp. 353–366, 2021.
https://doi.org/10.1007/978-3-030-77392-2_23

intrusions and enhance safe information sharing, with little focus on the device user [1]. However, the device user is often the last line of defense. In fact, in 2017 the U.S. GAO highlighted the lack of properly trained personnel as one of the needed areas of improvement for cybersecurity effectiveness and noted a lack of sufficiently trained staff and procedures for cybersecurity response [1]. Although it is the last line of defense, “the human factor remains the security’s weakest link in cyberspace” (p. 131, [4]). This highlights some critical questions. Are device users equipped with the training and tools necessary to recognize cybersecurity vulnerabilities and detect when a system is being compromised? Do device users know how to respond once a cybersecurity event is detected?

These questions are of particular interest to the Internet of Things (IoT) device industry as everyday electronic devices are becoming more connected to the outside world. Suresh et al. (2014) defines the Internet of Things as “a connection between humans – computers – things (p. 2, [5]).” From doorbells to refrigerators to smart phones, more devices are being connected to the internet than ever before. Consumers are adding these devices into their homes and connecting them with the internet creating “Smart Homes” [6]. These smart home devices are now ubiquitous in homes and workplaces of many people. While these smart devices may seem benign in terms of cybersecurity risks, they are connected to the internet and as such they pose a risk to private personal information leaks. Despite the widespread usage of IoT devices, there is a significant lack of knowledge in IoT security. Many smart home owner’s do not recognize risks associated with the IoT devices and trust device manufactures to protect their privacy [7]. Further, individuals who are knowledgeable about the risks of IoT devices do not use the recommended safety best practices [8]. For example, many users understand two-factor authentication can better protect their devices and accounts but still fail to utilize this technique as they find the cost of doing so to outweigh the associated risks [9]. As such, it is important to understand if consumers can effectively recognize and respond to potential cybersecurity threats to applications such as these.

The goal of this effort was to examine the human factors surrounding detection of, and response to, a cybersecurity event by a device user, who is not a cybersecurity expert. Specifically, how do device users, whose focus is not cybersecurity, make decisions regarding potential privacy vulnerabilities or events, and what steps can be taken to better prepare them to respond to such events? To achieve this, we reviewed the literature to determine what research has found regarding the human factors of cybersecurity decision making. The effort examined research conducted to date in various domains including IoT. The methods and findings, along with recommendations for promoting effective cybersecurity decision making in IoT and beyond, are described in the following sections.

2 Method

A literature review was conducted to identify what research exists regarding consumer preparation for, and decision making associated with, cybersecurity vulnerabilities and cybersecurity events across several domains, including IoT.

Using a compiled list of keywords targeting user decision-making associated with cybersecurity events, we performed an extensive keyword search of databases including: Sage Journals, ScienceDirect, Wiley Online, IEEE Xplore, Proquest, SpringerLink, Defense Technical Information Center, Taylor and Francis Online, and Florida Institute of Technology library holdings. The following keyword phrases were utilized: trust and cyber-attack, human factors and cyber-attack, cyber event and trust, system hack and trust/aviation, human detection of cyber events, human behavior cyber-attack, human cyber detection, cyber situational awareness, human cyber malicious attack, human cognitive cyber information hacking, prospect theory behavioral cyber threat, information security, IoT Cybersecurity, Smart Home, user trust of IoT devices, and framing theory. Throughout the duration of the literature review, we reviewed approximately 450 abstracts to determine if the articles focused on human factors of cybersecurity events. Abstracts were reviewed to ensure the focus of the article was on the device user and the decision process, detection of cybersecurity events, influencing factors, or the human response to cybersecurity events. Of the initially reviewed abstracts, we selected 72 of the publications for full review to determine if they were relevant to a device user's cybersecurity decision process. Based on a full review of these publications, we selected a total of 44 publications for analysis. We examined literature from several domains that explored how individuals make decisions related to cybersecurity events and associated human factors concerns. The domains included: Personal Computing (e.g., individual home computer use), Corporate Information Security (e.g., system security, encrypting files, updating software), Network Security (e.g., observing network activity on a server), IoT (e.g., smart home devices, artificial intelligence assistants), and General Cybersecurity (e.g., articles that addressed cybersecurity as a whole or across multiple domains). Twenty-two empirical studies, nineteen theoretical publications, and three online media sources were reviewed in detail and analyzed. See the summary of the literature review process is presented in Fig. 1.

