Cybersecurity

REVIEW Open Access

Review and insight on the behavioral aspects of cybersecurity

Rachid Ait Maalem Lahcen[1*], Bruce Caulkins[2], Ram Mohapatra[1] and Manish Kumar[3]

Abstract

Stories of cyber attacks are becoming a routine in which cyber attackers show new levels of intention by sophisticated attacks on networks. Unfortunately, cybercriminals have figured out profitable business models and they take advantage of the online anonymity. A serious situation that needs to improve for networks' defenders. Therefore, a paradigm shift is essential to the effectiveness of current techniques and practices. Since the majority of cyber incidents are human enabled, this shift requires expanding research to underexplored areas such as behavioral aspects of cybersecurity. It is more vital to focus on social and behavioral issues to improve the current situation. This paper is an effort to provide a review of relevant theories and principles, and gives insights including an interdisciplinary framework that combines behavioral cybersecurity, human factors, and modeling and simulation.

Keywords: Cybersecurity, Behavioral aspects, Human factors, Crime theories

Introduction

Gary Warner delivered in March 1, 2014, a TEDX Birmingham presentation about our current approach to cybercrime. Warner, the Director of the Center for Information Assurance and Joint Forensics Research, at the University of Alabama, Birmingham, explained the challenges of protecting individuals and reporting cybercrimes. Benefits of making money and conducting low risk illegal acts drive cybercriminals. The Internet Security Threat Report (Symantec 2017) shows that the average ransom was $373 in 2014 and it was $294 in 2015. It jumped to $1077 in 2016, and we surmise that it is due to the upsurge value of Bitcoin. A digital currency preferred by ransomware criminals because they can accept it globally without having to reveal their identities. The same report shows that the number of detection of ransomware increased to 463,841, in 2016; and more than 7.1 billion identities have been compromised in cyber attacks in the last 8 years. Malware attacks are on the rise, for instance, the recurrence of disk wiping malware "Shamoon" in the Middle East, and cyber attacks against Ukrainian targets involving the KillDisk Trojan. To show a historical damage that such malware can do, we give the example of the Ukranian power grid that suffered a cyber attack in December 2015. It caused an outage of around 225,000 customers. A modified KillDisk was used to delete the master boot record and logs of targeted systems' organizations; consequently, it was used in stage two to amplify attacks by wiping off workstations, servers, and a Human Machine Interface card inside of a Remote Terminal Unit. Trojan Horse viruses are considered the third wave of malware that spreads across the Internet via malicious websites and emails (Donaldson et al. 2015). There is no doubt that breaches of data are one of the most damaging cyber attacks (Xu et al. 2018). Figure 1 depicts three main cyber targets, or their combination based on the work discussed in Donaldson et al. (2015). They are usually referred to as CIA triad:

- Confidentiality threat (Data Theft) that can target databases, backups, application servers, and system administrators.
- Integrity threat (Alter Data) includes hijacking, changing financial data, stealing large amounts of

*Correspondence: rachid@ucf.edu
[1]University of Central Florida, Mathematics Department, Orlando, FL 32816, USA
Full list of author information is available at the end of the article

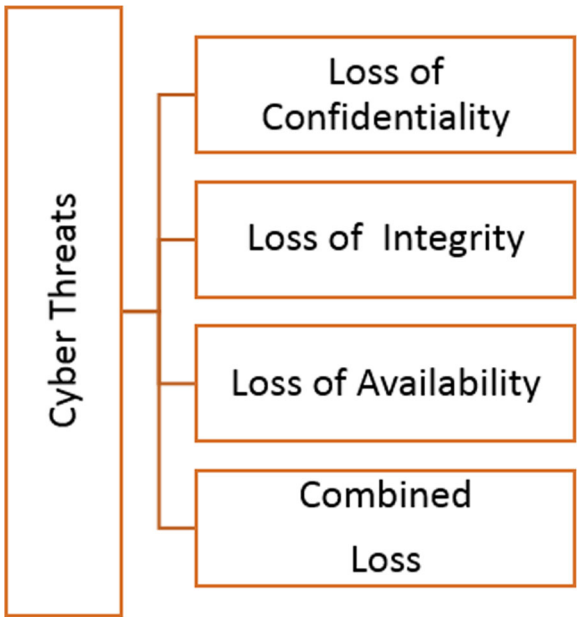

Fig. 1 Losses caused by cyber threats, modified based on Donaldson et al. (2015)

money, reroute direct deposit, and damage of organization image.

- Availability attacks (Denial Access) can be Distributed Denial of Service (DDoS), targeted denial of service, and physical destruction.

Attackers will try to penetrate all levels of security defense system after they access the first level in the network. Therefore, the defender should be more motivated to analyze security at all levels using tools to find out vulnerabilities before the attackers do (Lahcen et al. 2018). The 2018 Black Report pays particular attention to the period it takes intruders to hack organization's cyber system, both by stages of the breach and by industry. The clear majority of respondents say that they can gain access to an organization's system, to map and detect valuable data, to compromise it within 15 hours. Now, most industry reports say the average gap between a breach and its discovery is between 200 and 300 days (Pogue 2018).

It is clear that cyber offenders or criminals still have an advantage over cyber defenders. Therefore, what are the deficiencies in current research and what areas need immediate attention or improvement? Thomas Holt at Michigan State University's School of Criminal Justice argues that it is essential to situate a cybercrime threat in a multidisciplinary context (Holt 2016). Hence, based on literature review described in "(Related work") section, we believe that the behavioral side of cybersecurity needs more research and can improve faster if it is integrated with human factors, and benefit from sophisticated modeling and simulation techniques. Our study emphasizes two necessary points:

(1) Interdisciplinary approach to cybersecurity is essential and it should be defined based on cyberspace understanding. We adopt a definition by the International Organization for Standardization of cyberspace, *"the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form"* (Apvera 2018). This definition presents the cyberspace as a complex environment and initiates the interactions with people. Consequently, people's biases and behaviors influence the interactions with software and technology, which affect the cyberspace. We believe that advancing this interdisciplinary research could bring more relevance and increase of cybercrimes' manuscripts in top-tier journals. It is noticed that a low number of cyber-dependent crime manuscripts is due to a low number of criminologists who study cybercrime (Payne and Hadzhidimova 2018). Thus, we address several behavioral and crime theories. Based on the proposed interdisciplinary approach, cyber teams have to include individuals with different backgrounds ranging from IT, criminology, psychology, and human factors.

(2) Enterprises must account for possibility of vulnerabilities including human error in the design of systems. Avoiding a vulnerability is a much better option than trying to patch it, or spend resources in guarding it. This may sound as a trivial proposition yet, in reality, many defenders and users often deal with security as a secondary task when their primary function is not security. The authors in Pfleeger and Caputo (2012) stated that security is barely the primary task of those who use the information infrastructure. Also, system developers focus on the user's needs before integrating security into an architecture design. Afterwards, they add security tools that are easy to incorporate or meet some other system requirements. This is our rationale behind making modeling and simulation an essential component. The stakeholders such as users, managers, and developers, should be involved in building those models, and determine simulations that evaluate cognitive loads and response times to threats. Stakeholders can also use simulation to exercise real life scenarios of social engineering attacks. Furthermore, accounting for vulnerabilities may be affected by the budget. Enterprises keep cybersecurity's budget to a minimum. A report by Friedman and Gokhale (2019) found that financial institutions' on the average spending on cybersecurity is 10% of their IT spending or an average of 0.3% of revenue. Recently, some companies are spending more on cyber defense but in areas that may not maximize security. The report of Blackborrow and Christakis (2019) found that organizations are spending more on security but not wisely. This so called reactive

security spending and results in widespread inefficiency. By all means, this status increases the complexity of the security problem. Therefore, the perceptions of various industries about their cybersecurity needs vary, in most cases, they lack.

Related work

We conducted a comprehensive literature review using different criteria to capture both a historical stand point and the latest findings. We started the search of theories, human factors, and decision making strategies from 1980. It is important to acknowledge their historical contributions and explore how they can be applied to cybercrimes. We started the search of cybercrime reports from 2014 to understand cybercrime trends and magnitudes. The search of other subjects such as insider threat, hacking, information security, cyber programs, etc. is from the past decade. Some of the search commands: (cybersecurity AND human factors), (cybersecurity AND behavioral aspects), (cybersecurity AND modeling and simulation), (interdisciplinary approach and cybersecurity), (cybersecurity AND crime theories). Some of the databases that were searched are EBSCO, IEEE Xplore, JSTOR, Science Direct, and Google Scholar. It is worthwhile to note that several search results that include interdisciplinary cybersecurity awareness are about educational undergraduate students. This explains the urgency in educating future cyber professionals who will work in interdisciplinary cyber teams. We observed in recent conferences that few speakers debate whether there is talent's shortage or the problem is inadequate use of available tools. Nevertheless, our view is that the problem could be both. The two points mentioned in introduction (interdisciplinary approach and vulnerability in design) are used as criterion to decide related articles cited here.

It is acknowledged that human as the end user can be a critical backdoor into the network (Ahram and Karwowski 2019). The research done by Addae et al. () used behavioral science approach to determine the factors shaping cybersecurity behavioral decisions of users. The results suggest that security perceptions and general external factors affect individual cybersecurity adoptive behavior, and those factors are regulated by users traits (gender, age) and working environment. The authors in Maimon and Louderback (2019) conducted an interdisciplinary review reiterating that several criminological theories provide important frameworks that guide empirical investigations of different junctures within the cyber-dependent crime ecosystem. Also, they found that more research is needed and suspect that criminologists may not still bring cybercrime scholarship to the forefront of the criminological area. The authors in Payne and Hadzhidimova (2018) found that the most popular criminological explanations of cyber crime include learning theory, self-control theory, neutralization theory, and routine activities theory. In general, their finding reinforce the fact that integration of cybersecurity into criminal justice is not fast, probably because a few criminologists study cybercrimes. The work in Pfleeger and Caputo (2012) addresses the importance of involving human behavior when designing and building cyber technology. They presented two topics of behavioral aspects: (1) cognitive load that can contribute to inattentional blindness that prevents a team member to notice unexpected events when focusing on a primary task, and (2) biases that could help security designers and developers to anticipate perceptions and account for them in the designs. We will articulate more related work in the components' sections of the proposed framework.

