Information Systems Frontiers
https://doi.org/10.1007/s10796-019-09949-3

Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes

Mario Silic[1] · Paul Benjamin Lowry[2]

Abstract
What is happening in hacker's minds when they are committing criminal activities? How black hat hackers manage nerves, which is about managing fear and underlying emotions, and which tactics they employ during their decision-making process before, during and after committing a crime, is the question that could provide some initial insights on hacker's trajectories, their switch from black hat to white hat and ultimately about their behaviors and motivations. The main difficulty in answering this question resides with the access to hacker's data. To address this gap, we conducted interviews with 16 black hat hackers. Supported by the general strain theory and routine activity theory, we identified five techniques that they use to manage their nerves: shunting, minimization, plan B, thrill, and lens widening techniques. Each of these techniques help hackers to better manage their nerves and consequently, learn how to better cope with the fear. During their psychological decision-making processes, hackers use these five techniques to create a new mindset, behind which they hide, with the objective of minimizing and mitigating the inherent risks they encounter during their criminal activities. The theoretical importance of nerve is the key to a better understanding of black hat hacker's illegal acts, their behaviors and ultimately their actions.

Keywords Black hat hacker · Security · Criminology nerve management · General strain theory · Routine activity theory (RAT)

1 Introduction

In 2016, black hat hackers, that we define as individuals with extensive computer knowledge employed to get personal gains or for other malicious reasons by conducting illegal activities (Chandler 1996; Smith and Rupp 2002), were behind major cyber security incidents (Cisco 2018; EY 2018). This caused an average 20% loss of a company's customer base with a trend of the hacking becoming more business and corporate oriented with unprecedented levels of sophistication and impact (Cisco 2018). The resulting revenue loss opportunities push companies to increase their security investments, since it is unlikely that the magnitude and the impact of cybercriminal attacks will decrease, given the current rate of increase in internet traffic. Sony, Ashley Madison, JP Morgan are examples of recent security incidents which reveal the pervasiveness of this issue. To combat this trend, it is essential to get a better understanding of cybercrime's costs, benefits, and attractiveness (Kshetri 2006). However, little is known about the people behind these illegal cybercrime activities, for three key reasons: (1) given its criminal nature, it is difficult to obtain reliable data (Benjamin et al. 2019; Mahmood et al. 2010); (2) the fact that existing studies are anecdotal and rely on descriptive accounts and reporting (Crossler et al. 2013); and (3) the lack of a solid theoretical foundation to support the empirical evidence (Crossler et al. 2013; Mahmood et al. 2010). A key weakness in the IS security literature is that it focuses too much on policy compliance and non-malicious behaviors; by contrast, there is a clear need for more research on the "black hat" dimension of cyber security (Benjamin et al. 2019; Mahmood et al. 2010), with a focus on the malicious and deviant (i.e., criminal) behavior that threaten organizations (Crossler et al. 2013; Lowry et al. 2017; Willison and Lowry 2018; Willison et al. 2018).

Different theories, ranging from the differential association theory (Blackburn 1993), theory of operant conditioning (Skinner 1972), social learning theory (Bandura and Walters 1977; Lowry et al. 2016), to deterrence theory (Gibbs 1975;

✉ Mario Silic
mario.silic@unisg.ch

Paul Benjamin Lowry
Paul.Lowry.PhD@gmail.com

[1] University of St. Gallen, Mueller-Friedberg-Str. 8, 9000 St. Gallen, Switzerland

[2] Pamplin College of Business, Virginia Tech, Blacksburg, VA, USA

Published online: 04 September 2019

Willison et al. 2018), have all been relatively effective in explaining deviant behaviors and criminal continuation. However, because hacking is an unconventional criminal activity (Davis and Hutchison 1997), there is no single theory that well explains hacker[1] behavior. Interestingly, the role of emotion, stemming from the general strain theory (Agnew 1992), was found to be one of the central factors in driving deviant behavior that is fostered by anger and frustration. Although this theory was widely applied in traditional street crimes (Baron 2004), it is not clear what role emotion may play in the hacking context. In particular, we are interested in how black hat hackers process their fear and subsequently manage their nerves when committing a virtual crime. Clarifying this theoretical issue would be of high importance in better understanding the hacking criminal behavior. Notably, we would extend existing theoretical understandings of hacker-offending decision-making processes.

That is, we are particularly interested in understanding how black hat hackers manage fear and their nerves. Nerve management is about the ability to manage fear and underlying emotions. Nerve management is essential, since it drives the decision-making process during the criminal act (Cornish et al. 2008). Unlike other criminal activities (e.g., car thieves), where offenders develop various tactics (e.g., self-medication, shunting, fatalism) for committing crime (Jacobs and Cherbonneau 2017), black hat hackers, likely employ different tactics to create and manage their nerves because they are in a highly unique criminal context that is virtual and perceptually hidden in a computer system,.

The importance of better understanding these tactics is essential in better understanding black hat hacking, and ultimately how to thwart it. Indeed, in the hacking decision-making processes, calm nerves should facilitate better control of the crime situation, minimizing risks and possible sanction threats. It is particularly compelling to consider how black hat hackers manage their nerve, given that face the possibility of severe sanctions if they are caught (e.g., arrest, prosecution, loss of employment, and fines). According to Holt and Bossler (2014, p. 33): "The increasingly rapid adoption of technology at all ages in industrialized nations requires research identifying how the use of computers and the Internet affect adolescent development through adulthood and involvement in both on- and off-line offending" (p. 33). We argue that better understanding how emotional dimension, and more precisely a hacker's nerves, is managed could provide new insights into hacker trajectories and their psychological functioning. It is evident that nerve management could be an important unexplored dimension that could provide theoretical explanations of hacker's emotional states they have to cope with when confronted to crime situations.

[1] Throughout the text, for concision, we use the term, 'hacker' to refer to the 'black hat hacker.'

In this context, our study relies on the qualitative approach based on grounded theory (Corbin and Strauss 2008), which is particularly useful in dynamic environments (Strauss and Corbin 1994), such as the hacking context (Turgeman-Goldschmidt 2005). Indeed, according to Turgeman-Goldschmidt (2005, p. 10) "the best way to reach the true meaning of the criminal behavior of hackers requires using qualitative research methods in general and the grounded theory in particular because computer crime has yet to be extensively explored from the offenders' points of view (i.e., their perceptions, attitudes, behaviors, etc.)" (p. 10). By applying the grounded theory approach we can discover relevant categories and relationships among them (Strauss and Corbin 1994) to reveal the justification for the black hat hacker's motivations and psychological states that drive and shape their nerve management. We argue that the theoretical importance of nerve management is the key to a better understanding of the black hat hacker's illegal acts, behaviors and actions. It is crucial to understand how black hat hackers manage their nerves and which factors influence their decision-making process before and after committing a crime. The answer to this question could provide some initial insights on hacker's trajectories, their switch from black hat to white hat and their behaviors and motivations.