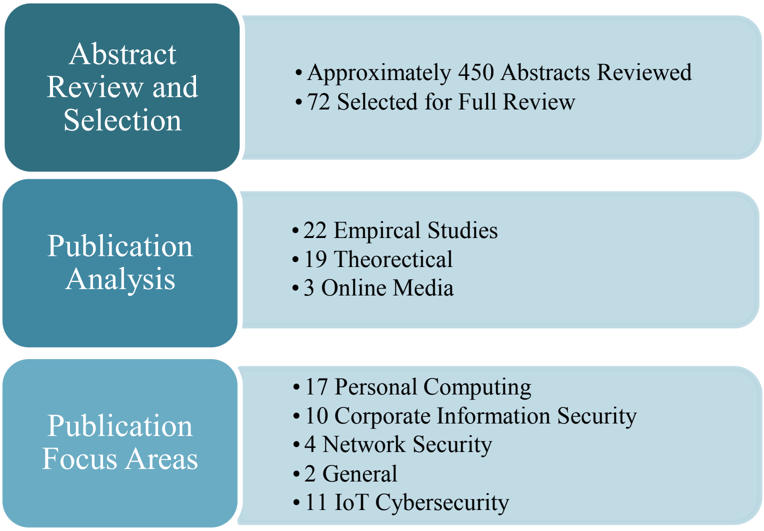

Fig. 1. Literature review process

Each article was analyzed and data related to human interaction with the cybersecurity event was extracted, including: (a) the type of event, (b) factors that influenced the decision process during the event, (c) the factors that influenced user response to the event, (d) how the event influenced a user's performance on, and future trust in, a system, and (e) mitigations, or steps that can be taken to improve human response to similar events. The research team then analyzed the data for trends and extracted two types of categorical themes: (a) stages of human response to cybersecurity events and (b) factors that influence human response to cybersecurity events. From this, a framework of factors which impact the three stages of human response to cybersecurity events was developed.

3 Results: Framework of Human Response to Cyber Security Event

Three stages of cybersecurity decision making were evident from the literature reviewed, including: (1) Susceptibility, the stage preceding the event which primarily encompasses behaviors that impact vulnerability to a cybersecurity event, (2) Detection of the event when it occurs, and (3) Response to the event after it occurs. Second, nine factors were identified from that literature that influenced a user's cybersecurity decision making process across these three stages, including: (a) perceived susceptibility, (b) safeguard cost and effectiveness, (c) privacy fatigue, (d) system trust, (e) system reliability, (f) system knowledge, (g) cybersecurity knowledge and experience, (h) saliency of the cybersecurity event, and (i) system transparency. Table 1 presents a mapping of the three stages of the cybersecurity decision making process to the nine factors which influence these stages. Also included in the table are descriptions and examples of the three stages, number of publications that provide support for each stage, and indication (via an X) of which stages are influenced by each factor.

3.1 Susceptibility Phase

The first stage of cybersecurity decision process, susceptibility, is the a priori state of the individual prior to experiencing a cybersecurity event. This stage focuses on one's perceptions of the likelihood of an attack. This includes awareness of potential cybersecurity events, how individuals view the security of their systems, and the preventative steps an individual user takes. There are several factors which impact an individual's susceptibility to experiencing a cybersecurity event. The following section describes the factors that influence the stage of susceptibility in individuals across a range of domains.

Perceived Susceptibility. Perceived susceptibility to cybersecurity events is a critical factor that influences susceptibility and all of the subsequent stages of the cybersecurity decision process. If someone does not feel that they are susceptible, when an anomaly occurs, they will not consider the possibility that a cybersecurity threat is the cause, and in turn, may not respond effectively [10]. Further, if individuals understand that they are susceptible and that there is a threat, they are more likely to exhibit safe security behaviors [11]. Research across multiple domains has shown that many individuals exhibit optimism bias, the belief that they are not at risk and do not need to take steps to prevent cybersecurity events [12, 13].