In summary, research has been consistent in acknowledging that behavioral aspects are still underexplored and the focus is more on the technology aspect. One of the challenges is the complexity of the models when addressing different theories. Our aim is to provide insights on current issues, for example, classifying insider threat under human error makes insider issue a design requirement. This insight makes our approach significant because it opens channels to use the best human factors practices found in healthcare, aviation and the chemical industry. It reinforces the idea of insider as a design requirement (prevention).

The rest of the paper proceeds as follows: "(Interdisciplinary framework)" section proposes the Interdisciplinary Framework, "(Behavioral cybersecurity)" section explains Behavioral Cybersecurity, "(Human factors)" section Human Factors is discussed, "(Modeling and simulation)" section deals with Modeling and Simulation component, and we mention Conclusion and Future Work in "(Conclusion and future work)" section.

Interdisciplinary framework

Because all partial solutions (Firewall, IDS/IPS, netflow, proxy, mail gateway, etc.) do not add up to a complete solution and the offenders still have the most latitude for variation at the network level (Kemmerer 2016), it is necessary to invest in interdisciplinary frameworks. In this section, we propose an interdisciplinary framework that enables understanding of interconnectivity of relations and should serve as a background to improve research and maturity of security programs. We focus on three areas based on the work of Caulkins (2017), depicted in a Venn diagram in Fig. 2:

- Behavioral cybersecurity is the main focus of our study. We address profiles and methods of hackers, insiders, behavioral, social, and crime theories. Weapons of influence that are largely used by the

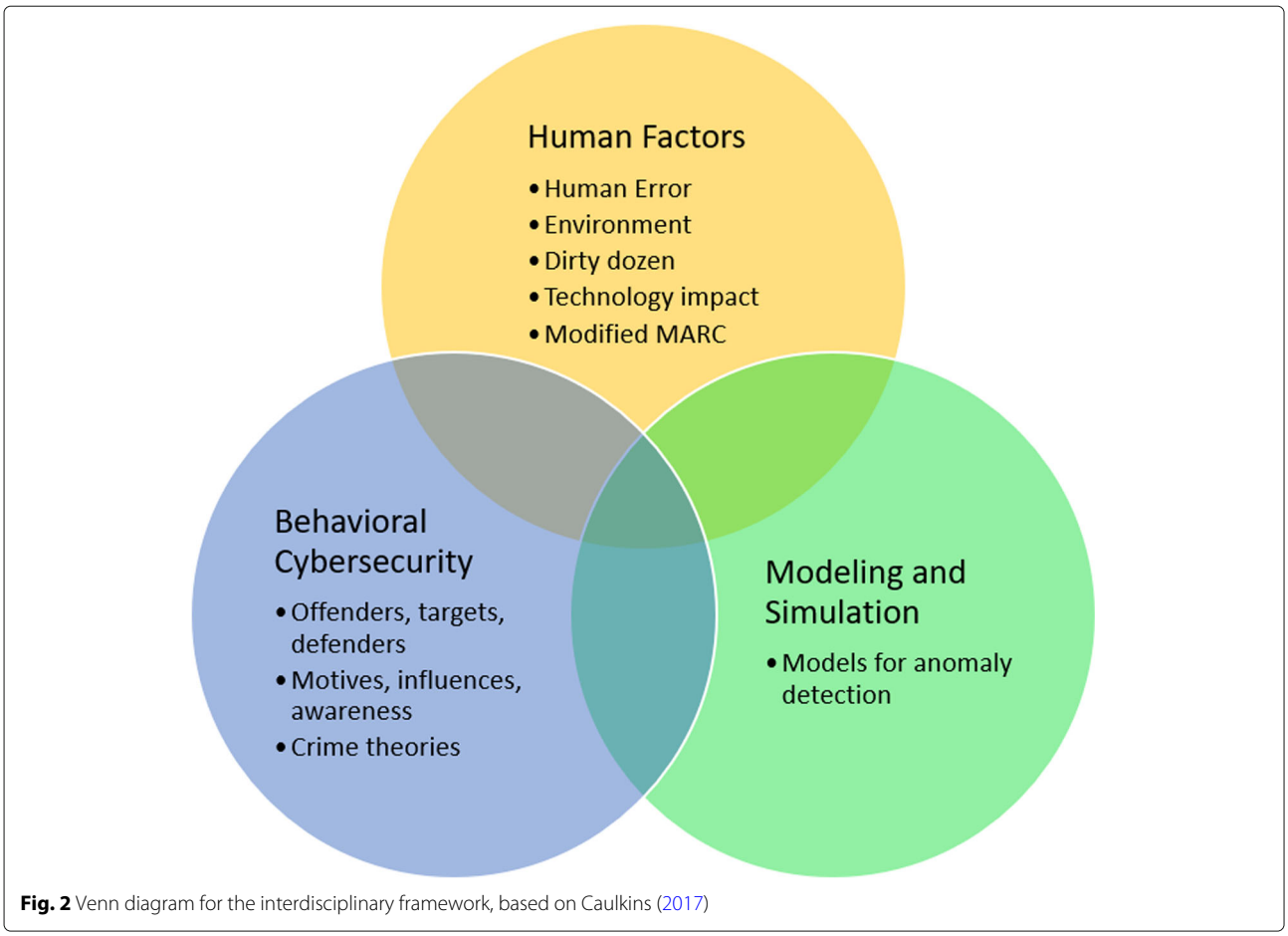

Fig. 2 Venn diagram for the interdisciplinary framework, based on Caulkins (2017)

offenders and mostly ignored by the defenders will also be identified.

- Integrate human factors discipline with behavioral cybersecurity. We give an insight on human factors that trigger human error. If we consider the insider problem as a human error, we can mitigate the risks by improving the environment, and plan it in the design requirement of future systems. The assumption is that system design enables insider risk because of the already existing vulnerabilities or conditions. The National Institute of Standards and Technology (NIST) recommends that the best method to involve everybody is to motivate everyone using incentives within the cyber economy (Addae et al.). Hence, it is worth integrating human factors to improve working environment, mitigate risks, and make the system's probability of failure lower.
- Using Modeling and simulation for researching, developing and implementing new techniques, tools and strategies is our recommendation. Modeling and simulation are useful for many reasons and can be extended to situations such as when real experimentation is not convenient, or dangerous, or not cost effective (Niazi 2019). Simulation can test applications of human factors, for example, whether the real process may cause a cognitive load that will inhibit the security end-user to miss important information or threats. We review modeling and simulation in literature, and we provide insight in that section based on our focus on human error.

There is no doubt that behavioral cybersecurity is important, and it needs more research. We emphasize the three components of this proposed interdisciplinary framework because human performance is not affected solely by training, which is the main focus of cyber defenders. It is affected by the system itself, people's biases, environment workload, administrative management, communication practices, human-computer interfaces, existing distractions, etc. Many factors still contribute to the slow research and implementation of interdisciplinary approaches. Unfortunately, many enterprises underestimate the severity of cyber incidents, or they pass the blame to one person when an incident occurs. For instance, Federal Trade Commission website reports that in September of 2017, Equifax announced a data breach

that exposed the personal information of 147 million people and Equifax has agreed to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. The settlement includes up to $425 million to help people affected by the data breach (FTC 2019). Yet, the settlement does little to those who file claims ($125 one time payout or credit monitoring for a number of years). Individuals cannot opt out of Equifax being their data steward which makes many persons nervous. Most of the online reports state that Equifax did not update a known vulnerability in the Apache Struts web-application software. Nevertheless, Equifax's Chief Executive told members of Congress on October 3, 2017, that the massive breach happened because of a mistake by a single employee.

Behavioral cybersecurity

Cybercrime offenders: hackers

Hackers' techniques

A hacker is a human that uses technical intellect to get unauthorized access to data to modify it, delete it or sell it by any means (Pal and Anand 2018). Although a hacker may follow various steps to execute a successful attack, a usual network intrusion involves reconnaissance to collect information, scanning to set up a vulnerability profile, gaining access or penetrating an access point or level, maintaining access by accessing other levels or planting programs to keep access, and covering tracks to hide the trails (Lahcen et al. 2018). The authors in Shetty et al. (2018) have surveyed hacking techniques:

- The dictionary attack to crack vulnerable passwords. This is like brute force to defeat security. It takes advantage of users not being able to remember difficult passwords or the ones that do not make any sense so they use relevant or easy passwords. Often hackers find those users who adopt weak passwords such as *123456* or *password*. Currently, companies are enhancing passwords' syntax and mandate specific changing procedures. Yet, users still use same passwords across websites.
- Structured Query Language (SQL) injection of harmful code to modify the SQL query structure. It manipulates website's database.
- Cross Site Scripting (XSS) is an attack vector that injects malicious scripts into victim's webpages.
- Phishing is a social engineering attack in which a phisher fools the user to reveal secret information. Some examples are discussed in the weapons of influence "(Weapons of influence)" section.
- Wireless hacking due to a weakness of some networks. Those networks do not even change vendor access point and default passwords. A Wi-Fi network can be hacked in wardriving if it has a vulnerable access point. A hacker uses port scanning and enumeration.
- The Keylogger is a software that runs in the background and captures the user's key strokes. With it, hackers can record credentials.

Literature review discusses several hacker profiles. They have various levels of education, they hold many certificates, and they are either self-employed or work for organizations. Hackers can be script kiddies who are the new and novice. Their intent is curiosity or notoriety. Cyber-punks such as virus writers, they have medium skill level and their intent could be notoriety with some financial gain. Insiders or previously called internals can be driven by many motives such as revenge or financial benefits. Insider's skills are usually high. The intent of petty thieves, virus writers, grey hat or old guard hackers is curiosity or notoriety, but their skill levels are high. The motive of professional criminals or black hat hackers can be financial and they hold very high capabilities. The motive of information warriors who are cyber mercenaries is mainly espionage, and they are placed under Nation State groups. Political activist or hacktivists are ideologically motivated, and they manage to include members who posses high level of skills (Hald and Pedersen 2012).

