March 2021

Self-Protection in Cyberspace: Assessing the Processual Relationship Between Thoughtfully Reflective Decision Making, Protection Motivation Theory, Cyber Hygiene, and Victimization

C. Jordan Howell
University of South Florida

Scholar Commons Citation

Howell, C. Jordan, "Self-Protection in Cyberspace: Assessing the Processual Relationship Between Thoughtfully Reflective Decision Making, Protection Motivation Theory, Cyber Hygiene, and Victimization" (2021). *Graduate Theses and Dissertations.*
https://scholarcommons.usf.edu/etd/8794

Self-Protection in Cyberspace: Assessing the Processual Relationship Between Thoughtfully Reflective Decision Making, Protection Motivation Theory, Cyber Hygiene, and Victimization

by

C. Jordan Howell

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Department of Criminology
College of Behavioral and Community Sciences
University of South Florida

Major Professor: George W. Burruss, Ph.D.
John K. Cochran, Ph.D.
Richard K. Moule, Jr. Ph.D.
David Maimon, Ph.D.

Date of Approval
March 23, 2021

Keywords: Cybercrime, Cybersecurity; Situational Crime Prevention; Target Hardening, Theoretical Integration, Rational Choice

Table of Contents

List of Tables

List of Figures

Abstract

The current study, using structural equation modeling, assesses the processual relationship between thoughtfully reflective decision making (TRDM), theoretical constructs derived from protection motivation theory (PMT), cyber hygiene, and online victimization to determine the cognitive decision-making process that leads to the adoption of online self-protective behaviors, which reduces the occurrence of victimization experiences. Findings, derived from a general sample of Internet users in the United States, reveal: (1) engagement in cyber hygiene practices, as a form of target hardening, decreases Internet users' experiences with online victimization; (2) thoughtfully reflective decision makers, in the face of cyber threats, develop higher threat appraisals and coping appraisals (i.e., perceived response efficacy); (3) Internet users' threat appraisals and perceived response efficacy increase engagement in cyber hygiene practices; and (4) TRDM directly, and indirectly through Internet users' threat appraisals and perceived response efficacy, increases engagement in cyber hygiene practices.

Results presented in the current study aid theoretical development in the field of criminology by: (1) demonstrating the effectiveness of target hardening practices (i.e., cyber hygiene) at reducing online victimization experiences; (2) expanding the scope of TRDM by demonstrating the theoretical construct's predictive efficacy on the adoption of online self-protective behaviors, an endogenous variable of widespread importance in the information security literature; and (3) integrating interrelated propositions from TRDM and PMT to provide a more robust theoretical model capable of predicting self-protection in cyberspace. Finally, the current study provides policy makers the information needed to configure the cyber-environment in a manner that will promote self-protection and decrease the frequency of cybercrime incidents.

Chapter One:
Introduction

Cybercrime costs the global economy billions of dollars annually (McAfee, 2017). Additionally, and in accordance with a report by Ponemon Institute (2016), 98% of organizations surveyed experience malware attacks, 70% experience phishing attacks, and 63% experience web-based attacks. Individual Internet users are also greatly affected by cybercrime. In the United States, over 800 cybercrime incidents are reported to the Internet Crime Complaint Center (2019) on any given day, and due to underreporting (Bidgoli & Grossklags, 2016), this is likely an underestimate of the true number of incidents that occur. In addition to the crimes reported, a recent report by the Center for Strategic and International Studies (2018), a nonprofit policy research organization, found that cyber-criminals make 80 billion daily automated network scans in attempt to identify vulnerable targets, which resulted in the loss of over 11 billion records since 2005 (PRCH, 2017). Regardless the metric or report used, it is evident that cyber-attacks against individuals are on the rise (IC3, 2020) with no evidence of a downward trend (Holt, 2011) in the absence of proactive, evidence-based mitigation efforts (Maimon & Louderback, 2019).

Understanding the behavioral patterns of the individuals constituting the cyber-environment is the first step in developing evidence-based policies and strategies aimed to protect Internet users. Within the cyber-environment exists a symbiotic relationship between offenders, guardians, targets, and enablers (Maimon & Louderback, 2019). The above statistics demonstrate that guardians (i.e., the cybersecurity industry and law enforcement agencies) are unable to protect Internet users (i.e., targets) from motivated offenders. Thus, Internet users are largely responsible for their own self-protection. Fortunately, behavioral factors have been identified that can minimize the risks associated with Internet connectivity.

The amalgamation of these behavioral safeguards is referred to as cyber hygiene (Cain et al., 2018; Vishwanath et al., 2020). Cyber hygiene is the online analogue of physical personal hygiene (Vishwanath et al., 2020). Like physical personal hygiene which aids in preventing viruses and infectious diseases that negatively impact an individual's health, cyber hygiene aids in preventing viruses and other infections which negatively impact an individual's Internet connected devices. Thus, cyber hygiene can be viewed as a set of best practices that promote self-protection in the cyber-environment. Although multiple studies have demonstrated the effectiveness of some of the behavioral safeguards that constitute cyber hygiene (Bossler & Holt, 2009; Choi, 2008; Holt & Bossler, 2013; Levesque et al., 2013, 2016; Wilsem, 2013), no known study directly tests whether cyber hygiene reduces Internet users' experiences with victimization.