For example, research has shown that executives often see their companies as less likely to be targeted and believe that they better protect themselves from a cybersecurity threat than their competitors [14]. Research has also shown that, with respect to IoT devices, younger generations, regardless of gender, expressed more concern towards the

Table 1. Cybersecurity decision response framework

		Phase		
		Susceptibility	Detection	Response
Hypothetical Examples		Checking the last time an application was updated to gauge current risk Feeling hesitant to open a link in an email with poor spelling	Noticing changes in device displays that were not initiated by the user or frequent and inexplicable program crashes	Checking security information to determine website safety; subsequent use/disuse of website after cybersecurity event
# of Supporting Studies		15	14	5
Factors influencing decision process	Perceived Susceptibility	X	X	X
	Perceived Safeguard Cost & Effectiveness	X		X
	Privacy Fatigue	X		X
	System Trust	X		
	System Reliability	X		
	System Knowledge	X	X	
	Cybersecurity Knowledge & Experience	**X**	**X**	**X**
	Saliency of Cybersecurity Event		**X**	
	System Transparency		**X**	

risk of susceptibility to cyberattacks, when compared to older generations, and these concerns were more likely to influence purchasing decisions [15].

Safeguard Cost & Effectiveness and Privacy Fatigue. Individuals will not engage in security compliance or assurance behaviors, such as frequently changing passwords, if they do not perceive safeguards as effective (i.e., do not understand how their behaviors improve cybersecurity), or feel that it is not their job or that the safeguard is too costly [16]. This can lead to negative attitudes towards security, and psychological distancing from security responsibility [17]. The resulting lack of effective security behaviors can leave systems more vulnerable to attacks. Choi et al. (2018) explain that as data breaches increase in frequency individuals may feel tired of taking actions to prevent data loss and will stop devoting energy to safeguarding information [9]. This is because the "fatigued" individuals believe the safeguard cost is greater than the safeguard effectiveness. This phenomenon is called privacy fatigue. For example, Breitinger et al. (2020) explain that while most individuals will use passwords on their smartphones, they do not take part in other recommended safe practices such as using a VPN while connected to public WiFi and turning off unused features, resulting in mobile devices being less secure than desktop computers [8].

Trust and Reliability. Trust in the system plays a key role in the susceptibility stage and is highly dependent on another factor, system reliability. Trust in a system is dynamic and contingent on system reliability and performance, and can be comprised of attitudes, expectations, attributes, feelings, intention, and traits [18]. If a system is highly reliable, individuals are likely to form habitual trust, which can decrease perception of risk, and as a result, decrease awareness and detection of a cybersecurity event [10]. Similar to findings from the trust-in-automation literature [19], consistent shutdowns or false alerts from a system can degrade a user's trust in that system's performance, this could eventually lead to disregard of a cybersecurity alert during a cybersecurity event that shares similar characteristics [20]. Therefore, system reliability is critical to ensure trust is properly calibrated. Research has also shown that ease of use, perceived usefulness, community interest, as well as an individual user's social network can also influence trust [21]. For example, smart home owners trust the device manufactures to protect their private data, and the user's perception of how useful and convenient the IoT device is influences their privacy behaviors and trust [7].

System Knowledge and Cybersecurity Knowledge and Experience. System knowledge impacts susceptibility to a cybersecurity event. Users who have system knowledge and understand associated cybersecurity vulnerabilities are more likely to trust a system's ability to protect information confidentiality, integrity, and availability, whereas individuals who lack system knowledge tend to exhibit misplaced trust in a system [22]. For example, IoT device use is ubiquitous in the modern world and these devices are used in places where many people may not consider cyber-vulnerabilities (e.g., utilizing a QR code in a grocery store [23]. If a device is connected to the internet in any way then it is not 100% secure from cybersecurity threats. Therefore, the question arises: do users have the knowledge of the system to protect themselves, as devices that were not originally connected become connected?

Knowledge of, and experience with, cybersecurity events also influence susceptibility. A study in 2010 found that the perceived damage after a cybersecurity attack affects an individual's likelihood to continue to use that system [24]. If there are comparable alternatives, individuals are more likely to move to comparable systems, even if the affected system has a higher perceived usefulness. Further, individuals who do not have a full mental model of how cybersecurity threats occur can develop ineffective coping mechanisms, which could include avoiding the use of a susceptible system altogether [25].