Insight on hackers' techniques

It is important to understand that hacking techniques and hackers' motives in order to anticipate hackers' moves. All hackers do not think the same way as defenders or in a linear manner. Consequently, defenders need to be interdisciplinary in order to take in account various techniques and combat. We support this assumption with one of the real stories of exploitation by hackers that Mitnick and Simon discussed in Mitnick and Simon (2005): Hackers changed firmware in the slot machines after hiring an insider or a casino employee. Their motive was money and their stimulus was that the programmers of the machines were human, hence, they most likely had a backdoor flaw in the programs. One hacker checked the patent office for a code since it was a requirement to include it for patent filing. The analysis of the code gave away its secret. The pseudo random generator in the machines was 32-bit random number generator and cracking it was trivial. The designers of the machine did not want real random number generation so they have some control over the odds and the game. The hackers in this story were programmers and their thinking was simple enough to find a sequence of instructions to reach their goal. At that time, casinos spend money in security guards and not in consulting with security sources. One hacker said that he did not even feel remorse because they are stealing from casinos who in return steal from people.

Therefore, we present some of the questions that should be answered periodically to predict hacker's next move: Is the attack surface defined? Attack surface involves the sum of all the attack vectors where a hacker can attempt to exploit a vulnerability. What is a critical or a most vulnerable or a most damaging asset if exploited? How are the access points protected? How can hackers access crown jewels? An example of crown jewels is the most valued data. Where crown jewels are located (servers, network, backups, etc.)? Are the inventories of authorized and unauthorized devices known? Are operating systems well configured and updated? Is a system in place to identify stolen credentials or compromised user accounts? What type of malware defenses are used? How effective are training or awareness programs? Are employees aware of social media risks? How is the situation of employees in the working environment? How effective and robust are the used intrusion detection systems? Is the reporting system of a potential threat or breach clear? Is there a plan to combat insider threat? We should highlight that many companies see that emphasizing prevention increases cost and reduces productivity. The increase of cost is due to interaction with security control and incident response. Lost of productivity is due to granting permissions or re-certifying credentials or users' accounts (Donaldson et al. 2015). We think that they should analyze costs of different options: prevention driven program, incident response driven program, or a hybrid option.

Cybercrime offenders: insiders

Insiders' threat

An insider is a hacker from inside the organization; hence, this insider has access rights and is behind the firewalls. Insider threat is broadly recognized as an issue of highest importance for cybersecurity management (Theoharidou et al. 2005). Several surveys have considered varying aspects of cybersecurity: The SANS Healthcare Cyber Security Survey (Filkins 2014), The Insider Threat Spotlight 2015 Report (Partners 2015), Department for Business Innovation and Skills, 2014 Information Security Breaches Survey (Willetts 2014), etc. The Insider Threat Spotlight 2015 Report stated that companies were more concerned by inadvertent insider threat data leak breaches than malicious data breaches (Partners 2015). However, their concerns do not surely translate to effective changes in cyber programs. According to the SANS Healthcare Cyber Security Survey, 51% considered careless insider as a main threat when it comes to human behavior as an aspect of cybersecurity (Filkins 2014). Many theories can be applied to understand insider risk and motives, and can be applied to behavioral models. Often policies and risk management guidance are geared towards rational cyber-actors while rationalities of users and defenders represent cyber-system vulnerabilities (Fineberg 2014). Irrational behavior can be dangerous and unpredictable, it builds on frustration or fury, and it can be motivated by lack of job satisfaction. Often cyber defenders do not verify irrational behaviors. The authors in Stanton et al. (2005) have concluded that end users' behaviors that occur in organizations could be sited within these behavioral groups leading to intentional damage, harmful misuse, unsafe tinkering, naive mistakes, mindful assurance, simple hygiene, and using intentionality and technical expertise as criteria. Myers et al. (2009) have added automated insiders such as bots to unauthorized use of privileges. The authors in Azaria et al. (2014) have divided related works into six categories including psychological and social theories, anomaly based approaches, honeypot based approaches, graph based approaches, game theory approaches, and motivating studies. The authors in Greitzer and Hohimer (2011) have described a predictive modeling framework CHAMPION that integrates various data from cyber domain, to analyze psychological, and motivational factors that concern malicious exploitation by the insider. The ontologies in CHAMPION represent knowledge in the specialized domain to reason about data. The reifiers are used for the feeding of the ontologies' primitive data types. The memory is used to store both the primitive data and the facts concluded by the reasoning system. In addition, the Auto-associative Memory Columns (AMCs) or reasoning components stacked in a hierarchy and are used for data's interpretation and are used to infer new statements. The authors in Cappelli et al. (2014) have discussed the Management and Education of the Risk of Insider Threat (MERIT) models that can be implemented to communicate insider's threat. They identified and validated seven observations after analyzing several insider IT sabotage cases. Those observations are insiders had personal predispositions, were disgruntled employees, were among those who suffered stressful events (sanctions), had behavioral precursors (drug use, aggressive, etc.), created unknown channels to attack after termination, or lacked physical and electronic access (exploited insufficient access). A limitation in dealing with insider threat research is the scarcity of data (Stolfo et al. 2008).

Insight on insiders' threat

We think that there is a confusion in classifying insider threat, and many organizations may not even have policies or controls addressing it. Another issue of concern is that organizations do not want to admit of having insider incidents, they choose firing the intruder, and protect their reputation. Our insight considers the insider as a human error to be addressed at the top level of any developed taxonomy. So we group all user errors and the insider into human error, summarized in Fig. 3.

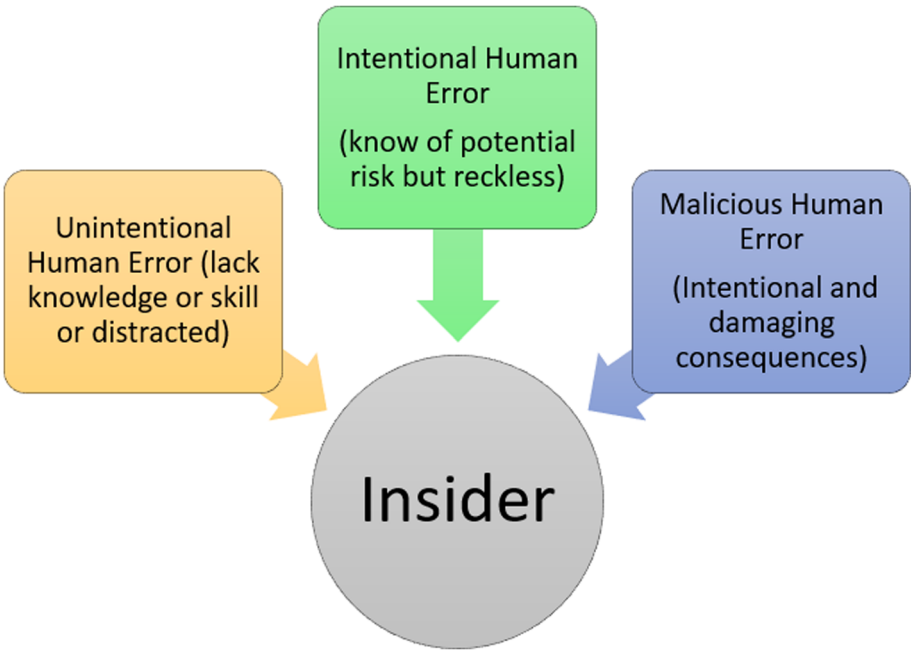

Fig. 3 Proposed UIM human error as insider-anomaly concept

For this purpose, we adopt a definition of human error mentioned by the Center for Chemical Process Safety (AIChE) in Rodriguez et al. (2017):

> *"Human error is any human action that exceeds some control limit as defined by the operating system."*

We believe our insight is important because it simplifies this confusing issue to Unintentional - Intentional - Malicious or (UIM) instead of several categories. Moreover, it also allows to adopt lessons learned from industries that have a long history in applying human factors, and built mature programs. Besides, this insight allows to comprehend that failures happen at the management level, at the design level, or at the technical expert levels of the company; and they result in human error or failure (Embrey et al. 1994). Obviously, UIM category is decided by its consequence or intent:

- Unintentional human error can be due to lack of organized knowledge or operating skills. This error may remain unintentional or transforms to another type (intentional or malicious).
- Intentional human error is caused by a user who knows of risky behavior but acts on it, or misuses assets. The wrong action may not necessarily bring a sudden harm to the organization, but it may still breach of existing laws or privacy.
- Malicious human error is the worst error as it is intentional with specific and damaging consequences in mind.

This classification does not downgrade the insider threat. It brings it upfront in the system design, similar to human errors that are usually considered at the beginning of designs. It is easier to blame the human during a cyber incident instead of blaming the cyber program or the design of the systems. In fact, the system design that did not consider the human factor is also to blame. Often the user does not see the security policies in the same way as those who wrote them or want them implemented. It is imperative to realize that users often exhibit their own biases in decision making (Fineberg 2014). This grouping can also be implemented in user's training and help make awareness easier. We give few examples:

- Unintentional error can happen from using a public Wi-Fi to access important accounts and not knowing about the risk. Or, while working, employee visits unsafe websites linked from social media.
- Intentional error can occur if a user writes a password on a sticky note, leaves it near computer or in desk's drawer and hoping no one else uses it.
- Malicious error can occur with employee stealing confidential data (exfiltration).

As mentioned, a user error can change from a UIM category to another. For example, a user should not activate links or download attachments in emails without a verification. If a new employee is not aware of social engineering tactics, the employee may click on those links (unintentional). This employee's clicking rate on those link

should decrease with training, if not, employee's action becomes intentional. Similarly, honeypots or decoys can be used to learn about user's normal or deviant activities. Some companies implement programs to simulate real life scenarios such as phishing exercises. We suggest that they are transparent with employees about the use of phishing simulators or other awareness programs. The goal should be to improve the culture of cyber awareness and not adding stress to workloads.

We previously described the cyber targets (Fig. 1), and mentioned that the defender should consider them in the system design that usually inspects requirements. (1) To define confidentiality requirement, the organization should characterize data and its location. The user should differentiate whether one is dealing with public, confidential, or limited data. Compromising data may happen on the computer of the user, in transit across an open or close network, on a front-end server, or in storage (Maiwald and Sieglein 2002). The user's access to confidential data should be updated if data classification changes or a user's status changes. Understanding that insider threat as a human error or anomaly within requirements of data security helps us to set up policies on credentials of persons who have access to confidential data. For example, to implement Just In Time (JIT) credentials. JIT helps to avoid permanent administrator (admin) privileges. It should in return mitigate the risk to steal admin credentials, and prevent admin data access outside the times in which there is no need to access confidential data. (2) Integrity is a system requirement. Data may be modified by the user, in transit across a closed or open network, a front-end server, or in storage (Maiwald and Sieglein 2002). Considering user's alteration of a system policy as an error helps to best treat integrity like confidentiality. Hence, the user's access and impact on system integrity need to be examined. (3) Availability is also a system requirement. Because system's components can be interconnected, a user who affects the availability of a part of a system can affect other parts. User's error to make a system unavailable can easily happen intentionally or unintentionally if the system design did not identify failure points.