In the following sections, we present the theoretical foundations for this study, followed by the research methodology. We then discuss our findings and conclude the study.

2 Theoretical Background

Our research applies grounded theory approach which should provide us relevant explanations, interpretations and implications. To apply and interpret our grounded theory development, we are supported by the theoretical foundations of general strain theory (Agnew 1992) and routine activity theory (RAT) (Cohen and Felson 1979).

2.1 Development of Crime

Based on its origins in the 1960's, the word "hack" meant improving programming flaws of mainframe computers by a group of MIT students. Fixing bugs and improving programming mistakes by doing small "hacks" was performed by an individual (i.e., hacker). This person was considered to have a higher level of computer knowledge and was able to alter programs or systems (Yar 2005). In 1963, one of the first incidents of malicious hacking was reported (telephone hackers) by MIT's student newspaper (Lichstein 1963). Hackers are now generally divided into two main groups: white hat and black hat hackers. These two groups have different motivations, objectives and rules. While white hat hackers are usually considered positively. They seek to

acquire new knowledge and to provide information about vulnerabilities, weaknesses and threats that they have identified in computer systems. By contrast, the black hat hackers attempt to achieve financial gain from their knowledge by blackmailing, sabotaging or engaging in other criminal activities (Schell and Dodge 2002). Previous studies that focused on the motivation behind hacking activities provided different explanations for their acts, such as justice (Rogers 2006), enjoyment and curiosity (Turgeman-Goldschmidt 2005), morality and connectedness (Teske 1997), among others. Regardless of the specific motivation to commit an illegal action, every hacker usually balances benefits and costs, before deciding whether or not to commit the crime (Probasco and Davis 1995). These intangible psychological costs relate to the amount of mental energy required to commit the crime. Fear of apprehension of punishment remains an important decision-making criteria before the crime is committed (Kshetri 2006).

Most individuals who commit crimes and act unethically believe that there is nothing wrong in what they are doing (Kallman and Grillo 1998). They do not perceive their actions as being really illegal, unethical or inappropriate. It is clear that for most black hat hackers, committing a cyber-crime does not increase their guilt level, as is the case for more conventional crimes (Phukan 2002). This is because it is not always easy to identify the victim, as well as different socio-cultural backgrounds where the cost of their acts is weighed against the context in which they operate (Deci and Ryan 2010).

To date, little empirical evidence has been provided to further explain the black hat hacker's motivations (Crossler et al. 2013; Holt and Bossler 2014; Holt et al. 2012; Mahmood et al. 2010; Schell and Holt 2009). This has contributed to the difficulty in getting the data (Benjamin et al. 2019). The majority of previous studies primarily focused on discussing hackers motivation, rather than providing empirical evidence (e.g., Cross 2006; Schell and Dodge 2002). Other studies that tried to understand the complex hacker's phenomenon, mostly focused on the student population (e.g., Hu et al. 2011; Rogers 2006). However, we believe students are a particularly poor sample frame from which to represent the complex psychological motivations behind black hat hackers' highly criminal. Moreover, the other flaw in these studies is they did not analyze the actual context in which hackers operate, such as hackers forums or Internet Relay Chats (e.g., Benjamin et al. 2015; Benjamin et al. 2019; Benjamin et al. 2016). Importantly, the few studies that used known hackers as informants (e.g., Holt 2009; Hu et al. 2011; Schell and Holt 2009; Young et al. 2007), revealed that hackers perceive a low level of potential sanction. They also believe that they will not be caught easily. This signals that the likelihood of punishment is low (Young et al. 2007). These findings indicate that hackers are able to manage their nerves in the face of great potential risks they engage in.

An assessment of cybercrime research by Holt and Bossler (2014, p. 33), has showed three kind findings that we build on: (1) that there is a considerable increase in scientific contribution on various forms of cybercrime; (2) that traditional criminological theories generally hold in the online context; but, also (3) that there are still important new avenues for research to explore, and especially to further examine "breadth of existing and recent criminological theory to expand our knowledge of cybercrimes." Notably, existing knowledge on hacker's motivations, ranging from political or religious reasons (Holt 2009) to money, entertainment, ego, cause, entrance to a social group, and status (The-Honeynet-Project 2004), is relatively well researched. However, little to no research on hacker's demographics, psychological predispositions, and social/behavioral patterns exists (Schell and Holt 2009). We position our research within the psychological boundaries in which emotional states and fear management are taking roots. This positioning is guided by the theoretical input that we detail in the following section.

There are several theories, originating from the criminology field, that fit well into the hacking context, such as self-control theory (Gottfredson and Hirschi 1990), RAT (Cohen and Felson 1979), situational action theory (Wikström 2004, 2006), or even theories borrowed from economics (Kshetri 2006; Leeson and Coyne 2005). However, due to the different context in which they operate, compared to other crime contexts where physical violence is usually present, we argue that there is a need to apply different theoretical insights to support the underlying premises. Hackers do not always operate rationally—especially in terms of operating through costs, benefits, and sanctions—as economic theories would suggest (Yar 2005). Something else is driving them and allows them to suspend threat of sanctions that most people would perceive. A lack of empirical studies to validate the applicability of certain theories in the hacking milieu and with known hackers, suggests that different theoretical premises should be incorporated into the theoretical foundation, when studying hacker's behaviors. We address this mystery.

To guide the interpretation of our grounded theory research, we rely on the general strain theory (Agnew 1992) and RAT (Cohen and Felson 1979). General strain theory argues that negative emotions can lead to anger and frustration, where individuals experiencing strains or stressors engage in crime to escape from those stressors. These negative emotions are particularly important in the hacking context as they could be a source of inspiration for illegal behavior. Several specific strains are advanced in the theory such as the failure to achieve positively valued goals (e.g., money) or the presentation of negatively valued stimuli (e.g., political motives such as injustice related to different causes) (Patchin and Hinduja 2011). The first strain is about unmet expectations of individuals that leads to disappointment. The second strain is a response to the negatively valued stimuli in which

individuals look for avoidance, leading to negative and illegal activities such as hacking. Finally, these negative emotions call for a way to relieve one's internal pressure. According to Patchin and Hinduja (2011) when people cannot achieve their goals then strain will be experienced, which can then cause them to turn to crime. Typically, this path to the criminal behavior can be seen among black hat hackers where failure to achieve positively valued goals, such as financial remuneration, leads to the criminal behavior.