Additionally, it is unclear why some individuals choose not to adopt good cyber hygiene practices despite their purported effectiveness at reducing susceptibility to online victimization (Cain et al., 2018; Fedler et al., 2013). Developing a theoretical model capable of predicting engagement in self-protection is an area of academic inquiry with widespread theoretical and practical importance that spans across sub-field boundaries. Findings from the situational crime prevention (SCP) literature demonstrate that simple behavioral modifications aimed at increasing self-protection can decrease the amount of victimization experienced by more than 50% (Clarke, 1995). For example, simple acts of target hardening such as installing anti-virus software can be used to mitigate 90% of incoming threats against an Internet connected device (Fedler et al., 2013). Thus, if individuals can be nudged to adopt target hardening practices such as cyber hygiene, or if target hardening is automated through environmental modifications (Newman, 1972), fewer criminal incidents will transpire due to blocked opportunities (Clarke, 1980). The adoption of computer security behaviors and victimization are focal to the information security and criminological literatures, respectively. Since the decision to engage, or not to engage, in computer security behaviors temporally precedes victimization (albeit a reciprocal effect likely exists) a theoretical model capable of predicting self-protection could be used to identify those most susceptible to victimization and nudge them to make higher quality decisions that ensure their safety. Therefore, criminologists should devote greater attention to developing such a model (Clubb & Hinkle, 2015; Ireland, 2020).

Engagement in cyber hygiene practices is a choice. Internet users must intentionally and consciously decide to adopt, or not adopt, the behavioral safeguards that constitute cyber hygiene. Since these behavioral safeguards have shown to be effective in thwarting victimization attempts (Fedler et al., 2013), engaging in cyber hygiene practices can be considered a good, or quality decision (Paternoster & Pogarsky, 2009). Determining why some individuals make quality decisions, while others do not, has been of interest to rational choice scholars for hundreds of years (Beccaria, 1764).

The rational choice approach operates on the assumption of human agency (McCarthy, 2002) and, resultingly, rational choice scholars treat individuals as decision makers who make choices and impose those choices on the world (Nagin, 2007). Decisions are considered rational when they correspond with the decision maker's preferences for outcomes (McCarthy, 2002; Nagin, 2007). However, not all decision makers are equally equipped in their capacity to act in accordance with their preferences or make conventionally "good" decisions (Paternoster & Pogarsky, 2009). On average, persons vary in their ability to collect and analyze information, weigh the costs and benefits of outcome alternatives, and make a decision that results in the desired outcome.

Recognizing that not all actions are rational (McCarthy, 2002) and that not all individuals are equally capable of making decisions that result in desirable outcomes (Baron, 2008), Paternoster and Pogarsky (2009) introduced the theory of thoughtfully reflective decision making (TRDM). TRDM describes the process of quality decision making and is defined as the "tendency of persons to collect information relevant to a problem or decision they must make, to think deliberately, carefully, and thoughtfully about possible solutions to the problem, apply reason to the examination of alternative solutions, and reflect back upon both the process and the outcome of the choice in order to assess what went right and what went wrong" (Paternoster & Pogarsky, 2009, p. 104-105). In essence, Paternoster and Pogarsky (2009) contended that behavioral outcomes, both conventional and criminal, are a function of TRDM. The few tests of TRDM that have been conducted find support for this claim. Specifically, thoughtfully reflective decision makers have been found to make decisions that enhance their human, social, and cultural capital (Paternoster et al., 2011), reduce their involvement in criminal and delinquent behavior (Maimon et al., 2012; Paternoster & Pogarsky, 2009), and decrease their susceptibility to online victimization (Louderback & Antonaccio, 2017). Additionally, and in direct relevance to the current study, Howell et al. (2021) found that thoughtfully reflective decision makers are more likely to adopt online self-protective behaviors. Although the authors failed to consider the cognitive mediating process that underlies this nexus, they alluded to a processual relationship in which TRDM operates through protection motivation theory (PMT) constructs to explain variation in Internet users' adoption of online security behaviors.

In accordance with PMT, the threat of a potential negative outcome triggers two independent parallel cognitive processes: threat appraisals and coping appraisals. The stronger the appraisals, the higher one's protection motivation, and thus the more likely an individual is to adopt the behavioral recommendation(s) (Rogers, 1975; 1983). Threat appraisals result in more protection motivation when individuals believe the threat of a potential negative outcome (i.e., severity and vulnerability) outweighs the maladaptive reward(s) of not adopting the recommended behavior(s) (Boss et al., 2015). Coping appraisals result in more protection motivation when an individual has faith in the behavioral recommendation(s) proposed to thwart the occurrence of a negative outcome (i.e., response efficacy) and their own ability to carry out the recommendation(s) (i.e., self-efficacy), but does not perceive the response cost associated with adopting the recommendation(s) to be too high.