Behavior, social and crime theories

Computer scientists, security researchers, psychologists, social scientists have attempted to explain the behavior of users in relation to cybersecurity. There is insufficient knowledge about the behavior of the user toward information technologies that defend systems and data from troubles such as malware, spyware, and interruptions (Dinev and Hu 2007). The authors in Greitzer and Hohimer (2011) have emphasized that the only way to be proactive in the cyber domain is to take behavioral or psycho-social data into account. At this point, we introduce theories that should help with such issues.

Theories: normative, planned behavior, social bond, and social cognition

There are questions about rationality when it comes to norms and the study of human cognition. The norms are essential to the study of informal argumentation, studies of judgment, and decision-making. Normative theories are studied in procedural theories forms and epistemic theories forms. It is difficult to resolve questions about suitable norms for a specific behavior without comprehending the origins of normativity (Corner and Hahn 2013). It is recognized that playing a matching game between a particular behavior and some prescriptive standard is not enough to understand the concept of normativity. Hence, Corner and Han attempted to answer what makes something normative? It seems that there is a continuing debate on this subject. Our modest understanding is that a rational human behavior happens when the behavior matches some criterion, and logic is used to evaluate arguments. Yet, logic has limitations and may not be appropriate to judge arguments' strength. Such limitations of logic encouraged the popularity to Bayesian probability as a calculating application for argument strength (Corner and Hahn 2013). Therefore, the authors make a good argument that the Bayesian is suitable for the normativity's requirements.

Another widely used theory is the Theory of Planned Behavior (TPB) depicted in Fig. 4. It uses a predictive model that indicates that subjective norms and attitudes influence behavioral intention. The latter influences actual behavior. The TPB postulates that people's behavioral intention is a good predictor of their real behavior. Another perception of behavior is the subjective norm. The ease or difficulty of performing behavior is the perceived behavioral control.

Generally, the greater is the attitude, subjective norm, and perceived behavioral control with respect to a behavior, the higher should be an individual's intention to demonstrates the behavior under consideration. The attitude is connected to beliefs (behavioral, normative and control). In addition, multiple authors structure social pressure as a cause to normative beliefs. Until now, insufficient research is done on subjective norms regarding cybersecurity. An area in which TPB can be useful in the study of insider threat; as TPB is used successfully in predicting several health behaviors like smoking and substance use. It will be useful to understand the roles of various behavioral factors and learn which ones will have the highest predictive value in order to integrate it in a preventive plan, or an intrusion detection system. Similar to the work of Pabian and Vandebosch that studied cyberbul-

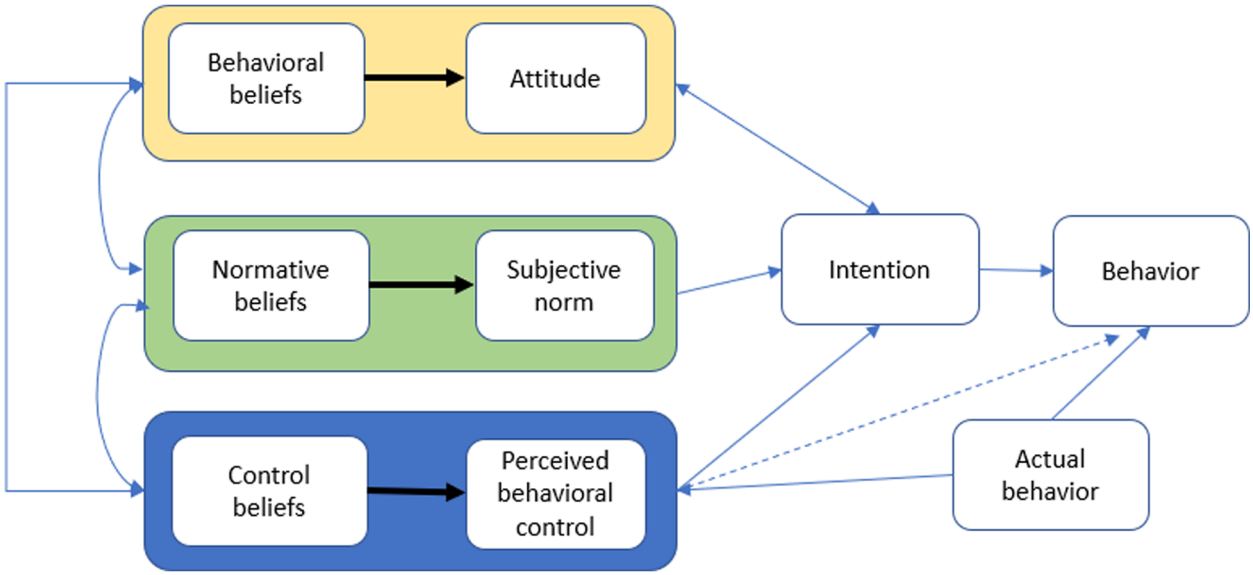

Fig. 4 Theory of Planned Behavior diagram, from Icek (2019)

lying using TPB; they found that cyberbullying intention is a predictor of self-reported cyberbullying behavior after six months (Pabian and Vandebosch 2013). The attitude is the primary direct predictor of intention followed by the subjective norm. The authors in Dinev and Hu (2007) have integrated TPB and Technology Acceptance Model (TAM) and found that technology awareness is a predictor to a user behavioral intention to use anti-virus or anti-spyware. Technology awareness had the strong influence on attitudes toward behavior and behavioral intention. They also found that awareness is highly correlated with both TPB and TAM beliefs, and recommended that for managers to create social advocacy groups and networks. Their role is to advocate for cybercrime awareness. The authors of Burns and Roberts (2013) have used TPB to predict online protective behaviors. Their findings indicate a significant relationship between a subjective norm and intention. It also emphasizes that external parties influence the intention of the user to engage in cyber protective behavior.

Social Cognition Theory (SCT) initiated as Social Learning Theory by Albert Bandura and became SCT in 1986. It postulates that cognitive factors are related to an environment and behavioral factors. Consequently, learning happens in a social context (Hardy et al. 1980) with reciprocal determinism. Figure 5 depicts SCT basic diagram based on Hardy et al. (1980). There is a reciprocal cause and effect between a person's behavior and both the social world and personal characteristics. Hence, criminal or deviant behavior is a learned behavior just like any other behavior. Social Bond Theory makes the assumption that weaker social bonds can increase the chance of a person to be involved in a crime.

The interesting part of SCT is that it tries to explain the maintenance of behavior, unlike other theories' concern of initiating a behavior. SCT can be applied to the cyber domain to investigate decision support and behavior. It can probably support a robust security framework that studies practice behaviors of self-users. For example, studying the impact of self-efficacy is a cornerstone of SCT, on decision and cyber behavior. Self-efficacy is not self-esteem and it is kind of self-evaluation which is significant in individual behavior (Hardy et al. 1980). Self-efficacy can influence the amount of effort, self-regulation, initiation of tasks, and handling of obstacles (Hardy et al. 1980). Also, ill-defined circumstances and performance requirements can bring inconsistencies to self-efficacy expectation and performance (Reardon 2011).

Theories: general deterrence, neutralization, self-control, and situational crime prevention

The authors of Theoharidou et al. (2005) have summarized criminology theories and security literature. It seems that all theories involve a motive and one theory is about the opportunity of a crime. Besides, General Deterrence Theory is based on a perpetrator committing a crime if the cost of sanction is less than the benefit of the crime. Hence, stiff punishment and awareness programs deter many potential perpetrators. Authors in Cheng et al. (2014) found that employees focus on the perceived benefits of personal internet use while, at the same time,

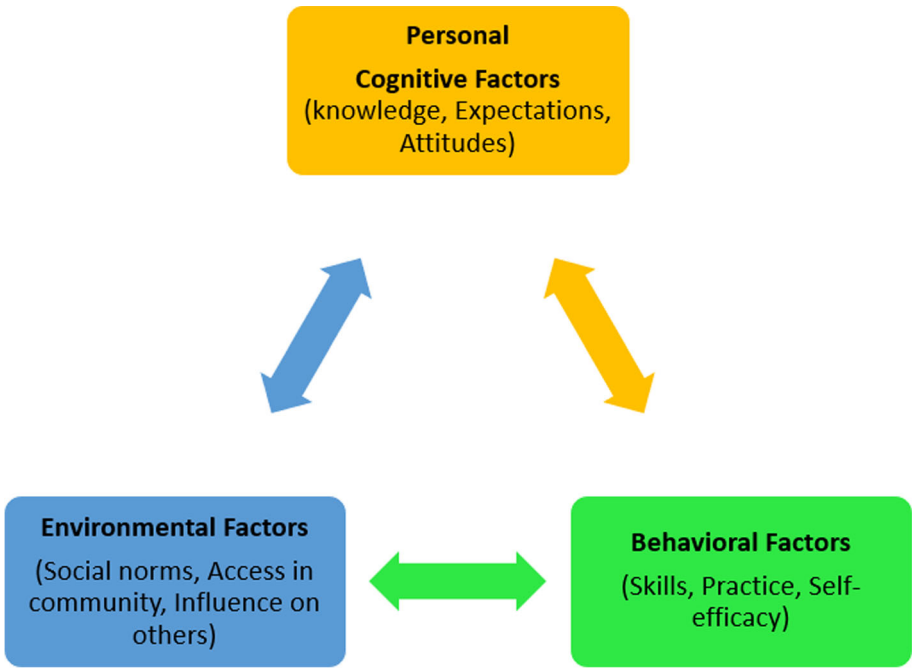

Fig. 5 Social Cognition Theory basic diagram

finding justification for their behavior and keep less attention to the expected punishment. They are less worried about severity of punishment, and more worried about the likelihood of being caught. Those users try to justify their deviant behavior as excusable. This is a topic of neutralization theory. Hence, employees could use neutralization techniques to justify risky security behaviors. Neutralization is an excellent predictor of employees' intention to violate information security policies (Siponen and Vance 2010). They see it as an indicator of a motivational state that exists just prior to committing an act. Self-control Theory postulates that criminal acts attract low self-control people as these acts provide pleasure to them. A low self-control individual prefers immediately gratifying activities that involve risky behaviors, and shows little empathy for others. Self-control theory's definition of crime is behaviors that provide momentary or immediate satisfactions and create negative consequences (Gottfredson 2017). This theory can be applied to cybercrime and may be integrated with other stated theories. The theory of Situational Crime Prevention (SCP) makes the hypothesis that a perpetrator must have an opportunity in addition to a motive. A motive without an apportunity will not yield to a crime. Hence, it is different because it looks at the opportunities and the formation of motives to excite crimes (Theoharidou et al. 2005). SCP framework includes rational choice, opportunity structure, specificity, and twenty-five techniques to reduce crime found in Freilich et al. (). The latest studies discussed complex issues in working with SCP, for instance, the competency and the responsibility to prevent a crime. Consequently, reducing cybercrime spike will depend on involving many parties such as law enforcement, government agencies, security companies, etc.