RAT suggests that crime commitment is the result of an opportunity, highlighting "*the convergence of motivated offender, suitable target, and the lack of a capable guardian at a particular place and time as the core elements necessary for a crime to occur*" (Groff 2008, p.99). *Motivated offenders* are individuals or groups that have the ability and motivation to commit a crime for various reasons. *Guardianship* refers to the ability to intervene into a crime (i.e., the hacking activity) and consequently, prevent it. Importantly, in our virtual cybercrime context, the concept of physical proximity is removed (Yar 2005). Consequently, the applicability of RAT to cybercrime is even more relevant because victims are placed in the "virtual proximity" to motivated offenders. That is, opportunity for black hat behavior is increased because it is easier for motivated offenders to find victims because they do not have to be physically proximate. Typically, the risk is greatly increased in online situations in which individuals demonstrate higher amounts of time spent online, higher use of internet banking or online purchases, and have overall more risky online behavior. Furthermore, RAT provides an explanation that in absence of capable guardianship, the costs of committing the crime are relatively low, which then increases the benefits. Capable guardians are usually translated into lack of security measures such as lack of antivirus, low malware protection, or inadequate network security in the organizational context (Reyns 2013). In all these situations, higher victimization can be expected as a consequence of a lack of actions on the victim's side. Consequently, the costs for hackers to perform illegal activities are relatively low as they have to invest much less of resources to conduct hacking.

Thus, it is one thing to be angry and have a general motivation for criminal hacking—a necessary but insufficient start from general strain theory—but a potential hacker needs a suitable target for which they can believe they can reasonable hack to express their anger—it cannot be just any target. Meanwhile, the "capable guardian" component of hacking is especially crucial in calculating the risks and uncertainties. As illustration, suppose a hacker is angry by the US government's policies and activities in the Middle East. Unless the hacker has unusual capabilities, and a network of similarly minded hackers, he/she probably would not consider hacking the Pentagon's computers to be a realistic target or one for which he/she could manage his/her nerves. This is because the "guardians" (and associated technologies) that protect the Pentagon's computer are among the best in the world. Instead, it would be more realistic to hack a regional newspaper website that is considered pro-US in its coverage.

Overall, general strain theory explains that different strains are impacting hacker's emotional state motivating him/her to crime, whereas RAT explains the crime context in which the "virtual proximity" is the main facilitator of the criminal behavior. Applying these theoretical lenses in our context, black hat hackers, when committing a cybercrime where costs and benefits of their acts are evaluated, manage their nerves differently than other more standard types of crimes (e.g. drug smuggling). In the next section, we conceptualize nerves and discuss nerve management from a hacker's perspective.

2.2 Nerve Management

In this section, we explain how nerve management works for hacker's in respect to both general strain theory and RAT. Overall, nerve management can be a useful technique that hackers can use to intervene into their cognitive reasoning to moderate and mitigate the fear that they may experience during their criminal acts. Nerve management is about managing the uncertainty and providing more clarity to their own decision-making space they create in their psychological and mental states when they engage in criminal activity. However, the technical knowledge (higher or lower) to hack in the system may not be enough to "*manage the intense emotions brought on by crime, while maintaining some minimal level of composure*" (Cherbonneau and Copes 2006, p.206). This is because without proper nerve management, it may not be possible to succeed in accomplishing the crime. Ironically, this may be why many black hat hackers eventually become white hat hackers. In a hacker's context, the manifestation of nerves occurs when hackers engage in risky illegal behaviors (e.g., illegally obtaining data, penetrating a target system, acquiring unauthorized access, and the like). Such risky and illegal activities can lead the hacker to be recognized by their peers (Levy 2001). However, many such hackers actually care about potential negative outcomes arising from their acts. For some hackers, it is not acceptable to ask for any ransom or to behave in an unethically acceptable way—leading to what is referred to as "white hat" hacker behaviors. It is evident that in all of these situations that emotions play an important role.

This criminal context in which negative emotions can lead to anger and frustration is well explained by the general strain theory (Agnew 1992). Strain theory explains that "When legitimate solutions are not available, non-economic strain results in non-compliant behavior (Agnew 1999)" (Wall et al. 2016, p. 51). Such non-economic strains are typically stressors like anger and negative emotions, and deviance is a way of dealing with or escaping from these stressors (Agnew 1999). Crucially, the relationship between emotions and nerve management needs to be better understood as the concept of

nerves is closely related to negative emotion (Jacobs and Cherbonneau 2017), which is a consequence of an anger frustration situation. This anger/frustration dimensions, the core premise of general strain theory (Agnew 1992, 1999), suggest that an offender will rely on these two factors to build the negative emotion and will, in turn, commit a crime.

Meanwhile, RAT theory argues that criminal behavior is the result of an opportunity. Although crime can be attractive to commit (Katz 1988), there is often an explanation for crime accomplishment because it provides an opportunity to commit an illegal act due to the absence of capable guardian (Reyns 2013) or simply due to the 'virtual proximity' context in which hacking is greatly facilitated.

Research explains that nerve develops as part of the group process, in which peer pressure is usually high (Hochstetler 2001). This leads to the negative act commitment by all individuals who are part of the group (Hochstetler 2001). This is typically true in the black hat context, because hackers within the same hacking group will want to show to their 'peers' that they can handle their nerves and commit an illegal act. This allows them to gain recognition and get access to a larger community, since they were able to deliver on their acts by demonstrating strong technical skills and knowledge. As illustration, "*one of the most effective ways of gaining respect is to manifest nerve. A man shows nerve by taking another person's possessions, messing with someone's woman, throwing the first punch, 'getting in someone's face,' or pulling a trigger*" (Anderson 2000, p. 92).

Thus, to these hackers, nerve management becomes a key goal or objective, so that they can prove their abilities to the greater group (Hochstetler 2002). This process appears to be happening frequently, with repetitive phases, where offenders demonstrate "*a sense of 'being on autopilot' or 'on automatic,' as they proceed from target to target*" (Hochstetler 2002, p. 63). It is not surprising that many black hat hackers use security tools (e.g., Metasploit Framework or nmap) to try to hack in an automated way. We also note that many hackers do not use out-of-the-box tools, but rather develop custom tools and approaches that can be difficult to detect by modern antivirus or other security tools. Regardless of the approaches used, hacking has become shockingly ubiquitous: A typical Web server on the Internet is attacked more than a quarter of a million times in a day (Vaughan-Nichols 2018).

3 Method

Again, our study used a qualitative research method based on grounded theory (Corbin and Strauss 2008). Grounded theory aims at uncovering social relationships and behaviors of groups, known as social processes (Crooks 2001). Importantly, by uncovering these processes, theory emerges from the data through an incremental and systematic approach (Parks et al. 2017; Urquhart et al. 2010). Grounded theory is particularly useful for deeply examining emerging issues caused by new sociotechnical phenomenon (Parks et al. 2017). Consequently, grounded theory has been used effectively in several hacker related studies (e.g., Turgeman-Goldschmidt 2005; Turgeman-Goldschmidt 2008), in which the outcome of the grounded theory is "a social construction of the social constructions found and explicated in the data" (Charmaz 1990, p. 1165).