Thus, loosely put, PMT is a cost-benefit model where risks associated with experiencing a negative outcome are compared to the costs of trying to prevent the negative outcome from occurring (Rogers, 1983; Sommestad et al., 2015). In a recent review of the literature, Sommestad et al. (2015) found overwhelming support for PMT in predicting both intent to adopt, and actual adoption of, computer security behaviors. However, since persons vary in their cognitive decision-making capabilities, and since thoughtfully reflective decision makers, on average, make decisions that result in better outcomes (e.g., less online victimization (Louderback & Antonaccio, 2017)), the cost-benefit analysis depicted in PMT may be a function of TRDM.

Taken together, TRDM and PMT both seem to predict online self-protective behaviors, but the true nature of the relationship between TRDM, PMT, and cyber hygiene is unclear. As noted above, Howell and colleagues (2021) alluded to a processual relationship in which the effect of TRDM on the adoption of online self-protective behaviors is mediated by theoretical constructs derived from PMT. Importantly, they failed to test the processual relationship between TRDM, PMT, and the adoption of online self-protective behaviors. Moreover, they neglected to observe whether the adoption of self-protective behaviors reduces Internet users' probability of experiencing online victimization.

To address these shortcomings, the current study seeks to parse out the processual relationship between TRDM, PMT, cyber hygiene, and victimization. After demonstrating that cyber hygiene is associated with a decrease in Internet users' likelihood of experiencing victimization, a newly developed theoretical model designed to explain variation in Internet users' adoption of self-protective behaviors is empirically evaluated. Specifically, structural equation modeling is used to assess the direct effects of TRDM and PMT constructs on the adoption of cyber hygiene practices in addition to the indirect effects of TRDM on the adoption of cyber hygiene practices through PMT constructs. Through the cross-disciplinary, end-to-end integration (Liska et al., 1989) of TRDM and PMT, which have both shown to be relevant predictors of online self-protective behaviors (Howell et al., 2021; Sommestad et al., 2015), the current study serves as an attempt to develop a more robust theoretical model capable of explaining why some individuals fail to adopt recommended self-protective behaviors (i.e., cyber hygiene) in the face of cyber threats despite their now proven effectiveness at reducing victimization experiences.

Chapter Two:
Literature Review

The current study has two primary objectives: (1) determine whether engagement in cyber hygiene practices reduces Internet users' online victimization experiences, and if so, (2) develop a theoretical model capable of explaining why some individuals fail to adopt good cyber hygiene practices despite their now proven effectiveness at reducing victimization experiences. This chapter provides literature relevant to the first objective and is divided into three sections: patterns of victimization, situational crime prevention and target hardening, and cyber hygiene. The first section provides a detailed overview of the victimization literature, drawing heavily from routine activity theory (RAT). Within this section, it is argued that offenders, who seek to maximize pleasure while minimizing pain (Becker, 1968), choose targets deemed as suitable and lacking capable guardianship (Cohen & Felson, 1979). The second section outlines the crime prevention methods inherent within situational crime prevention (SCP) (Clarke, 1980; 1983; 1995; Cornish & Clarke, 2003) and posits target hardening as an effective approach to reduce Internet users' victimization experiences. Specifically, it is argued that target hardening practices simultaneously increase capable guardianship and decrease target suitability by reducing motivated offenders' opportunities to engage in crime. Finally, the third section provides a conceptual overview of cyber hygiene and contends that good cyber hygiene is synonymous with target hardening in the cyber-environment (Cain et al., 2018; Maennel et al., 2018). The chapter concludes by documenting notable gaps within the literature the current study seeks to fill.

Patterns of Victimization

Victimization occurs when motivated offenders, suitable targets, and the absence of a capable guardian converge in time and space (Cohen & Felson, 1979). Rooted in the rational choice paradigm, which is discussed in depth in the following chapter, Cohen and Felson (1979) developed RAT in attempt to explain increased burglary rates in post-World War II society. Cohen and Felson (1979) argued that routine behavior changed within the United States as more women gained employment outside of the home and as innovations in technology produced expensive and portable appliances (e.g., televisions, radios, etc.). This societal change in daily routines connected motivated offenders with suitable targets (e.g., items that are expensive and portable) while simultaneously limiting the availability of capable guardianship. In accordance with RAT, the convergence of these three elements (i.e., motivated offenders, suitable targets, and the absence of a capable guardian) in time and space leads to crime

Most research examining the predictive efficacy of RAT presume criminal motivation is ubiquitous should the opportunity present itself and focuses on target suitability and capable guardianship, or the lack thereof (Akers et al., 2017). A suitable target is a person, location, or object that is desirable to a motivated offender and can be damaged or threatened. If a target is deemed as suitable, there is a greater chance a crime is committed to or against the target. Cohen and Felson (1979) outline the four components inherent within a suitable target: value, inertia, visibility, and accessibility. Capable guardianship refers to the capacity of a person or object to deter the motivated offender from engaging in a criminal act to or against the target or intervene during the commission of the criminal act. Although RAT was originally developed to explain macro-level trends in property crime rates (Cohen & Felson, 1979), it has since become a dominate victimology paradigm that has been successfully applied to a host of victimization patterns in both the physical world (Pratt & Cullen, 2005) and in cyberspace (Maimon & Louderback, 2019) at the macro- (Perkins et al., 2020) and micro-levels (Holt & Bossler, 2013) of analysis.