Multi-criteria decision-making

We should include Multi-criteria decision-making (MCDM) with above theories because conflicting ideas may arise and decisions need to be made to have good programs or models. MCDM is crucial for several real life problems including cybersecurity. However, the discussion on the usability of decision theory against cyber threats is limited, which indicates the existence of a gap (Wilamowski et al. 2017). Often, challenges rise during the evaluation of alternatives in terms of a set of deciding measures. There is no doubt that decision making in this paper's context cannot be easily modeled because of dealing with human element and judgement. A wide range of mathematical methods of MCDM for evaluation and validation of alternatives exist, and embedded in, linear programming, integer programming, design of experiments, Bayesian networks (Wilamowski et al. 2017). MCDM usually involve three steps when using numerical analysis of the alternatives: (1) identify alternatives to criteria, (2) attach numerical measures to the criteria and impact

of alternatives, and (3) rank each alternative after processing numerical values (Triantaphyllou et al. 1997). The weighted sum model remains the simplest and the most widely used MCDM method. The authors of Triantaphyllou and Mann (1995) have used the analytical hierarchy of the process for decision making in engineering and found challenges. For instance, when some alternatives are similar or very close to each other, the decision-maker needs to be very careful. They suggest trying to consider additional decision making criteria to considerably discriminate among the alternatives. We can assume so far that decision making theories can easily give different answers to the same cybersecurity problem, yet they should be used as tools to back a decision as the authors of Triantaphyllou and Mann (1995) suggested. The authors of Wilamowski et al. (2017) have studied two theories in decision making: Analytical Hierarchy Process (AHP) and an Analytical Network Process (ANP). They determined that a generalized application benchmark framework could be employed to derive a Measure of Effectiveness (MOE) that relate to the overall operational success criteria (mission performance, safety, availability, and security). MOEs continuance are measured under specific environmental and operational conditions, from the users' viewpoint. The AHP is an appropriate option if a situation requires rapid and effective decisions due to imminent threat. The ANP is appropriate if the time constraints are less important, and more far-reaching factors should be considered while constructing a defensive strategy. Their findings can provide cybersecurity policy makers a way to quantify the judgments of their technical team regarding cybersecurity policy.

The authors of Kabassi and Virvou (2015) have added Human Plausible Reasoning Theory (HPR) that is a cognitive theory to MCDM and provides more reasoning to a user interface. HPR depends on analyzing people's answers to ordinary questions about the world. HPR theory assumes dynamic hierarchies to represent human knowledge. HPR defines parameters of certainty as a set of criteria that should be taken into account in order to select the best hypothesis. Nevertheless, HPR does not propose precise mathematical methods for combining these criteria. Indeed, MCDM compliments HPR and improves control in an intelligent user interface (Kabassi and Virvou 2015).

Weapons of influence

We owe the credit, for this section's title, to the first chapter title of Cialdini's book *"Influence - The Psychology of Persuasion"*. Unfortunately, social engineers use weapons to influence and manipulates persons to disclose sensitive information or granting unauthorized access. Cialdini identified six principles of influence that guide human behavior (Rodriguez et al. 2017): Reciprocity, scarcity, authority, consistency, liking and consensus. The authors in Haycock and Matthews (2016) have addressed them in their "Persuasive Advocacy" article. Based on their analysis, we give some examples in which social engineering can exploit and direct human actions with a view to understanding reason that motivates cybercrime:

- Liking can give a false sense of credibility. Hackers can use it to build rapport, or encourage certain behaviors by generating fake likes, and artificially increasing the number of followers on social media to give the impression that other people are supporting that behavior.
- Reciprocity is due to feeling of obligation to return favors. Hackers can offer free services or products and expect access or data in return.
- Social proof or consensus summarizes how a person follows other's lead. Hackers can use this type of validation to influence users and gain access to data. When people are not certain they may easily reply to other persons, especially peers.
- Persuasion by peers. Hackers can persuade insiders to steal data for a cause that a peer or a role model is promoting.
- Individuals who decree expertise or credentials try to harness the power of authority. Authority can bring phony claims and influence a user that is wary of job loss.
- Consistency comes from the need to appear or to remain consistent. Hackers can find out about consistent actions and use them to distract a user prior to an attack.
- Scarcity of resources makes a user vulnerable. It can influence a user to take an immediate action without thinking about consequences such as a data breach.

Researchers found that the effectiveness of each one of these principles is due to the victim's personality characters. Examples from Uebelacker and Quiel (2014) and Caulkins (2017) about Cialdini principles' work in social engineering: Agreeableness of a user has increased the vulnerability towards liking, authority, reciprocity, and social proof. Neuroticism indicates a user is less susceptible to most social engineering attacks. Conscientious user may not resist the principles of authority, reciprocity, and commitment and consistency, especially, when commitments are made public. Extraversion user may have greater vulnerability for the scarcity principle since the latter is considered as an excitement. Conscientiousness may decrease user's susceptibility to cyber attacks. Yet, conscientiousness has a higher tendency to follow through commitments which may make the person susceptible to continuation of social engineering tactics. Agreeableness of a user may have increased susceptibility to phishing,

Table 1 Cialdini, Gragg, and Stajano principles (Ferreira et al. 2015; Caulkins 2017)

Cialdini six principles of influence	Gragg seven psychological triggers	Stajano seven principles of scams
Authority	Authority	Social compliance
Social proof	Diffusion responsibility	Herd
Linking and similarity	Deceptive relationship	Deception
Commitment and consistency	Integrity and consistency	Dishonesty
Scarcity	Overloading	Time
Reciprocation	Reciprocation	Need and greed
	Strong affect	Distraction

and share passwords. Openness reduces social engineering vulnerability as more digitally literate users better detect social engineering attacks. Authors in Halevi et al. (2013) have found that women are more vulnerable to prize phishing attacks than men, and they found a high correlation between neurosis and responsiveness to phishing attacks. In addition to Cialdini's work, researchers like Gragg and Stajano discussed what triggers of influence and scams. Table 1 is based on the work of Ferreira et al. (2015) and Caulkins (2017), and it summarizes the principles of Cialdini, Gragg, and Stajano.

Those authors found that phishing emails use social engineering and depend on liking, deception, and similarity principles. Distraction is the second most commonly used principle. The combination of principles increase success of phishing attacks (Ferreira et al. 2015). The elaboration likelihood model of persuasion in Cacioppo and Petty (2001) suggests that there are central (involve high elaboration) and peripheral (involve low elaboration) routes to persuasion. A person who is faced with a persuasive message will run through it using either a low or high elaboration.

Insight on discussed theories and principles

Applying described theories to cyber domains should help to identify targets by understanding opportunities of a crime. This can be a subject of asset management and risk assessment. What are the crown jewels? And what are their vulnerabilities? Should a company decoy offenders or harden the targets? Who may be interested in hacking them? A hacker type and technique are to be identified. A much better than a current situation in which those questions are asked during an incident response. Those theories can also explain an initiation of deviant behavior, maintenance of a behavior, and a motive of a cybercrime. They consider social and environmental factors that could be missed when preparing a prevention program. Little research is done in this field. One example is research can explore those theories' use to develop simple models like Persona non Grata that identify adversaries who can be inside or outside security perimeters. Integrating different theories can further classify a deviant behavior as a misbehavior or a beginning of an imminent attack. It seems that creating a social advocacy group and cyber awareness can help improve users' intentions and attitudes. Strong social bonds are much better than weaker social bonds. We also discussed decision making and understanding alternatives and norms. Weapons of influence are used by intruders, and the defenders lack the research to use them to defend confidentiality, integrity, and availability. The paper of Faklaris (2018) has suggestions on using weapons of influence to support IT professionals. The Commonly used attack vectors by social engineers are phishing (by email), vishing (phone call), impersonation and smishing (text message).

Human factors

Relate human factors to cybersecurity

For the Human Factors, researchers can learn from the health and aviation industries since they have extensive work in this discipline. Human factors is the discipline that works to optimize the relationship between the humans and technology. We pick the Map-Assess-Recognize-Conclude (MARC) process shown in Fig. 6 and found in Parush et al. (2017) to address behavioral aspects and focus on human error.