Our data was collected from in-depth interviews (Table 1) with 16 black hat hackers. Since one of the paper's authors was a former white hat hacker, we had easier access to the initial sample of seven black hat hackers, who when asked, suggested 11 informants. All of the interviewees contacted were black hat hackers who had committed at least one illegal act during their hacking career. Institutional Review Board (IRB) approval of the primary investigator was obtained prior to the project start to remove any possible ethical concern related to this project. Other recruitment criteria included the following: 1) the hacker is still active (did not switch to white hat); 2) the hacker is part of a group and does not act on their own (this makes it easier to verify if the hacker really belongs to a specific hacking group and is what he/she claims to be) and 3) the hacker is "present" for more than six months (we wanted to exclude novice and inexperienced hackers). We removed two informants that did not meet all of these criteria.

To increase the likelihood that the participants were legitimate black hat hackers, we conducted ethnographic observations on the Internet sources (e.g., forums) that were revealed by participants during the interview. This was done to increase the likelihood that no fake participants were interviewed but also to make sure that the claims advanced by participants (such as being black hat hacker) were true. By analyzing posts and interactions present on the identified sources were able to accurately confirm hacker's background and their claims (although we anonymized hackers real names/nicknames in the paper, the ethnographic investigation was done using their real pseudonyms).

The mean age for respondents was 22, with a range from 18 to 25 years of age. Detailed demographics are presented in Table 2.

All of the interviews were semi-structured (they took place between January 2017 and February 2018) and followed an open-ended approach. The interviews were between 42 and 61 min long (an average of 55 min). Due to the sensitive nature of the topic and since all interviewees wanted to preserve their complete anonymity, all of the interviews were conducted through secured fully encrypted communication (most of the time using skype). Interviewees did not receive any financial compensation for their participation (this was expected, since hacking involves showing to others their accomplishments through a "feeling of power" that hackers want to express (Leeson and Coyne 2005). All of the

Table 1 Interview details

Hacker (name)	Interview length (min)	Age	Hacking focus	Hacking life (in years)
Voodoo	45	22	- Phishing / Denial of Service	5
Phantasm	58	23	- ClickJacking Attacks	2
Trinity	54	25	- Malware, Virus, Trojan	4
L@ky	58	24	- System penetration / intrusion	3
LucNb	54	21	- System penetration / intrusion	6
NotoriusX	61	24	- Malware, Virus, Trojan	8
NbG	42	23	- Ransomware	5
JustiX	57	24	- Phishing / Denial of Service	8
Mr.trojan	60	22	- System penetration / intrusion	7
Crypto	59	23	- Social engineering	6
Hig Hacker	48	18	- Stealing financial data	3
B14D3	49	19	- Phishing / Denial of Service	4
M3M0RY	59	25	- Phishing / Denial of Service	9
Mr Binary	57	22	- Phishing / Denial of Service	4
Yuliux	55	20	- Ransomware, Malware	5
White Devil	60	20	- System penetration / intrusion	6

interviews were recorded. Four interviewees decided to scramble their voice to minimize any potential identification. The interview guideline (Appendix A) was pretested with one information security professional and one white hat hacker. Minor modifications were implemented to better formulate questions. The interview started with some generic questions for the participants, asking them their hacker name, how they became hackers, etc. The interview then focused on their motives to commit criminal activities and the way they manage their nerve, fear and emotions (e.g., a sample question we asked was: "Can you describe how you feel in the presence of a threat to be caught?" or "Are you afraid to be arrested by the police?"). The names the hackers used were not secret, and thus the interviewees did not have any objections against our using them. Therefore, in the following sections, we refer to their actual publicly available names.

Following Strauss and Corbin (1994)'s recommendations on conducting grounded theory building, we first started with initial open coding.. We proceeded with an axial coding by reducing and clustering different categories that we identified. Finally, we conducted selective coding by detailing and selecting the identified categories. In particular, we used nVivo software (nVivo is a graphical qualitative data analysis computer software package) to analyze the qualitative data, identify different information, patterns, and relationships present in the interviews. We combined or analyzed different categories and subcategories based on their relationships and then tested the theoretical propositions by referring back to the data. For example, we grouped different ideas based on general behavior patterns that emerged from interviews and the corresponding hacking activities that participants detailed during the interview process.

3.1 How Are Hackers' Nerves Managed?

In a typical crime situation, fear behind the act of committing the crime is associated with increased heart rate, faster breathing (Warr 2000) or the release of adrenaline into the blood. Physical agitation accompanied by nervousness, decrease in body temperature, mouth dryness or even psychological signals such as anger, frustration, outrage, are the main signs of fear (Ferraro and Grange 1987). Fear can be seen as "an inhibitory emotion" that should, in most cases, prevent and mitigate criminal offenses (Topalli and Wright 2013, p. 52). Because the emotion of fear drives deterrence (Beccaria 2009), it is expected that the perceived risk of getting caught or sanction risk will be the result of the fear (Gibbs 1975). For Cusson (1993, p. 55) "fear is obviously at the heart of deterrence," but "is not a calculated risk." It would, therefore, be expected that hackers behave the same and manage their nerves accordingly. However, hackers are a different type of offender, since they are usually hiding their identity behind their computers. Therefore, they are usually not facing the victim, as is the case with street crimes. It is still expected that the fear generated by the thought of the possibilities of apprehension, would influence the way nerves are managed in the hacker's mind. However, in reality, the way this cognitive process is managed is different from other criminal situations (e.g., robbery).

3.1.1 From Cognitive Distortion to Broken Windows: Shunting and Minimization Techniques

Cognitive distortion refers to rationalizing attitudes, beliefs or thoughts about one's own or other's social behavior (Barriga

Table 2 Demographics

Summary Variable	Mean Value	Standard deviation
Mean age	22	2.0
Average interview length (in min)	55	5.5
Average hacking life (in years)	5.3	1.92

and Gibbs 1996). In the hacking context, a particularly suitable cognitive distortion is minimizing or mislabeling, where the antisocial behavior is followed by the mentality where the offender believes that no harm is really done, and that his/her actions can even be seen and accepted as admirable. When asked how they felt about their acts, whether it is something they consider to be dangerous, illegal or criminal, they all expressed the same feeling that it was a 'non-violent' act which did not harm anyone. For example, Voodoo said:

> *"…this is just harmless exploration. It's not a violent act or a destructive act. It's nothing."*

Phantasm explained that his/her acts are not violent at all, since it is all about learning:

> *"Not at all. Well, first of all, I was just looking around, playing around. What was fun for me was a challenge to see what I could pull off."*

All of the interviewees confirmed the belief that there was nothing really wrong in what they were doing. The cognitive tactic employed in this context can be referred to as shunting. This is similar to but slightly different from neutralization (Sykes and Matza 1957). Shunting involves only thinking about the positive outcomes and putting aside any fear that may arise from the action (Jacobs and Cherbonneau 2017). Lord Nikon explained that he/she is not even thinking about any negative consequences. He/she sees it as something positive, where he/she will get a new 'power' through his/her acts:

> *"Well, it's power at your fingertips. You can control all these computers from the government, from the military, from large corporations. And if you know what you're doing, you can travel through the internet at your will, with no restrictions. That's power; it's a power trip."*

Trinity has a slightly different view when asked about what he/she considers to be illegal:

> *"At the first time when I came into the headlines for my breach…, I was a little bit afraid that I was getting caught…I did not leak all the database only a little bit to make them aware of it. If it's legal? In my opinion, it is legal when you only leak a little bit database to make them aware of it."*

Several others confirmed Trinity's position that only doing [leaking] a little is not a problem. This sort of minimization technique is an interesting method that hackers use to cognitively minimize the severity of their acts.