In fact, RAT is often regarded as a general theory of crime due to its proven utility in explaining various types of victimization patterns across units of analysis (Ngo & Paternoster, 2011). In the physical world, RAT has been successfully applied to multiple behaviors at the macro-level including property offenses (Cohen & Felson, 1979), assault (Mcneeley & Wilcox, 2015), robbery (Smith et al., 2000), burglary (Zhang et al., 2007), sexual offenses (Tewksbury et al., 2008), and environmental crimes (Corcoran et al., 2016). At the micro-level, RAT has been successfully applied to physical assault (Stewart et al., 2004), robbery (Spano & Nagy, 2005), burglary (Coupe & Blake, 2006), homicide (Messner & Tardiff, 1985), fraud (Holtfreter et al., 2008), sexual offenses (Mustaine & Tewksbury, 2002), vandalism (Tewksbury & Mustaine, 2000), and larceny (Mustaine & Tewksbury, 1998). The overarching implication inherent within each of these studies, and in the routine activities approach more generally, is that to reduce victimization experiences, opportunities conducive to crime must be restricted by increasing guardianship and/or decreasing target suitability (Clarke, 1983). This remains true in both offline and online environments (Maimon & Louderback, 2019).

Patterns of Online Victimization

The relevance of RAT in explaining victimization patterns in cyberspace has been a point of discourse in the cyber-criminological literature (Reyns et al., 2011; Yar, 2005). Based on the assertion the cyber-environment is ‘anti-spatial’ (Mitchell 1996, 8) and lacks temporal ordering, Yar (2005) contended the “spatio-temporal ontologies” of virtual and non-virtual environments are distinctly different (p. 414). To that end, Yar (2005) argued motivated offenders, suitable targets, and the absence of a capable guardian are unable to converge in cyberspace in a fashion consistent with the RAT framework. However, Reyns et al. (2011) convincingly argued that these three elements can and do converge via networked systems. In other words, the configuration of the cyber-environment facilitates the convergence of victims and offenders irrespective of their geographic location (Maimon & Louderback, 2019).

Despite this debate, RAT is among the most widely tested criminological theories in cyberspace, with most studies finding moderate support for the theory (Maimon & Louderback, 2019) at both the macro- (Perkins et al., 2020) and micro-levels of analysis (Holt & Bossler, 2013). At the macro-level, researchers have found that victimization patterns are a function of the routine activities of Internet users. For example, Maimon et al. (2013) found that cyber-attacks launched against university networks occur most frequently during business hours, which they attribute to the increased visibility and accessibility of potential targets. Additionally, Song, Lynch, and Cochran (2015) found that Internet user behavior across States (within the United States) can be used to predict cyber-victimization patterns in a manner consistent with the theory.

The RAT framework also provides an explanation for cyber-victimization patterns at the country-level. For example, Howell et al. (2019) found that attacks against websites are less likely to occur against countries that demonstrate the presence of capable guardianship (i.e., strong military presence) and more likely to occur when some criteria of target suitability are met. Specifically, attacks against websites occur more frequently in Asian nations and in nations with computer vulnerabilities that can be exploited by the hacker. Additionally, Holt, Burruss, and Bossler (2018) found increased target suitability (i.e., technological infrastructure, political freedom, and less organized crime) resulted in an increase in reports of malware infections cross-nationally. Furthermore, Kigerl (2012) found that wealthier nations (as a result of target suitability) experience higher amounts of phishing and spam. Corroborating these findings, Perkins et al. (2020) found multiple indicators of target suitability are predictive of the amount of malicious spam a country receives.

Similar trends emerge when applying the RAT framework to cyber-victimization patterns at the individual-level. The majority of studies find that offenders, who seek to maximize pleasure while minimizing pain (Becker, 1968), choose targets deemed as suitable and lacking capable guardianship (Bossler & Holt, 2009; Choi, 2008; Choi & Lee, 2017; Holt & Bossler, 2013; Marcum et al., 2010; Pratt et al., 2010; Van Wilsem, 2011; Wilsem, 2013). For example, capable guardianship decreases the likelihood of computer infection (Choi, 2008; Holt & Bossler, 2013), data loss (Bossler & Holt, 2009), and hacking victimization (Wilsem, 2013); whereas target suitability increases the likelihood of experiencing consumer fraud (Pratt et al., 2010), online threats (Van Wilsem, 2011), computer infection (Choi, 2008), online harassment (Holt & Bossler, 2009; Marcum et al., 2010), and interpersonal violence (Choi & Lee, 2017).