3.2 Detection Phase

The second stage of the cybersecurity decision process is detection of the cybersecurity event. This includes the ability of a user to detect and correctly identify a cybersecurity event, or distinguish a cybersecurity attack from a system anomaly due to a potential system error. Several of the factors that influence susceptibility also influence how likely an individual is to detect a cybersecurity event. The following section describes the factors that influence the stage of detection.

Cybersecurity Knowledge and Experience. A user's knowledge of, and experience with cybersecurity events can also affect their ability to detect such events. A study conducted by Ben-Asher and Gonzalez (2015), which examined participants' response to malicious network attacks, found that cybersecurity experts, or those with extensive cybersecurity experience and knowledge, were more effective at detecting malicious attacks, and had significantly fewer false alarms than their novice counterparts [26]. The authors suggest this may be due to the experts' ability to detect relevant cues and meaningful patterns indicative of a cybersecurity attack. IoT device users are often unaware of security setting or security mitigations for the device [6] and as such, users are vulnerable to IoT manufacturers pulling personal data from the IoT device. Many users do not perceive the risk associated with IoT devices or regard them as convenient enough to be worth the risk [7].

System Knowledge and System Transparency. A user's system knowledge can influence their ability to detect a cybersecurity event. Multiple studies have shown that users must have sufficient knowledge about how the system operates to determine whether system behavior is abnormal, and potentially indicative of a cybersecurity attack [27], as cited in [25, 26, 28–30]. System transparency also impacts detection of a cybersecurity event. A user must use information that the system provides to determine if a threat is occurring. If the system does not provide information related to current system processes (e.g., confirmation that the most up-to-date security patches are installed), new software installed, or system status (e.g., system resources currently being overloaded), individuals cannot determine if the abnormal system behavior is due to a cybersecurity event [31]. Furthermore, manufacturers are often not transparent with device security and frequently users cannot change the security settings [6]. This practice leads to a lack of awareness of the risks the device poses and means by which to instill protections.

Saliency of Cybersecurity Event. Saliency of a cybersecurity event can also influence detection. For example, a conspicuous attack is one that results in obvious cues, such as a computer crashing or control of the computer being taken over, versus a less salient attack which may only result in slowed system response. A study conducted by Hirshfield et al. (2015) found that users are more likely to detect salient cybersecurity attacks than less salient attacks that appear to be due to a user or system error [30].

3.3 Response Phase

The third stage of the cybersecurity event response is user execution of a response to the cybersecurity event. The literature suggests that multiple factors impact how an individual responds to cybersecurity events. The following section describes the factors that influence the response stage.

Perceived Susceptibility, Safeguard Cost Effectiveness, and Privacy Fatigue. In a study examining computer user response to spyware, Huigang and Yaijong (2010) found that individual response to potential cybersecurity threats was influenced by a chain reaction of inter-related factors [32]. Individuals must (1) believe the threat exists (perceive susceptibility), (2) believe that the threat is avoidable (perceive safeguard effectiveness), and be willing to burden safeguard cost (e.g., financial, time-related, or resources costs with implementing safeguards such as frequently changing passwords), and (3) detect the threat. If the threat is perceived as low risk or safeguards costs are perceived as either too high cost or ineffective at combating the threat, individuals may not take the steps necessary for cybersecurity protection. Interestingly, the attitudes individuals have towards cybersecurity and their behaviors tend to differ, a phenomenon referred to as the privacy paradox [33]; while many individuals may state that they care about protecting the security of their devices, due to a perception of high safeguard costs, safeguards necessary to ensure security are not implemented. The concern and worry expressed towards cybersecurity events also depends on the type of information being held by the device [34]. For example, users tend to be more concerned about the privacy of bank account information compared to height and weight information.