Another interesting method used by hackers has its origins in the Broken windows theory (Wilson 2003), which suggests that policing methods that target minor crimes are welcome. This is because a fast reaction will most likely prevent bigger crimes to happen. However, these "minor" crimes in the hacking milieu are usually not sanctioned. This provides justification for hackers to continue with their acts, which could lead to more harmful actions. One hacker explained that risks are low, as the cost of their acts is also low. Therefore, they do not expect the police to chase them for small losses. L@ky commented:

> *[It seems like a lot of risk for the $2K you've made so far]"…Well, that is publicly. And in less than a month. It is no risk for me, as they can't do anything. Like I said, quick easy cash in about a month."*

Another hacker explained

> *"I'm never hacking a company based in my country – no police will come and take me down for such a small cost – If I steel few millions, it would probably be different – but I'm cautious about the amount."*

Clearly, nerves are managed through calculated risks that each hacker weighs to understand possible gains and losses, but this 'calculation' may not be as rational as the hacker believes it to be. This behavior can be associated to bounded rationality, as seen in security contexts in general (e.g., D'Arcy and Lowry 2019), because the decisions hackers make are 'bounded' by their cognitive limitations and also influenced by their emotions. As illustration, one hacker (LucNb) boldly claimed that

> *"only inexperienced or novice hackers do not pay attention to the risks vs fear to get caught – so they make errors and cross the line...I never do that."*

3.1.2 Plan B, Thrill and Lens Widening Techniques

Interestingly, most of the interviewed hackers claimed that they do not worry too much about being apprehended, whether their illegal acts are small or large. The majority of the interviewees claim to have some sort of a backup plan. For example, Trinity said

"Well, it is a little more complicated than that, but I have plans in case something happens."

Others also highlighted that they usually have a backup plan, in case things go wrong. They emphasized the importance of having a Plan B. For example, L@ky explained:

"I'm not afraid. In case something goes wrong – I'm ready and I know what I will do…I don't worry so much."

This 'Plan B scenario' thinking is important in nerve management. Having a Plan B, reduces the psychological discomfort associated with uncertainty (Shin and Milkman 2016). It not only it drives a hacker's state of mind regarding removing or mitigating the risk factors, it also contributes to a better focus on the Plan B scenario. These hackers feel more comfortable in the way their nerves are managed, since they do not fully perceive the inherent risks. This is because they convince themselves they are somehow "secured" by the Plan B scenario that they have put in place. However, when hackers were asked what exactly their Plan B is, most of the them gave a vague and unclear answer. Several of them did not want to clearly explain their back up plan. A few others tried to explain it, but their answers were generic. As illustration, one noted that his/her plan B is:

"I will co-operate and turn to white hat hacker…I'm sure I will not go to prison not pay any penalties…this is anyway not big deal…I did not harm to anyone."

Another important technique used by hackers to manage their nerves is experiencing the thrill. *Thrill* corresponds to a social entertainment method used by hackers to satisfy their inner psychological needs (Turgeman-Goldschmidt 2005). Thrill is a positive, powerful emotion that they thus use to cover up the natural fear that should be resulting from the huge risks they are taking. For example, NotoriusX commented:

"I was just in it for the thrill" and Ley2x added "To be honest, there is a thrill in knowing that what I do would be illegal except for a legal document that says I'm allowed to do it without getting in trouble."

Hiding behind the thrill, provides an opportunity for hackers to go after novelty and intense sensations, as a result of achieving their goal (e.g., breaking into a system). This pursuit of new experience for its own sake, despite the risks, shows how nerves can be more effectively managed.

Lens widening refers to a technique, in which offenders believe that their acts are not that dangerous (Jacobs and Cherbonneau 2017). This allows them to believe that there is really no reason to be nervous. It is a "bigger picture" view, in which offenders compare their acts against other illegal activities and by doing so, they attribute a lower score to the seriousness of their acts. For example, NbG explained:

"what I do is nothing; there are people that get killed daily and all I do is just sneaking around a bit and looking what is behind the curtain; the risk of getting caught is minimal…I will not go to jail for that."

A similar behavior can also be found in neutralization theory via the 'denial of injury technique,' in which an offender insists that his/her actions did not cause any meaningful harm or damage (Sykes and Matza 1957).

Another hacker added that most of the time hacking acts do not get reported. This is because companies are afraid of the impact that the hacking may have on their image. This supports the lens widening view of the majority of the interviewees, who highlighted that their acts are rarely reported. When they are reported or when an investigation takes place, they seem to be "protected" by the gravity of their acts, which in their view, is not that high. Consequently, they should not be punished or risk some more serious consequences. This is because there are so many more serious crimes, compared to their hacking activities. They serve a good cause, as explained by JustiX:

"all I do is to help companies…when I find a bug I to send them an email informing them about my findings… of course, I learn a lot from their security issues…and I will not get caught – why should I? I just helped them by informing them about the security vulnerability I discovered."

4 Discussion

Our study used grounded theory building approach, supported by the theoretical lens we applied from general strain theory (Agnew 1992) and RAT (Cohen and Felson 1979), to better understand the theoretical importance of nerve management by black hat hackers. In particular, we sought to understand, through theory building process, how black hat hackers manage their nerves and which techniques they use in their decision-making process before and after committing a crime.

Drawing from a sample of 16 hackers, we investigated how hackers manage their nerves during illegal hacking activities. According to Jacobs and Cherbonneau (2017), nerves and nervousness are recognized but relatively understudied parts of the offender decision-making process. In that context, "nerve management is, therefore, best considered to be an intervening exercise in the threat perception process, that moderates the fear-offending relationship through its effect on nervousness" (Jacobs and Cherbonneau 2017, p. 14).

Through our grounded theory study, we identified five broader techniques that hackers use to better manage their nerves, including: shunting, minimization, Plan B, thrill and lens widening techniques.

As can be seen from the five techniques described earlier, these hackers are essentially trying to trick themselves to better manage their nerves by implementing different strategies that should help them better cope with the threat. All of the identified techniques have a common purpose, which is to minimize the fear of sanctions, in such a way that offenders feel better and minimize the threat-perception process.