Taken together, the aforementioned studies demonstrate that offenders choose targets deemed as suitable and lacking adequate protection (i.e., capable guardianship). Since law enforcement officers (Burruss et al., 2019) and the cybersecurity industry (Holt, 2011; IC3, 2020; Maimon & Louderback, 2019; McAfee, 2017; Ponemon Institute, 2016) have proven ineffective in their role as guardians, Internet users (i.e., potential targets (Maimon & Louderback, 2019)) are tasked with their own self-protection (Maimon et al., 2020). As noted above, self-protection entails restricting opportunities conducive to victimization by increasing guardianship and/or decreasing target suitability (Clarke, 1983). In accordance with the SCP perspective, and as stated by Clarke (1983), “the most obvious way to reduce criminal opportunities is to obstruct or target harden” (p. 241). In other words, to decrease the probability of being victimized, Internet users should engage in acts of “target hardening” (Clarke, 1983) by applying self-protective behaviors (i.e., cyber hygiene) that increase the required efforts for motivated offenders to commit crimes to or against them. In the following section, SCP techniques are discussed with emphasize on the applicability and effectiveness of target hardening as a means to reduce cybercrime incidents.

Situational Crime Prevention and Target Hardening

Recognizing the ineffectiveness of the criminal justice system to detect, punish, and prevent crime, scholars such as Jeffery (1971) and Newman (1972) were working in the early 1970s toward devising environmental solutions to crime reduction. Jeffery (1971) published *Crime Prevention Through Environmental Design*, which argued the criminal justice system should be more proactive in its approach to curtail criminal events from occurring. Specifically, Jeffery suggested the abandonment of punishment and treatment philosophies in favor of a preventative approach geared toward manipulating the physical environment conducive to crime.

Shortly thereafter, Newman (1972) coined the term “defensible space,” which argued crime can be thwarted through architectural design. For example, grouping housing units in a manner that facilitates surveillance, establishes certain pathways for movement, and defines certain areas of activity leads residents to adopt territorial attitudes and create self-policing measures. These social and architectural alterations combine to decrease opportunities conducive to crime. These views, and the recognition of opportunity as a key component of criminal behavior, were in radical contrast to the contemporary academic climate and leading dispositional theories of the time (Clarke, 1980).

Clarke, in continuation of the event-based perspective to crime reduction, developed SCP. In essence, SCP attempts to curtail crime by manipulating the specific situational characteristics conducive to engagement (Clarke, 1980; Welsh & Farrington, 2009). Integrating rational choice models of crime (see chapter three) with the routine activities perspective (Cohen & Felson, 1979), SCP scholars believe criminal behavior can be thwarted at the event-level through blocked opportunities. Stated differently, SCP scholars (Clarke, 1980; 1983; 1995; Cornish & Clarke, 2003) recognize that victimization is patterned and predictable and that if opportunities conducive to crime are removed, a decline in criminal incidents will follow suit.

SCP suggests that offenders operate with agency: crime is a choice (Clarke, 1980) that can be altered through decreasing the rewards and increasing the pains associated with the event. Cornish and Clarke (2003) outline five categories that influence decision making: (1) increase effort, (2) increase risks, (3) reduce rewards, (4) reduce provocations, and (5) remove excuses (Clarke, 1980; 1983; 1995; Cornish & Clarke, 2003). Within each of the five categories there are five techniques that can be used to reduce the likelihood of a criminal incident (see Cornish & Clarke, 2003). Of the twenty-five techniques across the five categories, Clarke (1983) emphasizes the efficacy of one specific technique*,* "target hardening", which increases motivated offenders' efforts to engage in crime. Specifically, Clarke (1983) stated "the most obvious way to reduce criminal opportunities is to obstruct or target harden" (p. 241). Target hardening, as the name suggests, is the process of strengthening the security of a potential target by increasing the required effort to commit crimes to or against the target.

Unlike most dispositional theories of crime, SCP is especially useful in providing practical efforts to reduce offending. Moreover, SCP's crime reducing techniques are applicable to any type of crime occurring in any type of setting so long as the prevention methods are tailored to the situation (Clarke, 1995). In other words, the prevention of different crime types requires the adoption of different preventative measures. For example, the installation of steering locks on parked cars reduces an individual's likelihood of having their vehicle stolen (Webb, 1994), but does not prevent burglary from occurring inside the home.