Cybersecurity Knowledge and Experience. A user's cybersecurity knowledge and experience can impact detection as presented above but can also influence how they respond to a cybersecurity event. In a study examining participant response to secure and insecure websites, Kelly and Betenthal (2016) found that participants with high levels of cybersecurity knowledge collected more information before proceeding with a login (as indicated by mouse trajectories), than individuals with low levels of cybersecurity knowledge [35]. As a result, those with high levels of cybersecurity knowledge were also more likely to proceed in logging into secure websites whereas those with low levels of cybersecurity knowledge failed to recognize the right cues and logged into unsecure websites. In a study conducted by Rosoff, Cui, and John (2013), computer users were asked how they would respond to a cybersecurity dilemma encountered while downloading online music or buying from an online store [36]. Results indicated that recall of prior cybersecurity experiences influenced how the users would respond: recall of negative cybersecurity experiences (e.g., experienced a loss of data due to a virus) led to less-risky responses; recall of positive cybersecurity experiences (e.g., remained unaffected during a security breach) led to higher-risk responses.

4 Strategies for Improving Response

The three stages presented in the framework of a device user's cybersecurity decision process provide opportunities to better support the user in making the right decision. The literature review uncovered numerous mitigation strategies that can be utilized to achieve this. Below we present mitigation strategies, including system design, training, and procedure recommendations that can be utilized to target each of the three stages of the cybersecurity decision process across numerous domains, whether an individual is using an IoT device at the office or using their personal computer at home.

4.1 Mitigations for the Susceptibility Stage

Increase Awareness of Cybersecurity Vulnerabilities. Users need to be aware of cybersecurity vulnerabilities and how these can affect their systems. Employees who do not manage security as their main job, often do not understand how their behaviors affect security [16]. Removing the bias that they are not susceptible is the first step. SETA (Security Education, Training, and Awareness) programs, or programs focusing on improving attitudes, effort, and one's responsibilities to improve cybersecurity, have shown to decrease unsafe behaviors and improve precaution taking [17]. Increased awareness training could provide users insight into the vulnerabilities in their IoT devices. For example, users could be made aware of their own current exposure to cybersecurity threats such as the sharing of their private information with third party vendors. Since many users do not perceive themselves at risk, demonstrating their actual exposure could influence them to change their behaviors and take more precautions. Similarly, awareness could be increased by a company's own IT department explaining actual events that have happened at the company.

Develop Procedures and Training for Cybersecurity Safeguards. Users should be trained on procedures that can help protect their systems from potential cybersecurity vulnerabilities. Given that steps to ensure security may cost users much needed time to perform their primary task, safeguards must be quick, logical, and easy to complete. Individuals are likely to avoid effective security behaviors if a) they believe they are unlikely to be targeted, b) risks are low, c) they find safeguards ineffective, d) they find safeguards too costly, or e) they lack the skills to implement safeguards [37]. An example, of a procedure to help maintain user compliance with cybersecurity safeguards would be to provide a "security status update" which would highlight current vulnerabilities and ways to protect oneself in a brief and easy to understand format. This status update could be sent to users on a weekly basis the same way some smartphones send a weekly activity log. These updates would convey best practices, and over time, train users to have better cybersecurity habits.

Utilize Positive Framing in Training. Too much fear instilling during training can cause users to not exhibit safe security behaviors. Framing training in a positive frame (i.e., what you will gain from protection), versus loss (i.e., what will happen if you do not protect your systems) has been shown to be a more effective method for security training [11, 36, 38]. For example, a company could create a cybersecurity training course that highlights the benefits of following these recommended best practices. Instead of telling users, “if you do not take precautions you will get hacked”, the training could convey “taking precautions will keep you safe and save you precious time and energy in the long run.”

4.2 Mitigations for the Detection Phase

Increase System Transparency. It is important that the information systems provide users with information regarding data source, validation, and update feeds. This includes detail regarding activity, changes, inconsistencies, and potential compromises that are relevant to the cybersecurity of their system information. If the display does not give enough detail on information sources and the status of these sources, it will be very difficult for an individual to correctly determine if an event is a cybersecurity attack [31]. Many IoT systems such as a smart watch and fitness tracking applications collect personal information and track user behavior [39]. These devices should make it evident to individual users what information is being collected, where it is being stored, and how it is being used. Applications should also inform users about the integrity of the storage location, whether it is being stored locally on the device or remotely on a server, and what parties have access to this information.

Provide System Feedback. Information systems should provide feedback when false alarms, errors, or failures occur, allowing users to have a better understanding of “normal” system behavior [18]. Users need to understand what unreliable system behavior looks like (e.g., from error alerts), in order to have a baseline with which to compare a cybersecurity event.