From a theoretical perspective, our research offers several new insights. First, we addressed the calls to further investigate black hat research (Mahmood et al. 2010) to better unmask the mystery of the hacker world (Crossler et al. 2013), by gaining access to real known hackers as the subjects of our study. This addresses one of the primary challenges in the hacking research. By doing so, we contribute to expanding the existing theoretical basis of general strain theory (Agnew 1992) and RAT (Cohen and Felson 1979), by highlighting theoretical justifications that each of these theories offer to better understand hacking in a nerve management context. In particular, the stressors that hackers experience are important factors that drive their emotional states. Also, the "virtual proximity" together with absence of capable guardians provide explanations of why hacking is unique as a criminal activity and highlights the importance of these two dimensions for research and prevention. We further propose newly uncovered techniques that contribute to the frustration or anger phenomenon, which is occurring in the hacker's mindset. All five techniques (i.e., shunting, minimization, Plan B, thrill, and lens widening) contribute at different levels, to better manage nerves when experiencing strains or stressors. These techniques are well-positioned within past research that has called to further understand the psychological predispositions behind criminal acts (Schell and Holt 2009), and in particular, the emotional states of hacker's minds. In such a context, our findings bring new theoretical insights on top of the already established criminological theories. This adds new dimension to the existing cybercrime knowledge which was in need of better understanding of hacker's motivations and the applicability of traditional theories of crime to virtual offenses (Holt and Bossler 2014).

Because negative emotions influence the way nerves are managed, emotions are better controlled in the presence of shunting or minimization techniques. This is because offenders will try to escape reality and try to minimize or shed their negative thoughts and emotions. Parallel to that process, as suggested by RAT, crime is the result of an opportunity, in which the motivated offender will create Plan B and will use his/her thrill and lens widening techniques to control the fear. As a result, they will be better able to manage their nerves. That is, hackers are weighing costs and benefits and use the suitable technique to reduce and minimize the negative outcomes in their minds. However, the hackers are deluding themselves somewhat as in reality they are operating with 'bounded rationality' influenced by emotions, and do not fully rationally calculate costs and benefits. This process results in unconscious decisions that downplay the risks and increase benefits, such as: "there is no big risk in getting caught"; "Plan B exists and will save me if I get into trouble"; or, "This is a small act that I'm doing…it's no big deal in reality." This sheds light on the inner motivational states that hackers are going through, when trying to manage their nerves more effectively.

Our research thus offers valuable new insights on the psychological reasoning in the hacker's decision-making process, during their crime life cycle. By using different techniques, hackers are indirectly trying to convince themselves that their acts, which are digital crimes, are not as important as other physical crimes (e.g., robbery). Therefore, they delude themselves into thinking that the inherent risks cannot be the same and should not be seen in the same way. This is an important insight, since it suggests that the seriousness of their acts is not clearly understood, communicated, or explained. Notably, we contribute to having a clearer understanding of a hacker's cognitive profile, which should contribute to a better understanding of hacker's criminal actions and behaviors. Although, this may not be the perfect representation of the black hat hacker as even within the same hacking group there are notable differences in their skills and abilities to conduct hacking (Holt and Bossler 2014; Holt et al. 2012) our study provides some initial insights into psychological structure of hacker's motivational states.

Notably, some of the interviewees eventually recognized the gravity of their acts, but only after having negative experiences with the police. We thus argue that policy makers (e.g., government officials, legal and justice system policy makers) should learn from this when building and defining criminal laws in respect to hacking. Part of the issue here is that authorities need to change the calculus that hackers apply to their nerve management, such that they see greater risk and fear, and thus are less likely to have the nerve to go through with the act. Here, broadly warning and communicating potential hackers of specific and severe consequences for specific types of hacking, versus vague consequences would be a step forward. Crucially, this communication needs to be reframed from the typical obscure legalese of lawyers to the actual language used by hackers.

For these reasons, they should try to better communicate not only the risks for hackers, but also the harm of the hackers' acts for their victims —not only for companies but also for people's lives whose data is exploited (such as their privacy and identity theft). Moreover, they should communicate the monitoring and policing efforts they are doing, especially on the dark Web, to increase a sense of 'guardianship' to decrease

the hacker's belief they are anonymous and cannot get caught, or that if they do get caught it will actually be a 'big deal.' Better communication and sensibility toward the hacking community should thus create positive effects in mitigating hacker's criminal objectives and goals. Education can be leveraged in which ex- black hat hackers could be used to spread the message and teach new and existing hackers on the possible consequences of their crimes. Highlighting the fact that there are small or large acts, could be one opportunity to be explored by the policy makers. It would strengthen the message that no matter how small the financial impact can be, the hacking crime can have similar consequences in terms of the sanctions and punishment, as the other types of crimes. Also, policy makers need to understand this activity as more than mere "hacking" but understand it can involve identity theft, stolen currency, disabling mission-critical systems that not only can lead to devasting economic consequences but can threaten human life (e.g., traffic control systems, industrial control systems, utility systems, military systems.

Furthermore, it is important to explain to hackers that their Plan B is not what they think of. In reality, Plan B is usually going to prison or paying high fines. Interestingly, this area of justice system was highlighted by Holt and Bossler (2014) as being one of the important areas that should provide more insights on how the courts and correctional system should react when confronted to cybercrime situations. In particular, Plan B, in this context, should be correctly positioned within the correctional system to account for the recent evolution and past experiences of offending through technological means. Further understanding of this relationship of two opposite sides, offender vs justice system, we could further "understand how the larger criminal justice system is responding to cybercrimes at all levels" (Holt and Bossler 2014, p. 34).

Moreover, this improved communication can come from those who actively manage and protect servers. The calculus is clearly different in considering hacking a Pentagon computer versus the Web site of a small-town newspaper. Here, perceptions of the strength of the US government may be just as important as the actual strength of the guardianship and technologies involved protecting the computers. Thus, one approach for lesser-known entities would be to leverage the reputation and explicitly communicate the guardianship of a better-known entity (e.g., IBM, Oracle).

Future research could further extend our initial findings on the importance of hackers managing their nerves and fear in such a way that future studies could, for example, study the passage from black hat (illegal) crimes to white hat (ethical hacking) activities. This could provide some new insights on how the hacker's inner psychological motivations are driven and what motivates them to become good one day. Our research is also limited by the fact that we could not verify with 100% certainty that the hackers we interviewed are who they pretend to be; however, we did conduct ethnographic observations to verify the participants' hacker identity and their behaviors as 'black hat.' Unfortunately, we could not collect any detailed demographics about the interviewees, due to the nature of their activities. This is a substantial challenge when studying any serious criminal behavior. Another challenge relates to the actual definition of the black hat hacker. Although provide a definition in this paper, in reality, the definition of who exactly is and is not a black hat hacker is a challenging topic that is not easy to address. Finally, as motivations of black hat hackers can be different ones ranging from state-sponsored attacks to hacktivism, the way their nerve is managed can also be impacted differentially. For example, if a black-hat hacker is supported by a State and a large group of professional hackers, their nerve management calculus is going to be quite different than for a lone black-hat hacker. Thus, future research should look at nerve management for these different kinds of motivations.