Mapping the user and the environment requires asking a set of questions on their characteristics, roles, knowledge, skills, experience, tasks, responsibility, personality traits, access points and locations, human machine interface, etc. Assessment can analyze known factors, collect facts on user capabilities and limitations, and the working environment. While assessing, one can recognize the emerging factors that were not initially included in the mapping and can cause a human error. The two types of emergent factors are environmental (physical and human) and human (psychological, physical). For example, fatigue or distraction can contribute to unintentional mistake, and loss of vigilance can cause intentional mistakes. Fatigue, distraction and loss of vigilance could be emergent factors. Norman argues that humans will make errors in the best designed systems so the systems should be designed to minimize the effect of the error (Norman 1983). We agree with this view, as human errors are known to cause a variety of accidents in various industries and organizations. In aviation, twelve human errors or dirty dozen that lower people's ability of performance and safety, which could lead to maintenance errors are: lack of communication, complacency, lack of knowledge, distraction, lack of teamwork, fatigue, lack of resources, pressure, lack of assertiveness, stress, lack of awareness,

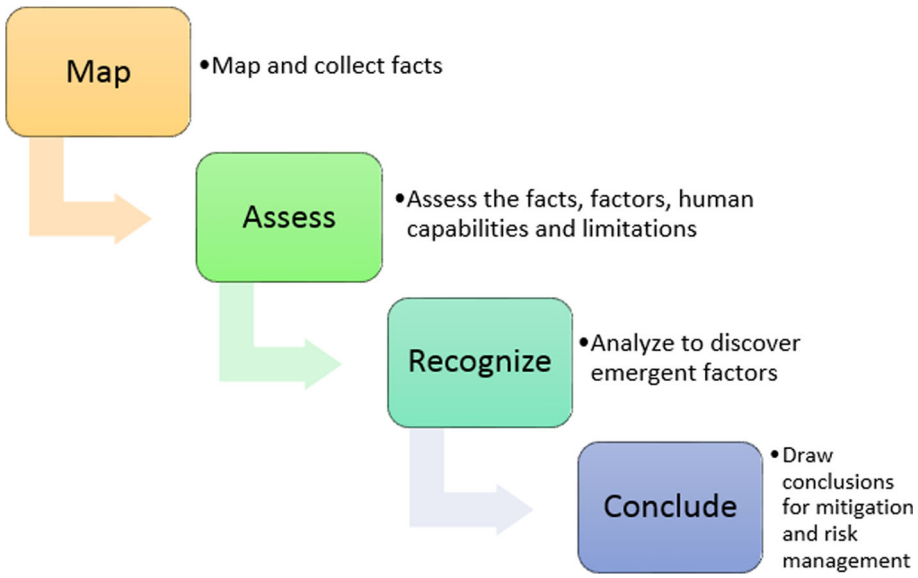

Fig. 6 Interpretation of MARC process, based on Parush et al. (2017)

and norms (Dupont 1997). We can easily relate those factors to cybersecurity.

Lack of communication is a problem for any organization. The survey by Ponemon Institute LLC (2014) found that 51% report lack of information from security solutions and are unsure if their solution can tell the cause of an attack. Lack of communication can certainly affect awareness negatively. Human factor integration can contribute to environmental situations involving work shifts, communication during emergencies, communication of concerns and risks to contractors, identification of tools, and communication of changes to procedures and plans. The main aim is to not miss important information, or create misunderstandings, or increase cost due to dealing with unhelpful information. Complacency can cause false confidence at both organizational level and at the user level. A user can feel confident because current behavior did not cause a breach, yet it does not mean that intentional wrong doing would not cause a future breach. Lack of knowledge can cause unintentional mistake such as not logging off accounts, or writing difficult to memorize password on a paper, etc. Distraction was already mentioned as a mistake and as a tactic of an attack. Lack of team work can cause a breach because hackers have an understanding on how IT teams work, and they can take advantage of their dysfunction. Fatigue was already mentioned as a problem factor. The environment in which the user is working can cause pressure and stress while it does not provide actionable policies or training to strengthen weaknesses. We discussed in SCT that environment affects behavioral factors. Lack of assertiveness can be connected to communication and self-efficacy. Lack of assertiveness can lead to not communicating directly with teammates potential concerns, or proposing possible solutions, or asking for a feedback. Lack of awareness can be caused by not being vigilant. Norms were discussed in Normative Behavior theory, and the user can conduct negative or unsafe behavior, or take a wrong action in ambiguous cases.

Insight based on chemical industry

Behavioral cybersecurity can benefit from the pitfalls recognized by human factors in other industries. We mention here our insight as an interpretation of human errors in cybersecurity based on common mistakes that happen in chemical industry sites, that are labeled as major hazard sites (Noyes 2011). A parallel comparison of major vulnerable cyber environment to a major hazard site is the following:

- Cyber defenders and users are not superhuman, and may not be able to intervene heroically in emergencies. The incident response team is formed by many members and its efficiency depends on many factors such as the team's budget, training, whether teams are internal or external, available tools, etc. Actually, more research is needed on resilience and agility function of those response teams.
- Not documenting assumptions or data sources when documenting probabilities of human failure. As mentioned previously, designs and plans are usually geared towards rational cyber-actors.

- Assuming that a defender will always be present, detect a problem and immediately take an appropriate action.
- Assuming that users and defenders are well-trained to respond to incidents. Note that training does not prevent violations.
- Assuming that defenders and users will always follow procedures.
- Assuming that defenders and users are highly motivated and thus not prone to unintentional errors or malicious violations.
- Ignoring the human element, especially human performance as if the cyberspace is unmanned.
- Inappropriate use of defense tools and losing sight of techniques or tools where they are the most effective.
- Not knowing how to manage human error.

Moreover, we interpret three concerns that match with our literature review based on Noyes (2011):

1 The focus is more on technology than human aspects.
2 Ignoring initial vulnerabilities in design and development of systems and focus on training.
3 Blame incidents on a user with or without investigating the system and management failures.

Modeling and simulation

Network security and all the tools associated with it do not provide perfect security. In fact, perfect security does not exist. Hence, there is a continuous need to develop new solutions and tools and test them. This is where modeling and simulation are helpful to save time and keep the cost down while creating test-beds or environments in which those new tools or strategies are tested. Several tools are already established for network simulation since the 1990s such as Network Simulation Testbed (NEST), Realistic and Large (REAL), OMNeT++, SSFNet, NS2, NS3, J-Sim, OPNET and QualNet (Niazi 2019). Yet, not many of these tools are created to address the human element. The main challenge is to validate reliability and dependability of simulation in a comparison to real-life scenarios or data sets. The anonymity problem makes the challenge more difficult. The author in Cohen (1999) discussed the complexity issue in modeling; a simple model may not be as accurate, and the fully detailed models of every threat and defense mechanisms may have higher accuracy but are costly. Exploring answers to many questions about hackers' or insiders' behaviors could help research (or enterprises) to use modeling and simulation to detect anomalies and respond. For instance, what are all possible user behaviors? (Start an application, send a ping, open a file, etc.), what are acceptable or normal behaviors? (Open an authorized file, start an application, etc.), and what are unacceptable behaviors? (Open or attempt to open an unauthorized file, ping, send a bulk of pages to a printer, and browse irrelevant sites that probably can come from copying and pasting disable emails URLs, etc).

The theoretical models of human behavior have been developed and some examples are stated in Goerger (2004):

(1) Baysian-networks are useful to reason from effects to causes or from causes to effects or by a mixed of inferences. Baysian networks are directed graphs and their models belong to the family of probabilistic graphical models. They can be used to simulate the impact of actions or motives, and build in action to mitigate the overall risk. Researchers have used Bayesian network models in intrusion detection systems. Those models have the flexibility to be combined with other techniques, yet authors in Xie et al. (2010) warn that the combination should be done with preserving Bayesian networks strength to identify and represent relevant uncertainties. Many of the behavioral theories can be tested by simulation. In Dutt et al. (2013), Instance-Based Learning Theory predicts that both defender and adversary behaviors are likely to influence the defender's accurate and timely detection of threats. The defender's cyber awareness is affected by the defender's cognitive abilities (experience and tolerance) and attacker's strategy (timing of threats).

(2) A neural-network is a set of algorithms, that are designed to recognize patterns based on a cognitive model or try to mimic the properties of the human brain. Neural-network models are relatively fast, but require a training set to learn and apply learning in operating mode. There are several types of neural network and they are surveyed in Berman et al. (2019) and Parveen (2017). They have useful applications in security and are already used in intrusion detection systems for anomaly detection (Parveen 2017). Their work can be expanded in similar ways that banks currently using them to detect fraudulent transactions. Hence, they can be trained to detect abnormal behaviors. Yet, they still face the challenge of being used as a black box. The recommendation is to use them in combination with artificial intelligence or other models.

(3) While an agent based system could identify characteristics of the environment, it might be able to link user-based actions with their destructive impact on systems. Agent-based modeling is used by social scientists to analyze human behavior and social interactions. Those models are useful to study complex systems and the interaction of the networks can be shown using visualization methods.

(4) Multi-Agent System is a behavior model in which agents can act autonomously on behalf of their users. Agents can work individually or cooperatively. The Multi-Agent System is used recently in studying smart grid communication protocols.

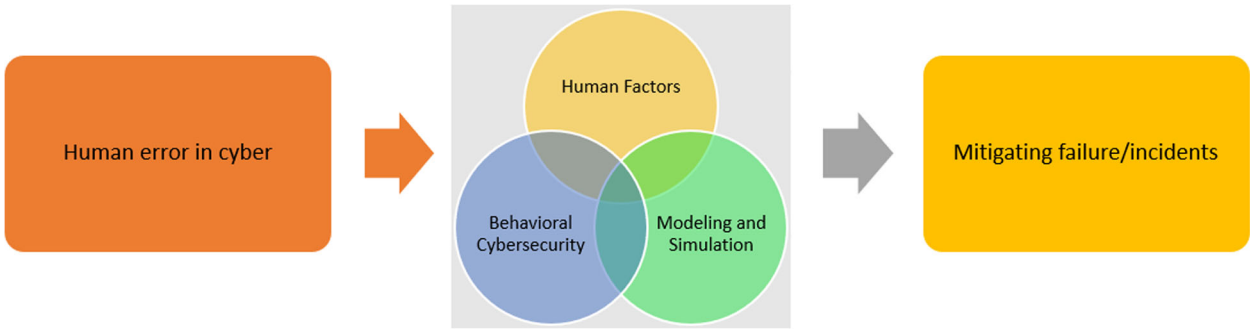

Fig. 7 Mitigating human error concept model using proposed framework

(5) A rule-based or knowledge based system endeavors to imitate human behavior using an enumeration of steps with causal if/then association. Hence, there is precoding of possible situations. This causes a problem where rules are not determined before. Rule-based models are used in detecting anomalies in intrusion detection systems. In Chen and Mitchell (2015), authors proposed a methodology to transform behavior rules used for intrusion detection to a state machine.