Provide Security Alerts and Status. Information systems should incorporate automated detection and alert of cybersecurity vulnerabilities and compromises, where possible. Given that most users are not cybersecurity experts, they will need support in detecting and diagnosing these events. Further, during normal operations, information systems should provide symbols or notifications that connections are secure, safe, and up-to-date [20, 35]. For example, providing security messages, when users’ private information is requested, that prompt users to decide what information to share and whether to accept or deny a request to access specific information [40]. Providing alerts such as these allows devices to be more transparent to users.

Train System Knowledge. Users need to have an understanding of where both incoming information comes from and where outgoing information goes. This allows a user to discern between system behavior and cybersecurity threat behavior. System knowledge has shown to improve a user’s correct detection of a cybersecurity attack across information security, networking, and personal computing domains [22, 25, 26, 35]. Increasing system knowledge in less reliable systems will assist users in understanding what is causing behavior in the system, and whether or not it should raise concern [10, 18, 22]. For example, IoT devices should inform users about different aspects of the system and implications for cybersecurity and privacy, including disclosing the type of sensors, what data is collected, when the next security update will be, what physical actuations the device has, purpose of data collection, and where data is being stored [41]. Providing this information will allow a user to be aware of what the device is doing with their information and detect any suspicious activity.

4.3 Mitigations for the Response Phase

Develop Procedures and Training for Cybersecurity Response. Users should be provided procedures for how to respond to a potential cybersecurity threat. Providing individuals with procedures to determine if a cybersecurity attack has occurred can improve the rate of correctly identifying cybersecurity events [20, 25, 42]. An example of a system that helps one determine whether a cybersecurity event has occurred would be an antivirus software on a PC. These software packages give step by step instructions for handling the event. Implementing software packages like this on all IoT devices would have users better identify and respond to cybersecurity events.

Provide Opportunity to Report Potential Cybersecurity Events. Users should be given access to a reporting system that allows reporting of any system behavior that they suspect might be due to a cybersecurity vulnerability. Such a system provides the opportunity to improve the system security and inform procedures and training [43]. For example, many banking applications will show users how to identify and report unauthorized account activity. In the case of IoT devices this could be a form on the manufacturer's website or within the controlling application.

Train Basic Cybersecurity Knowledge. While training all users as cybersecurity experts is infeasible, training users on basic cybersecurity knowledge, relevant to their systems, will increase their ability to detect the onset of cybersecurity events and to effectively respond. It is inevitable that as information systems, whether they be smart home IoT systems or smartphones become more automated and digitized, future users will need to exhibit more computer aptitude to support more effective performance [44].

5 Conclusion

This research effort sought to explore the human factors associated with the cybersecurity decision process for device users who are not cybersecurity experts. A review of literature in this domain revealed three key stages in this process that are influenced by nine separate factors. Based on the literature review findings, this paper puts forward recommended mitigations for influencing these nine factors and improving cybersecurity response in a range of domains. Such mitigations have shown great promise. For instance, in federal agency network systems, there has been a 50% drop in incident reports from 2015 to 2016, due to the implementation of mitigation strategies such as adding cybersecurity infrastructure for reporting and managing cybersecurity events [1]. By taking the necessary actions, the human factors associated with cybersecurity and privacy can be more effectively managed. Developers can use this framework to design features that allow users to make more educated decisions about managing their data.

If one understands how the apparent safeguard costs affect decision making regarding user settings, developers could develop better applications and companies could educate their employees on making good privacy decisions in order to protect company data.

Future steps in this effort involved validating the framework. Currently we are administering an online survey to college students and military personnel examining their cybersecurity perceptions, knowledge and behaviors associated with IoT device use. The results of this ongoing study will provide information to help develop guidance for the development of applications to address all three stages. Future studies should empirically examine user response to simulated cybersecurity or privacy events to more thoroughly examine the proposed influencing factors and to explore the effectiveness of the recommended mitigations.