Overall, in this research, we have investigated the theoretical importance of nerve management in the unique hacking decision-making offender context. We contribute to the current state of cybercrime scholarship by providing new theoretical insights into the complex psychological and motivational reasoning behind hacking illegal activities. In particular, we identified five cognitive and presentational tactics that black hat hackers use to shape their nerve management. This has important implications on how the perception of threat is managed and provides important insights on why hacking, as one type of the crime, is differently approached and management from emotional and fear perspectives when compared to more traditional crime contexts (e.g., street crime). These insights provide valuable insights to different stakeholders (e.g., legal and justice system) which should benefit from our findings as it suggests how fear, and consequently nerve, is managed in the unique hacking context.

5 Conclusion

Our study investigated how black hat hackers manage their nerves when conducting crime activities. We identified five techniques they use: shunting, minimization, Plan B, thrill, and lens widening techniques. Each of these techniques helps hackers to better manage their nerves and consequently, learn how live with their fear. During their psychological decision-making processes, hackers turn to these five techniques to create a new mindset. It allows them to hide with the objective of minimizing and mitigating the inherent risks they incur during their criminal activities.

Appendix 1: Interview Guideline

Introduction

The interview will not take more than 1 h. I will be recording the session because I don't want to miss any of your comments. All comments and responses will be kept strictly confidential which means that your responses will be shared only with research team members and will ensure that any information from the report does not identify you as the respondent. Do you have any questions at this stage?

Introductory questions

1. Can you tell us your name (hacker nickname), gender and age?
2. Can you briefly describe who you are and when you started to hack?
3. Can you confirm which type of hacker you are and what does that mean to you?

About Hacking

4. Can you provide more information your hacking debuts and how did you learn?
5. What motivates you to hack? What attracted you to black hat hacking?
6. Is what you do illegal?
7. What is the scope of your hacking activities? On which online sites (e.g., forums) you are active?

Hacking vs Fear

8. What is your perception regarding risks behind hacking activities? Please explain.
9. How do you see the criminal side related to your activities? Please explain.
10. Do you worry about being apprehended? Please explain.
11. Do you have any backup plans? Please explain.
12. Do you have any bad feelings when hacking? Please explain.
13. How do you manage your fear? Please explain.

Outlook / Interview Closing

14. What are the challenges in doing the hacking job? Please explain.
15. How do you see your future in hacking? Please explain.

Interview closing

a) Would you like to add anything else?
b) If not, I will analyze all information provided together with other interviews in the following weeks and would be happy to send you a copy to review if you are interested. Thank you very much for your time!

General probes used during the Interview

- Would you give me an example?
- Can you elaborate on that idea?
- Would you explain that further?
- I'm not sure I understand what you're saying.
- Is there anything else?

References

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology, 30*(1), 47–88.

Agnew, R. (1999). A general strain theory of community differences in crime rates. *Journal of Research in Crime and Deliquency, 36*(2), 123–155.

Anderson, E. (2000). *Code of the street: Decency, violence, and the moral life of the inner city*. New York, NY: WW Norton & Company.

Bandura, A., & Walters, R. H. (1977). *Social learning theory*. New York, NY: General Learning Press.

Baron, S. W. (2004). General strain, street youth and crime: A test of Agnew's revised theory. *Criminology, 42*(2), 457–484.

Barriga, A. Q., & Gibbs, J. C. (1996). Measuring cognitive distortion in antisocial youth: Development and preliminary validation of the "how I think" questionnaire. *Aggressive Behavior, 22*(5), 333–343.

Beccaria, C. (2009). *On crimes and punishments and other writings*. Toronto Buffalo, London: University of Toronto Press.

Benjamin, V., Li, W., Holt, T., & Chen, H. (2015). *Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops*. Paper presented at the 2015 IEEE international conference on intelligence and security informatics (ISI), Baltimore, MD, USA.

Benjamin, V., Zhang, B., Nunamaker, J. F., Jr., & Chen, H. (2016). Examining hacker participation length in cybercriminal internet-relay-chat communities. *Journal of Management Information Systems, 33*(2), 482–510.

Benjamin, V., Valacich, J., & Chen, H. (2019). DICE-e: A framework for conducting darknet identification, collection, evaluation with ethics. *MIS Quarterly, 43*(1), 1–22.

Blackburn, R. (1993). *The psychology of criminal conduct: Theory, research and practice*. Oxford, England: John Wiley & Sons.

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law, 24*(2), 229–251.

Charmaz, K. (1990). 'Discovering'chronic illness: Using grounded theory. *Social Science & Medicine, 30*(11), 1161–1172.

Cherbonneau, M., & Copes, H. (2006). 'Drive it like you stole it': Auto theft and the illusion of normalcy. *British Journal of Criminology, 46*(2), 193–211.

Cisco. (2018). 2018 Annual Cybersecurity Report. Retrieved from https://www.cisco.com/c/en/us/products/security/security-reports.html. Accessed 13 Jan 2018

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Corbin, J., & Strauss, A. (2008). Basics of qualitative research: Techniques and procedures for developing grounded theory. In *London: Thousand oaks*. CA: Sage.

Cornish, D. B., Clarke, R. V., & Wortley, R. (2008). *The rational choice perspective* (Vol. 21). Cullompton, UK: Willan Publishing.

Crooks, D. L. (2001). The importance of symbolic interaction in grounded theory research on women's health. *Health Care for Women International, 22*(1–2), 11–27.

Cross, T. (2006). Academic freedom and the hacker ethic. *Communications of the ACM, 49*(6), 37–40.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101.

Cusson, M. (1993). Situational deterrence: Fear during the criminal event. *Crime Prevention Studies, 1*, 55–68.

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal, 29*(1), 43–69.

Davis, R. W., & Hutchison, S. C. (1997). *Computer crime in Canada: An introduction to technological crime and related legal issues*. Canada: Carswell Legal Publications.

Deci, E. L., & Ryan, R. M. (2010). *Self determination theory Corsini Encyclopedia of Psychology*. Online: Wiley Online Library.

EY. (2018). 21st EY Global Information Security Survey. Retrieved from https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf

Ferraro, K. F., & Grange, R. L. (1987). The measurement of fear of crime. *Sociological Inquiry, 57*(1), 70–97.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. New York, NY: Elsevier New York.

Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime*: Stanford University press.

Groff, E. R. (2008). Adding the temporal and spatial aspects of routine activities: A further test of routine activity theory. *Security Journal, 21*(1–2), 95–116.

Hochstetler, A. (2001). Opportunities and decisions: Interactional dynamics in robbery and burglary groups. *Criminology, 39*(3), 737–764.

Hochstetler, A. (2002). Sprees and runs: Opportunity construction and criminal episodes. *Deviant Behavior, 23*(1), 45–73.

Holt, T. J. (2009). *The attack dynamics of political and religiously motivated hackers*. NewYork: Paper presented at the Cyber Infrastructure Protection.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40.