When the correct preventative measure is applied, SCP techniques, such as "target hardening", are "highly effective" at reducing the frequency of criminal incidents (Clarke 1995, p. 17). Target hardening techniques include any effort to increase motivated offenders' perceived efforts of engaging in crime by increasing capable guardianship and/or decreasing target suitability. In the physical world, myriad target hardening techniques have been effectively used to mitigate a variety of crime types. To prevent the use of slugs in parking meters (Decker, 1972) and ticket machines (Clarke et al., 1994), for example, city officials install slug rejectors. The installation of transparent barriers reduces assaults against bus drivers (Poyner, 1993) and the number of robberies in post offices (Ekblom, 1988) and banks (Clarke et al, 1991). Target hardening techniques, such as armored doors on airplanes, have even been linked to a reduction in acts of terrorism (Clarke & Newman, 2006). Given the success of target hardening techniques at reducing various forms of crime, and the assumption that the SCP framework can be applied to all forms of crime across all settings (Clarke 1995), target hardening techniques should aid in the reduction of crimes occurring within the cyber-environment (Maimon & Louderback, 2019).

Target Hardening in Cyberspace

Advocates of the SCP approach have long recognized that technological advancements create new opportunities for crime and victimization. In fact, Clarke (2004, p. 55) noted ''The Internet has created a completely new environment in which traditional crimes—fraud, identity theft and child pornography—can take new forms and prosper.'' Moreover, Newman and Clarke (2013) outlined elements of information systems that are themselves conducive to crime using the acronym SCAREM: stealth, challenge, anonymity, reconnaissance, escape, and multiple [“multiplied”] offending. In doing so, the authors posited, “the online environment … is nothing short of criminogenic” due to cyber-offenders’ ability to launch attacks undetected, willingness to commit crimes for the sheer challenge, access to anonymizing technologies, potential for conducting reconnaissance before launching an attack, near guarantee of escape upon the commission of a crime, and potential to engage in multiple crimes simultaneously (Newman & Clarke, 2013, p. 17).

Given the criminogenic nature of the cyber-environment (Newman & Clarke, 2013) and large body of evidence demonstrating that cyber-offenders are rational actors who choose suitable targets lacking capable guardianship (Maimon & Louderback, 2019), the SCP approach appears well-suited for preventing cybercrimes (Newman & Clarke, 2013). Although criminologists have theorized how SCP can be tailored to curtail cybercrime incidents, (Anandarajan & Malik, 2018; Beebe & Rao, 2005; Denning & Baugh, 1999; Hinduja & Kooi, 2013; Harknett et al., 2010; Holt & Bossler, 2015; Martini & Choo, 2014; Newman & Clarke, 2013; Reyns, 2010; Willison & Siponen, 2009; Vidal & Choo, 2017), scant research has tested SCP in the cyber-environment (Maimon & Louderback, 2019). However, findings from various academic disciplines illustrate that cybercrime reduction can be achieved through cyber-environmental modifications and target hardening practices in a manner consistent with the theory.

Providing support for Jeffery (1971) and Newman’s (1972) assertion that opportunities conducive to crime can be reduced through architectural design, various studies have demonstrated that slight modifications to the cyber-environment alter behavioral patterns in a fashion the promotes self-protection and reduces criminal engagement. For example, Maimon et al. (2017, 2020) deployed honeypot Wi-Fi networks at various locations (i.e., coffee houses, restaurants, and hotels) across the state of Maryland and monitored the behavior of the Internet users who connected to the networks. The research team, by owning the networks, was able to view websites visited through the networks. Additionally, they gathered supplemental information pertaining to the physical environment in which the networks were deployed (e.g., number of place managers, seating arrangement, and availability of other Wi-Fi sources). Findings demonstrated that individuals were more likely to access the unsecure networks, thus putting their personal information at risk of being stolen, in establishments that did not offer legitimate public Wi-Fi and had fewer on-duty employees (i.e., place managers). Additionally, the presence of place managers increased Internet users' adoption of physical security behaviors, such as concealing a screen (Maimon et al., 2020). Modifications to the virtual environment also increased Internet users' engagement in protective behaviors. Specifically, uncertainty regarding a Wi-Fi network's legitimacy and security protocols decreased Internet users' willingness to access websites that handle sensitive information while on the network (Maimon et al., 2017). Taken together, these studies demonstrate that simple environmental modifications can change routine behavior and reduce opportunities conducive to crime.

Furthermore, a growing body of research conducted by Maimon and his colleagues (Howell et al., 2017; Maimon et al., 2014; Maimon et al., 2019; Testa et al., 2017; Wilson et al., 2015) demonstrate that hackers' perceptions of risk can be increased through automated messages threatening legal sanction, which in turn alters decision making in a manner consistent with SCP (Cornish & Clarke, 2003). Specifically, examinations of system trespasser behavior on compromised computer systems illustrate that automated warning messages that appear upon successfully infiltrating a computer system reduce the duration of system trespassing incidents (Maimon et al., 2014) and the probability of commands being typed during longer incidents involving first-time trespassers (Wilson et al., 2015). Additionally, hackers who believe they are being monitored are more likely to use clean tracks (Maimon et al., 2019) and intelligence gathering (Howell et al., 2017) commands in attempt to reduce their risk of being detected and sanctioned. These commands hide the hacker's identity and gather information about the target, respectively. Although the authors of these studies interpret the findings as supportive of restrictive deterrence (Gibbs, 1975) in cyberspace, these findings also lend support to the crime prevention properties inherent within SCP (Cornish & Clarke, 2003).