Conclusion and future work

Behavioral aspects of cybersecurity are becoming a vital area to research. The unpredictable nature of human behavior and actions make Human an important element and enabler of the level of cybersecurity. The goal from discussing reviewed theories is to underscore importance of social, behavior, environment, biases, perceptions, deterrence, intent, attitude, norms, alternatives, sanctions, decision making, etc. in understanding cybercrimes. Although those theories have some limitations, they can still collectively be used to strengthen a behavioral model. Both the user's and the offender's behaviors and intentions should be understood and modeled. Improving this area will definitely help improve readiness and prevent incidents. No system is 100% secure, but maximizing security cannot happen without considering the human element. The motto of *Trust, but Verify* mentioned by President Ronald Reagan applies to cybersecurity. There is a level of trust that is going to be put on a cyber domain in order to be able to work with it, however an ongoing verification is necessary. Employees have to be knowledgeable of the risks, and differentiate desired from undesired behaviors. Yet, some employees may not comply because of implementing techniques of neutralization. Cyber awareness training should be personalized because employees may have different credentials or levels of access and responsibilities. They also have their own biases to security. One size fits all awareness programs are not effective. There is a level of trust that needs to be put on employees, however, technology and cyber awareness must be taught, and a verification of compliance is necessary. More training is not always the solution. A conceptual framework that is interdisciplinary is proposed to bring together behavioral cybersecurity, human factors and modeling and simulation. Enterprises should be involved in research to make sure that models work the way they are intended. Using a model that is available for the sake of convenience without personalizing it may not be proper. George E. P. Box quote,

"All models are wrong, but some are useful"

should motivate researchers and organizations to ask more questions about the usefulness of a model, which in return promotes revising policies and approaches to security. Therefore, coordinating behavioral aspects and technical aspects of cybersecurity should be typical to each organization. Our future work will contribute to the three main concerns stated at the end of Section 3. For instance, we will explore cyber incidents such as insider threat from the perspective of human error using the proposed framework. A concept model is depicted in Fig. 7.

The model can also support mitigating failure due to social engineering, or weapons of influence. Hence, future work will support a different kind of cyber ontologies. We will also study deception games using game theory with different attacker-defender scenarios. The final statement is remain vigilant and be prepared to expect the unexpectable.

Abbreviations

AHP: Analytical hierarchy process; ANP: Analytical network process; AMCs: Auto-associative memory columns; XSS: Cross site scripting; DDoS: Distributed denial of service; HPR: Human plausible reasoning theory; IDS: Intrusion detection system; JIT: Just in time; MAP: Map-assess-recognize-conclude; MOE: Measure of effectiveness; MCDM: Multi-criteria decision-making; NIST: National institute of standards and technology; SCP: Situational crime prevention; SCT: Social cognition theory; SQL: Structured query language; TAM: Technology acceptance model; TPB: Theory of planned behavior; UIM: Unintentional - intentional - malicious

Acknowledgements
The authors would like to thank the journal for the opportunity to publish an open access paper, and many thanks to the outstanding reviewers for their hard work and feedback.

Authors' contributions
All authors contributed to different parts of the manuscript. They participated in revising and approving revisions. The author(s) read and approved the final manuscript.

Authors' information
Rachid Ait Maalem Lahcen is a Mathematics Instructor at University of Central Florida (UCF) Orlando Florida. He holds a Master of Sciences in Mechanical Engineering, a Master of Sciences in Modeling & Simulation, a graduate certificate in Mathematics, and a graduate certificate in Modeling and Simulation of Behavioral Cybersecurity. All from UCF. His research interests are cybersecurity, graph network, inverse problems, numerical methods and students' learning.
Bruce Caulkins is a Research Assistant Professor and Director of the Modeling & Simulation (M&S) of Behavioral Cybersecurity Program at the Institute for Simulation & Training (IST) at the University of Central Florida (UCF). He is a retired Army Colonel with over 28 years of experience in tactical, operational, and strategic communications and cyberspace operations. In his last military assignment, he was the Chief of the Cyber Strategy, Plans, Policy, and Exercises Division (J65) within the U.S. Pacific Command. In this capacity, he gained extensive insight into cyber capabilities, operational requirements, combatant command requirements, coalition and partner cyber/communications interoperability, and human factor requirements. He also led over a dozen coalition and partner interoperability exercises, to include the HADR-focused PACIFIC ENDEAVOR. Bruce previously taught at and ran several communications and cyber-related schools within the Army's Training and Doctrine Command. He earned his Ph.D. in Modeling and Simulation at the University of Central Florida, focusing on anomaly detection within intrusion-detection systems. His research interests include behavioral aspects of cybersecurity; threat modeling; cyber workforce development; anomaly detection; cyber security and analysis; cyber education and training methodologies; predictive modeling; data mining; cyber strategy; and, cyber policy.
Ram Mohapatra received his Ph.D. from Jabalpur University India, and taught in American University of Beirut, University of Alberta, Edmonton, York University, Downsview, and at the University of Central Florida, Orlando from 1984where he serves as a Professor of Mathematics. His research interests are in Summability Theory and Sequence Spaces, Fourier Analysis and wavelets, Frame and Approximation Theory, Variational Inequalities and Optimization Theory, Harmonic Functions and Complex Analysis. He has written over 150 research papers in refereed journals. His current research interest is Cyber Security and Graph Theory. In addition to the journal papers, he has written many book chapters, edited seven monographs/ proceedings of conferences, and written two books: one on Fuzzy Differential Equations and the other on Biomedical Statistics with computing. He serves as a member of the editorial Board of five journals in Mathematics.
Manish Kumar is presently working as assistant professor in the Department of Mathematics at the Birla Institute of Technology and Science, Pilani at Hyderabad campus, Hyderabad, Telangana, India. Dr. Kumar obtained his Master of Science in Mathematics from Banaras Hindu University, Varanasi, Ph. D. in Department of Applied Mathematics at Indian School of Mines, Dhanbad, and received various awards. Dr. Kumar is guiding several undergraduate students and published various research papers in national and international journals of repute. Dr. Kumar had chaired a session at the International Congress in Honor in Faculty of Arts and Science, Department of Mathematics in Bursa, Turkey, and also organized a Symposium in ICNAAM 2013 at Rhodes in Greece. Dr. Kumar is member of several national and international professional bodies and societies. Dr. Kumar has visited and delivered invited talks in several national and international conferences, including his recent talk on "Two stage hyper-chaotic system based image encryption in wavelet packet domain for wireless communication systems" at ICM 2018 in Rio de Janeiro, Brazil. Dr. Kumar research areas are pseudo-differential operators, distribution theory, wavelet analysis and its applications, digital image processing, and cryptography.

Funding
The authors declare that this work was not funded.

Availability of data and materials
No data is used in this paper.

Competing interests
The authors declare that they have no competing interests.

Author details
[1]University of Central Florida, Mathematics Department, Orlando, FL 32816, USA. [2]Institute for Simulation and Training, 3100 Technology Pkwy, Orlando, FL 32826, USA. [3]Birla Institute of Technology and Sciences - Pilani, Hyderabad Campus, Hyderabad 500078, Telangana, India.

Received: 6 October 2019 Accepted: 10 March 2020
Published online: 21 April 2020

References
Addae JH, Sun X, Towey D, Radenkovic M Exploring user behavioral data for adaptive cybersecurity. User Model User-Adap Inter 29(3):701–750. https://doi.org/10.1007/s11257-019-09236-5
Ahram T, Karwowski W (2019) Advances in Human Factors in Cybersecurity. In: AHFE: International Conference on Applied Human Factors and Ergonomics. Springer, Washington D.C. pp 66–96. https://doi.org/10.4018/978-1-5225-9742-1.ch003
Apvera (2018) The Essential Guide to Risk Management & Compliance (GRC) 2018, Tech. rep.. Apvera
Azaria A, Richardson A, Kraus S, Subrahmanian VS (2014) Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data. IEEE Trans Comput Soc Syst 1(2):135–155. https://doi.org/10.1109/TCSS.2014.2377811
Berman DS, Buczak AL, Chavis JS, Corbett CL (2019) A survey of deep learning methods for cyber security. Inf (Switzerland) 10(4). https://doi.org/10.3390/info10040122
Blackborrow J, Christakis S (2019) Complexity In Cybersecurity Report 2019 - How Reducing Complexity Leads To Better Security Outcomes. Tech. Rep. May, Forrester's Security & Risk research group
Burns S, Roberts L (2013) Applying the Theory of Planned Behaviour to predicting online safety behaviour. Crime Prev Community Saf 15(1):48–64. https://doi.org/10.1057/cpcs.2012.13
Cacioppo JT, Petty RE (2001) The elaboration likelihood model of persuasion. Adv Exp Soc Psychol 19:673–676. https://doi.org/10.1558/ijsll.v14i2.309
Cappelli D, Moore A, Trzeciak R (2014) The CERT Guide to Insider Threats How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). In: SEI Series in Software Engineering represents, 2nd edn. Addison-Wesley, Westford, Massachusetts
Caulkins B (2017) Lecture title Modeling and Simulation of Behavioral Cybersecurity, Retrieved on December 26, 2018 from IDC 5602 Cybersecurity: A Multidisciplinary Approach
Chen IR, Mitchell R (2015) Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems. IEEE Trans Dependable Secure Comput 12(1). https://doi.org/10.1109/tdsc.2014.2312327
Cheng L, Li W, Zhai Q, Smyth R (2014) Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. Comput Hum Behav 38:220–228. https://doi.org/10.1016/j.chb.2014.05.043
Cohen F (1999) Simulating Cyber Attacks, Defences, and Consequences Modeling, Simulation, and Data Limitations in Information Protection. Comput Secur 18:479–518
Corner A, Hahn U (2013) Normative theories of argumentation: Are some norms better than others? Synthese 190(16):3579–3610. https://doi.org/10.1007/s11229-012-0211-y
Dinev T, Hu Q (2007) The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. J Assoc Inf Syst 8(7):386–408. https://doi.org/10.17705/1jais.00133
Donaldson S, Siegel S, Williams CK, Aslam A (2015) Enterprise Cybersecurity - How to Build a Successful Cyberdefense Program Against Advanced Threats. Apress Media LLC, New York