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology, 6*(1), 891–903.

Hu, Q., Zhang, C., & Xu, Z. (2011). *How can you tell a hacker from a geek? Ask whether he spends more time on computer games than sports*. Blacksburg, Virginia: Paper presented at the DeWald Information Security Research Workshop.

Jacobs, B. A., & Cherbonneau, M. (2017). Nerve management and crime accomplishment. *Journal of Research in Crime and Delinquency, 54*(5), 617–638.

Kallman, E. A., & Grillo, J. P. (1998). *Ethical decision making and information technology: An introduction with cases*. Collingdale: DIANE Publishing Company.

Katz, J. (1988). *Seductions of crime: Moral and sensual attractions in doing evil*. New York, NY: Basic Books.

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security and Privacy, 4*(1), 33–39.

Leeson, P. T., & Coyne, C. J. (2005). The economics of computer hacking. *JL Econ. & Pol'y, 1*, 511.

Levy, S. (2001). *Hackers: Heroes of the computer revolution* (Vol. 4). New York, NY: Penguin Books New York.

Lichstein, H. (1963). Telephone Hackers Active. *The Tech, 43*(20), 20.

Lowry, P. B., Zhang, J., Wang, C., & Siponen, M. (2016). Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning (SSSL) model. *Information Systems Research, 27*(4), 962–986.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the Centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546–563.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS Quarterly, 34*(3), 431–433.

Parks, R., Xu, H., Chu, C.-H., & Lowry, P. B. (2017). Examining the intended and unintended consequences of organisational privacy safeguards enactment in healthcare. *European Journal of Information Systems, 26*(1), 37–65.

Patchin, J. W., & Hinduja, S. (2011). Traditional and nontraditional bullying among youth: A test of general strain theory. *Youth & Society, 43*(2), 727–751.

Phukan, S. (2002). *IT ethics in the internet age: New dimensions. Paper presented at the proceedings of informing*. Cork, Ireland: Science & IT Education Conference.

Probasco, J. R., & Davis, W. L. (1995). A human capital perspective on criminal careers. *Journal of Applied Business Research, 11*(3), 58.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216–238.

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation, 3*(2), 97–102.

Schell, B. H., & Dodge, J. L. (2002). *The hacking of America: Who's doing it, why, and how*. Westport, CT, USA: Greenwood Publishing Group Inc..

Schell, B. H., & Holt, T. J. (2009). *A profile of the demographics, psychological predispositions, and social/behavioral patterns of computer hacker insiders and outsiders Online consumer protection: Theories of human relativism (pp. 190–213)*. Online: IGI Global.

Shin, J., & Milkman, K. L. (2016). How backup plans can harm goal pursuit: The unexpected downside of being prepared for failure. *Organizational Behavior and Human Decision Processes, 135*, 1–9.

Skinner, B. F. (1972). *Beyond freedom and dignity*. New York: Bantam Books.

Smith, A. D., & Rupp, W. T. (2002). Issues in cybersecurity; understanding the potential risks associated with hackers/crackers. *Information Management & Computer Security, 10*(4), 178–183.

Strauss, A., & Corbin, J. (1994). Grounded theory methodology. *Handbook of Qualitative Research, 17*, 273–285.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664–670.

Teske, N. (1997). Beyond altruism: Identity-construction as moral motive in political explanation. *Political Psychology, 18*(1), 71–91.

The-Honeynet-Project. (2004). *Know your enemy: Learning about security threats*. Boston, Massachusetts: Addison-Wesley Professional.

Topalli, V., & Wright, R. (2013). Affect and the dynamic foreground of predatory street crime *Affect and cognition in criminal decision making* (Vol. 42). New York, NY.

Turgeman-Goldschmidt, O. (2005). Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review, 23*(1), 8–23.

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology, 2*(2), 382.

Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the 'theory'back into grounded theory: Guidelines for grounded theory studies in information systems. *Information Systems Journal, 20*(4), 357–381.

Vaughan-Nichols, S. J. (2018). Your website is under constant attack. Retrieved from https://www.zdnet.com/article/your-website-is-under-constant-attack/. Accessed 13 Jan 2019

Wall, J. D., Lowry, P. B., & Barlow, J. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems, 17*(1), 39–76.

Warr, M. (2000). Fear of crime in the United States: Avenues for research and policy. *Criminal Justice, 4*(4), 451–489.

Wikström, P.-O. H. (2004). Crime as alternative: Towards a cross-level situational action theory of crime causation. *Beyond Empiricism: Institutions and Intentions in the Study of Crime, 13*, 1–37.

Wikström, P.-O. H. (2006). *Individuals, settings, and acts of crime: Situational mechanisms and the explanation of crime*. New York: Cambridge University Press.

Willison, R., & Lowry, P. B. (2018). Disentangling the motivations for organizational insider computer abuse through the rational choice and life course perspectives. *The DATA BASE for Advances in Information Systems, 49*(April), 81–102.

Willison, R., Lowry, P. B., & Paternoster, R. (2018). A tale of two deterrents: Considering the role of absolute and restrictive deterrence in inspiring new directions in behavioral and organizational security. *Journal of the Association for Information Systems, 19*(12), 1187–1216.

Wilson, J. Q. (2003). *Broken windows: The police and neighborhood safety James Q. Wilson and George L. Kelling Criminological Perspectives: Essential Readings (Vol. 400, pp. 29038)*. London: SAGE.

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal of Crime and Justice, 44*(4), 387–399.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management, 24*(4), 281–287.

Mario Silic is a post-doctoral researcher at the Institute of Information Management, University of St. Gallen, Switzerland. He holds a Ph.D. from University of St Gallen, Switzerland. His research motivation focuses on the fields of information security, open source software, human-computer interaction and mobile. He has published research in Journal of Management Information Systems, Security Journal, Information & Management, Computers & Security, Computers in Human Behavior, and others.

Paul Benjamin Lowry is the Suzanne Parker Thornhill Chair Professor and Eminent Scholar in Business Information Technology at the Pamplin College of Business at Virginia Tech. He is a former tenured Full Professor at both City University of Hong Kong and The University of Hong Kong. He received his Ph.D. in Management Information Systems from the University of Arizona and an MBA from the Marriott School of Management. He has published 220+ publications, including 120+ journal articles in MIS Quarterly, Information Systems Research, J. of MIS, J. of the AIS, Information System J., European J. of Information Systems, J. of Strategic IS, J. of IT, Decision Sciences J., Information & Management, Decision Support Systems, and others. He is a department editor at Decision Sciences J. He also is an SE at J. of MIS, J. of the AIS, and Information System J., and an AE at the European J. of Information Systems. He has also served multiple times as track co-chair at ICIS, ECIS, and PACIS. His research interests include (1) organizational and behavioral security and privacy; (2) online deviance, online harassment, and computer ethics; (3) HCI, social media, and gamification; and (4) business analytics, decision sciences, innovation, and supply chains.