Target hardening techniques have also proven useful in preventing cyber-attacks against individuals (Levesque et al., 2013, 2016) and organizations (Back & LaPrada, 2020; Rege, 2014). At the organizational level, Rege (2014) explored the influences of affecting attacker decision-making and found attacks on power grids can be reduced by amplifying the security procedures in place (i.e., prevention and intrusion systems). At the individual-level, findings demonstrate that Internet users' engagement in recommended security behaviors can reduce various forms of victimization including, but not limited to, password cracking (Weir et al., 2010); computer infection (Choi, 2008; Holt & Bossler, 2013; Levesque et al., 2013, 2016), data loss (Bossler & Holt, 2009), and hacking victimization (Wilsem, 2013). For example, Levesque et al. (2013; 2016) used two clinical trials to assess the effectiveness of antivirus software in detecting and preventing computer infections on personal computing devices. In the first of these studies, Levesque et al. (2013) recruited 50 participants from the Université de Montréal campus, provided them with personal computing devices that were monitored by the research team, and found nearly 50% of the devices would have been infected without the installation of anti-virus software. In a follow-up study, Levesque et al. (2016) monitored nearly 27 million computer systems and found the effectiveness of anti-virus software ranges from 90% to 98%.

Taken together, would-be offenders' decisions to engage in cybercrime can be altered through decreasing the rewards and increasing the pains associated with the event (Clarke, 1980; Maimon & Louderback, 2019). The above studies demonstrate that reducing cybercrime incidents can be accomplished through modifications to the cyber-environment and through the implementation of target hardening techniques. Although preliminary evidence indicates cyber-environmental alternations can hinder system trespasser behavior at a small scale, it is unclear how generalizable these findings are to the larger cyber-offender population (Bossler, 2017). Large scale crime reduction efforts through (cyber)architectural design would require collaboration among key stake holders such as law enforcement agencies, cybersecurity companies, and cybercrime scholars to introduce an evidence-based approach to cybersecurity that considers both the human and technical elements of a cybercrime incident. Although this approach has a promising future with the advent of interdisciplinary research groups such as the Evidence-Based Cybersecurity Research Group operating out of Georgia State University, it is still in its infancy. In the absence of widespread collaborative efforts, law enforcement agencies (Burruss et al., 2019) and the cybersecurity industry (Holt, 2011; IC3, 2020; Maimon & Louderback, 2019; McAfee, 2017; Ponemon Institute, 2016) have proven to be ineffective guardians. Thus, Internet users are tasked with their own self-protection and must engage in target hardening techniques to reduce motivated offenders' opportunities to commit crimes to or against them.

Myriad target hardening techniques have been identified that decrease the occurrence of certain forms of online victimization (Cain et al., 2018). However, no singular technique can prevent all forms of online victimization. For example, preventing computer infection can be accomplished using anti-virus software (Levesque et al., 2013, 2016); whereas a strong password is necessary to protect against brute force attacks (i.e., password guessing) (Weir et al., 2010). To that end, self-protection in cyberspace requires the adoption of a multitude of target hardening techniques. Fortunately, behaviors have been identified that, when combined, afford an Internet user some level of self-protection. The amalgamation of these behavioral safe-guards can be referred to as cyber hygiene (Cain et al., 2018). Cyber hygiene, as a form of target hardening, is believed to reduce victimization experiences by increasing the amount of effort associated with engaging in crime. Stated differently, engagement in cyber hygiene practices increases capable guardianship and decreases target suitability and (Cohen & Felson, 1979), in accordance with RAT (Cohen & Felson, 1979) and SCP (Cornish & Clarke, 2003), will reduce Internet users' experiences with online victimization. The following section provides a comprehensive overview of cyber hygiene.

Cyber Hygiene

Although cyber-victimization can stem from exploited software vulnerabilities, human behavior is often considered the weakest link in cybersecurity (Sasse & Flechais, 2005). This is especially true when considering personal computing environments, which receive 95% of all cyber-attacks (Talib et al., 2010). In a personal computing environment, it is critical for users to implement self-protective behaviors because, unlike in corporate settings, users do not have a team of cybersecurity professionals monitoring and protecting their network and sensitive information. Fortunately, a multitude of target hardening practices have been identified that, when combined, can help safe-guard individuals from being victimized (Cain et al., 2018).

The amalgamation of these safeguards can be referred to as cyber hygiene. The expression "cyber hygiene" was popularized during the 2014 National Campaign for Cyber Hygiene, which was organized by the Center for Internet Security (CIS) and the Governors

Homeland Security Advisors Council (GHSAC) to promote cybersecurity as a public health issue (Maennel et al., 2018). Depicting cyber hygiene as the online analogue of personal hygiene, the campaign suggested that preventative measures can be used to mitigate cybercrime incidents much like hand washing prevents the spread of disease. Since the campaign, cyber hygiene has been applied in various contexts (Maennel et al., 2018) to describe both the human (Maybury, 2015) and technical (Mansfield-Devine, 2017) aspects of self-protection at the individual (Cain et al., 2018) and organizational (Dodge et al., 2012) level. Recognizing the inconsistencies and often contradictory usage of cyber hygiene, Maennel et al. (2018) provided a conceptual overview and formal definition to assist in achieving a universally recognized understanding of the expression.