Dupont G (1997) Human Error In Aviation Maintenance. https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.faa.gov%2Fabout%2Finitiatives%2Fmaintenance_hf%2Flibrary%2Fdocuments%2Fmedia%2Fhuman_factors_maintenance%2Fhuman_error_in_aviation_maintenance.pdf&data=02%7C01%7Crachid%40ucf.edu%7C12bb36a6d43b4079629208d7cc912306%7Cbb932f15ef3842ba91fcf3c59d5dd1f1%7C0%7C0%7C637202796057556002&sdata=xRO8qOMjAMovJLrEJMArj4%2B%2BYHTO6Pl9FdyDO9UQJR4%3D&reserved=0. Accessed 28 Dec 2019

Dutt V, Ahn YS, Gonzalez C (2013) Cyber situation awareness: Modeling detection of cyber attacks with instance-based learning theory. Hum Factors 55(3):605–618. https://doi.org/10.1177/0018720812464045

Embrey D, Kontogiannis T, Green M (1994) Guidelines for Preventing Human Error in Process Safety. Am Inst Chem Eng. https://doi.org/10.1002/9780470925096

Faklaris C (2018) Social Cybersecurity and the Help Desk : New Ideas for IT Professionals to Foster Secure Workgroup Behaviors. Baltimore, MD: USENIX Symposium on Usable Privacy and Security

Ferreira A, Coventry L, Lenzini G (2015) Principles of Persuasion in Social Engineering and Their Use in Phishing. Springer International Publishing. https://doi.org/10.1007/978-3-319-20376-8_4

Filkins B (2014) New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations. Sans Inst. https://www.qualys.com/docs/sans-threats-drive-improved-practices-state-of-cybersecurity-health-care-organizations.pdf. Accessed 30 Mar 2020

Fineberg V (2014) BEC: Applying Behavioral Economics to Harden Cyberspace. J Cyber Secur Inf Syst 2(1):27–33

Freilich JD, Newman GR, Freilich JD, Newman GR Situational Crime Prevention. In: Oxford Research Encyclopedia of Criminology and Criminal Justice, February 2020. pp 1–28. https://doi.org/10.1093/acrefore/9780190264079.013.3

Friedman S, Gokhale N (2019) Pursuing cybersecurity maturity at financial institutions: Survey spotlights key traits among more advanced risk managers. Tech. rep. Deloitte Center for Financial Services analysis

FTC (2019) Equifax Data Breach Settlement. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement. Accessed 27 Dec 2019

Goerger SR (2004) Validating human behavioral models for combat simulations using techniques for the evaluation of human performance. Tech. Rep. 3. Naval Postgraduate School, MOVES Institute, Monterey, CA

Gottfredson M (2017) Self-Control Theory and Crime. https://doi.org/10.1093/acrefore/9780190264079.013.252

Greitzer FL, Hohimer RE (2011) Modeling Human Behavior to Anticipate Insider Attacks. J Strat Secur 4(2):25–48. https://doi.org/10.5038/1944-0472.4.2.2. http://scholarcommons.usf.edu/jss/vol4/iss2/3/

Hald SL, Pedersen JM (2012) An updated taxonomy for characterizing hackers according to their threat properties. Int Conf Adv Commun Technol ICACT:81–86

Halevi T, Lewis J, Memon N (2013) Phishing, Personality Traits and Facebook. https://doi.org/10.1111/j.1469-0691.2005.01161.x. http://arxiv.org/abs/1301.7643

Hardy AB, Howells G, Bandura A, Adams NE (1980) Tests of the generality of self-efficacy theory. Cogn Ther Res 4(1):39–66

Haycock K, Matthews JR (2016) Persuasive Advocacy. Public Libr Q 35(2):126–135. http://dx.doi.org/10.1080/01616846.2016.1200362

Holt TJ (2016) Cybercrime through an interdisciplinary lens. Routledge Taylor & Francis Group. https://doi.org/10.4324/9781315618456

Icek A (2019) Theory of Planned Behavior Diagram. http://people.umass.edu/aizen/tpb.diag.html. Accessed 7 Sept 2019

Kabassi K, Virvou M (2015) Combining decision-making theories with a cognitive theory for intelligent help: A comparison. IEEE Trans Hum Mach Syst 45(2):176–186. https://doi.org/10.1109/THMS.2014.2363467

Kemmerer M (2016) Detecting the Adversary Post- Compromise with Threat Models and Behavioral Analytics. https://www.mitre.org/sites/default/files/publications/pr-16-3058-presentation-detecting-adversary-post-compromise.pdf. Accessed 27 Dec 2019

Lahcen RAM, Mohapatra R, Kumar M (2018) Cybersecurity: A survey of vulnerability analysis and attack graphs. In: International Conference on Mathematics and Computing. Springer. pp 97–111

Maimon D, Louderback ER (2019) Cyber-Dependent Crimes: An Interdisciplinary Review. Ann Rev Criminol 2(1):191–216. https://doi.org/10.1146/annurev-criminol-032317-092057

Maiwald E, Sieglein W (2002) Security Planning & Disaster Recovery. Brandon A. Nordin, Berkeley, California

Mitnick KD, Simon WL (2005) The art of intrusion : the real stories behind the exploits of hackers, intruders, & deceivers. Wiley

Myers J, Grimaila MR, Mills RF (2009) Towards insider threat detection using web server logs. In: Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research Cyber Security and Information Intelligence Challenges and Strategies - CSIIRW '09. p 1. http://portal.acm.org/citation.cfm?doid=1558607.1558670

Niazi MA (2019) Modeling and Simulation of Complex Communication Networks. Modeling and Simulation of Complex Communication Networks Edited by Muaz A. Niazi. The Institution of Engineering and Technology, London. https://doi.org/10.1049/pbpc018e

Norman D (1983) Design Rules Based on Analyses of Human Error. Commun ACM 26(4):254–259

Noyes J (2011) The human factors toolkit Human factors in the management of major accident hazards. https://doi.org/10.1049/pbns032e_ch4

Pabian S, Vandebosch H (2013) Using the theory of planned behaviour to understand cyberbullying. Eur J Dev Psychol 11(4):463–477. https://doi.org/10.1080/17405629.2013.858626. T4 - The importance of beliefs for developing interventions M4 - Citavi

Pal SK, Anand S (2018) InfoSec : A Comprehensive Study. IUP J Comput Sci XII:45–65

Partners CR (2015) Insider Threat Spotlight Report. Tech. rep. Crowd Research Partners

Parush A, Parush D, Ilan R (2017) Human factors in healthcare: a field guide to continuous improvement. Morgan & Claypool

Parveen J (2017) Neural Networks in Cyber Security. Int Res J Comput Sci 9(4):2015–2018

Payne BK, Hadzhidimova L (2018) Cyber security and criminal justice programs in the United States: Exploring the intersections. Int J Crim Justice Sci 13(2):385–404

Pfleeger SL, Caputo DD (2012) Leveraging behavioral science to mitigate cyber security risk. Comput Secur 31(4):597–611. https://doi.org/10.1016/j.cose.2011.12.010

Pogue C (2018) Decoding the minds of hackers. https://www.nuix.com/black-report/black-report-2018

Ponemon Institute LLC (2014) Exposing the Cybersecurity Cracks : A Global Perspective. Tech. Rep. April. Ponemon Institute LLC

Reardon S (2011) Antismoking drive tries cigarette ads, in reverse. Science 333(6038):23–24. https://doi.org/10.1126/science.333.6038.23. https://science.sciencemag.org/content/333/6038/23

Rodriguez MA, Bell J, Brown M, Carter D (2017) Integrating Behavioral Science with Human Factors to Address Process Safety. J Organ Behav Manag 37:301–315

Shetty SS, Shetty RR, Shetty TG, D'Souza DJ (2018) Survey of hacking techniques and it's prevention. IEEE Int Conf Power Control Signals Instrum Eng ICPCSI 2017:1940–1945. https://doi.org/10.1109/ICPCSI.2017.8392053

Siponen M, Vance A (2010) Neutralization: New insights into the problem of employee information systems security policy violations. MIS Q 34(3):487–502. https://doi.org/10.1038/174197b0

Stanton JM, Stam KR, Mastrangelo P, Jolton J (2005) Analysis of end user security behaviors. Comput Secur 24(2):124–133. https://doi.org/10.1016/j.cose.2004.07.001

Stolfo SJ, Bellovin SM, Hershkop S, Keromytis AD, Sinclair S, Smith SW (2008) Advances in information security: Insider attack and cyber security - Beyond the hacker. Springer, New York

Symantec (2017) Internet Security Threat Report ISTR 22 Government Internet Security Threat Report. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf. Accesssed 27 Dec 2019

Theoharidou M, Kokolakis S, Karyda M, Kiountouzis E (2005) The insider threat to information systems and the effectiveness of iso17799. Comput Secur 24(6):472–484

Triantaphyllou E, Kovalerchuk B, Mann L, Knapp GM (1997) Determining the most important criteria in maintenance decision making. J Qual Maint Eng 3(1):16–28. https://doi.org/10.1108/13552519710161517

Triantaphyllou E, Mann SH (1995) Using the analytic hierarchy process for decision making in engineering applications: some challenges. Int J Ind Eng Appl Pract 2(1):35–44

Uebelacker S, Quiel S (2014) The social engineering personality framework. In: Proceedings - 4th Workshop on Socio-Technical Aspects in Security and Trust, STAST 2014 - Co-located with 27th IEEE Computer Security Foundations Symposium, CSF 2014 in the Vienna Summer of Logic 2014, January. pp 24–30. https://doi.org/10.1109/STAST.2014.12

Wilamowski GC, Dever JR, Stuban SMF (2017) Using Analytical Hierarchy and Analytical Network Processes to Create CYBER SECURITY METRICS. Defense ARJ. https://doi.org/10.22594/dau.16-760.24.02

Willetts D (2014) 2014 Information Security Breaches Survey: Technical Report. Tech. rep. Department of Business Innovation & Skills

Xie P, Li JH, Ou X, Liu P, Levy R (2010) Using Bayesian networks for cyber security analysis. In: Proceedings of the International Conference on Dependable Systems and Networks. pp 211–220. https://doi.org/10.1109/DSN.2010.5544924

Xu M, Schweitzer KM, Bateman RM, Xu S (2018) Modeling and Predicting Cyber Hacking Breaches. IEEE Trans Inf Forensic Secur 13(11):2856–2871. https://doi.org/10.1109/TIFS.2018.2834227

Publisher's Note