References

1. GAO, Cybersecurity: Actions needed to strengthen U.S. Capabilities, GAO-17-440T, Washington, D.C., 14 February 2017
2. Chief of Naval Personnel Public Affairs: Security Breach Notification of Sailors' PII FAQ (2016). https://www.public.navy.mil/bupers-npc/Documents/PII_Data_Breach_FAQ.pdf
3. Morgan, S.: 2017 cybercrime report. Cybersecurity Ventures (2017)
4. Wiederhold, B.K.: The role of psychology in enhancing cybersecurity. Cyberpsychology Behav. Soc. Netw. **17**, 131–132 (2014)
5. Suresh, P., Daniel, J.V., Parthasarathy, V., Aswathy, R.H.: A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In: 2014 International Conference on Science Engineering and Management Research (ICSEMR), pp. 1–8 (2014). https://doi.org/10.1109/ICSEMR.2014.7043637
6. Covington, H.: Smart homes: IoT security and ethical concerns. In: Proceedings for the Northeast Region Decision Sciences Institute (NEDSI), pp. 531–547 (2019)
7. Zheng, S., Apthorpe, N., Chetty, M., Feamster, N.: User perceptions of smart home IoT privacy. In: Proceedings of the ACM on Human-Computer Interaction (2018). https://doi.org/10.1145/3274469
8. Breitinger, F., Tully-Doyle, R., Hassenfeldt, C.: A survey on smartphone user's security choices, awareness and education. Comput. Secur. **88** (2020). https://doi-org.portal.lib.fit.edu. https://doi.org/10.1016/j.cose.2019.101647
9. Choi, H., Park, J., Jung, Y.: The role of privacy fatigue in online privacy behavior. Comput. Hum. Behav. **81**, 42–51 (2018). https://doi.org/10.1016/j.chb.2017.12.001
10. Pienta, D., Sun, H., Thatcher, J.: Habitual and misplaced trust: the role of the dark side of trust between individual users and cybersecurity systems. In: 2016 International Conference on Information Systems (2016)
11. Mittal, S.: Understanding the human dimension of cyber security. Indian J. Criminol. Criminalistics **34**(1), 141–152 (2017)
12. Rhee, H., Ryu, Y., Kim, C.: Unrealistic optimism on information security management. Comput. Secur. **31**(2), 221–232 (2012)
13. Pfleeger, S.L., Caputo, D.D.: Leveraging behavioral science to mitigate cybersecurity risk. Comput. Secur. **31**(4), 597–611 (2012)
14. Coovert, M.D., Dreibelbis, R., Borum, R.: Factors influencing the human-technology interface for effective cyber security performance. In: Zaccaro, S.J., Dalal, R.S., Tetrick, L.E., Steinke, J.A. (eds.) Psychosocial Dynamics of Cyber Security, pp. 267–290. Routledge (2016)

15. Albert, L.J., Rodan, S., Aggarwal, N., Hill, T.R.: Gender and generational differences in consumers' perceptions of internet of things (IoT) devices. E-J. Soc. Behav. Res. Bus. **10**(3), 41–53 (2019)
16. Zaccaro, S.J., Dalal, R.S., Tetrick, L.E., Steinke, J.A. (eds.): Psychosocial Dynamics of Cyber Security. Routledge, Milton Park (2016)
17. Burns, A., Roberts, T., Posey, C., Bennett, R., Courtney, J.: Assessing the role of security education, training, and awareness on 'insiders' security-related behavior: an expectancy theory approach. In: 2015 48th Hawaii International Conference on System Sciences (2015)
18. Hoffman, R.R., Lee, J.D., Woods, D.D., Shadbolt, N., Miller, J., Bradshaw, J.M.: The dynamics of trust in cyberdomains. IEEE Intell. Syst. **24**(6), 5–11 (2009)
19. Lee, J.D., See, K.A.: Trust in automation: designing for appropriate reliance. Hum. Factors **46**(1), 50–80 (2004). https://doi.org/10.1518/hfes.46.1.50_30392
20. Conti, G., Ahamad, M., Stasko, J.: Attacking information visualization system usability overloading and deceiving the human. In: Proceedings SOUPS' 2005 (2005)
21. AlHogail, A.: Improving IoT technology adoption through improving consumer trust. Technologies **6**(3), 64 (2018). https://doi.org/10.3390/technologies6030064
22. Jang, Y., Chang, S., Tsai, Y.: Smartphone security: understanding smartphone 'users' trust in information security management. Secur. Commun. Netw. **7**, 1313–1321 (2014)
23. Daubert, J., Wiesmaier, A., Kikiras, P.: A view on privacy & trust in IoT. In: 2015 IEEE International Conference on Communication Workshop, ICCW 2015, pp. 2665–2670 (2015). https://doi.org/10.1109/ICCW.2015.7247581
24. Lee, M., Lee, J.: The impact of information security failure on customer behaviors: a study on a large-scale hacking incident on internet. Inf. Syst. Front. **14**(2), 375–393 (2010)
25. Furman, S., Theofanos, M., Choong, Y., Stanton, B.: Basing cybersecurity training on user perceptions. IEEE Secur. Priv. **10**(2), 40–49 (2012)
26. Ben-Asher, N., Gonzalez, C.: Effects of cyber security knowledge on attack detection. Comput. Hum. Behav. **48**, 51–61 (2015). https://doi.org/10.1016/j.chb.2015.01.039
27. Grazioli, S.: Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the Internet. Group Decis. Negot. **13**, 149–172 (2004)
28. Proctor, R.W., Chen, J.: The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. Hum. Factors **57**(5), 721–727 (2015)
29. Legg, P.A.: Enhancing cyber situation awareness for Non-Expert Users using visual analytics. In: 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (2016)
30. Hirshfield, L., et al.: The role of the device users' suspicion in the detection of cyber attacks. Int. J. Cyber Warfare Terrorism **5**(3), 28–44 (2015)
31. Mahoney, S., Rothe, E., Steinke, K., Pfautz, J., Wu, C., Farry, M.: A cognitive task analysis for cyber situational awareness. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 54, no. 4 (2010)
32. Huigang, L., Yaijong, X.: Understanding security behaviors in personal computer usage: a threat avoidance perspective. J. Assoc. Inf. Syst. **11**(7), 394–413 (2010)
33. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. Science **347**(6221), 509–514 (2015)
34. Brough, A.R., Martin, K.D.: Critical roles of knowledge and motivation in privacy research. Curr. Opinion Psychol. **31**, 11–15 (2020). https://doi-org.portal.lib.fit.edu. https://doi.org/10.1016/j.copsyc.2019.06.021
35. Kelley, T., Bertenthal, B.: Real-world decision making: logging into vs. insecure website. In: USEC 2016 (2016)
36. Rosoff, H., Cui, J., John, R.: Heuristics and biases in cyber security dilemmas. Environ. Syst. Decis. **33**(4), 517–529 (2013)

37. Liang, H., Xue, Y.: Understanding security behaviors in personal computer usage: a threat avoidance perspective. J. Assoc. Inf. Syst. **11**(7), 394 (2010)
38. Sharma, K.: Impact of framing and priming on 'users' behavior in cybersecurity. Masters thesis (2017)
39. Lee, H., Kobsa, A.: Understanding user privacy in Internet of Things environments. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), pp. 407–412 (2016). https://doi.org/10.1109/wf-iot.2016.7845392
40. Jia, Y.J., et al.: ContexloT: towards providing contextual integrity to appified IoT platforms. In: NDSS, vol. 2, no. 2, p. 2 (2017)
41. Emami-Naeini, P., Agarwal, Y., Faith Cranor, L., Hibshi, H.: Ask the experts: what should be on an IoT privacy and security label? In: 2020 IEEE Symposium on Security and Privacy (SP), pp. 447–464 (2020). https://doi-org.portal.lib.fit.edu. https://doi.org/10.1109/SP40000.2020.00043
42. Bowen, B.M., Devarajan, R., Stolfo, S.: Measuring the human factor of cyber security. In: 2011 IEEE International Conference Technologies for Homeland Security (HST), pp. 230–235. IEEE (2011)
43. Fagan, M., Fagan, M., Megas, K.N., Scarfone, K., Smith, M.: Foundational cybersecurity activities for IOT device manufacturers. US Department of Commerce, National Institute of Standards and Technology (2020)
44. Meneghello, F., Calore, M., Zucchetto, D., Polese, M., Zanella, A.: IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. **6**(5), 8182–8201 (2019). https://doi-org.portal.lib.fit.edu. https://doi.org/10.1109/JIOT.2019.2935189