In accordance with Maennel et al. (2018), cyber hygiene is defined as "a set of practices aiming to protect from negative impact to the assets from cyber security related risks" (p. 1). Embedded within this definition is emphasis on the human factor in risk reduction. Internet users must actively engage in routine preventative behaviors to thwart victimization attempts. Importantly, cyber hygiene varies based on the security requirements of the individual or organization. The practices required to protect a banking network differ from the practices needed to protect Internet users operating in a personal computing environment. The current study focuses on cyber hygiene at the individual-level. Thus, cyber hygiene refers to an Internet users' (i.e., end-user) adoption of self-protective practices.

Cain et al. (2018) outlined a number of cybersecurity best practices that constitute cyber hygiene, including using anti-virus software, updating software, creating and maintaining complex passwords, not sharing passwords, avoiding interacting with phishing scams, keeping personal information off social media, and not connecting to public Wi-Fi. Similar to how the adoption of personal hygiene practices does not completely eliminate the risk of contracting an infectious disease, the adoption of cyber hygiene practices cannot completely eliminate the risk of an Internet connected device becoming infected with malicious software. However, higher levels of cyber hygiene are believed to reduce victimization experiences (Cain et al., 2018).

The purpose of anti-virus software is to protect and secure Internet enabled devices and the information stored on these devices. Most anti-virus software scan files to ensure a computer system is not infected with a virus, remove infected files, and, most importantly, protect the device from being infected in the first place. Security software is readily available through for-profit cybersecurity companies such as Kaspersky, McAfee, and Norton, with a variety of free options that can be found through a quick Google search. Yet, one study found 67% of individuals surveyed did not have updated antivirus software installed on their computer (AOL/NCS, 2004).

In addition to having security software, it is imperative that individuals update the general software used on their Internet connected devices. Hackers often take advantage of known vulnerabilities in software applications, and individuals with outdated software are most susceptible to these attacks. Once a vulnerability is found, companies rush to patch the security hole by releasing updated software. Those who choose not to update their software do not receive the security patch and are thus exposed to attacks that would be otherwise ineffective.

Dawson and Stinebaugh (2010) demonstrate that weak passwords are also a major source of vulnerability. Without a strong password in place, cybercriminals can bypass other security measures by guessing (i.e., dictionary attack) the password and gaining access to the target system. A dictionary attack is a brute force attack that attempts to gain unauthorized entry into a computer system by systematically entering every word in a dictionary of common passwords (e.g., 12345 or pa$$word). Strong passwords are less likely to be included in the dictionary, and therefore help to secure a system against dictionary attacks. Although the term “strong” is relative, strong passwords are typically defined as those with random symbols, letters, and numbers (Cain et al., 2018). By using passwords with these features, it makes guessing the password more complex. However, passwords containing random symbols, letters, and numbers can be harder for a user to memorize, which can create issues for a user when attempting to access their account. For these reasons, other types of passwords (e.g., long phrases) have been suggested, but the inclusion of random symbols, letters, and numbers is still considered to be the best practice within the academic literature (Cain et al., 2018). In addition to using strong passwords, individuals should not share their password (Hoonakker et al., 2009) or use the same password for multiple accounts (Ashford, 2009). Although these recommendations have been made public, 31% of individuals use the same password for multiple accounts (Grawemeyer & Johnson, 2011), roughly one-third of users share their passwords with friends and family (Furnell, 2005), and only 71% of individuals create passwords with a special character (Cain et al., 2018).

Persons can also protect themselves online by avoiding phishing scams. Phishing is a socially engineered attack that attempts to solicit personal information through emails designed to stimulate a response from the recipient. Phishing attempts can be sent to multiple people at once through spam emails (Perkins et al., 2020), or targeted at a specific individual (i.e., spear phishing). Those launching spear phishing scams pose as someone, often a trusted coworker, to have the victims send personal information (e.g., usernames, passwords, credit card information), or to click a hyperlink that often results in running malware (Caputo et al., 2013). The recommended steps to avoid phishing scams include considering unfamiliar emails with caution (i.e., not interacting with the email when possible), and not opening unfamiliar links or downloading information from non-secure sources. Response rates for phishing emails are alarmingly high. For example, after training employees at an organization of the dangers of phishing and how to prevent victimization, 60% of the employees still opened a malicious link sent to them in a simulated exercise (Caputo et al., 2013).

Good cyber hygiene also requires limiting social media engagement by not posting personal information or interacting with strangers. Information (e.g., geographical, financial, and personal) posted on social media sites can be stolen (Arachcilage & Love, 2014). Some information that is posted on social media (e.g., geographic and account information) can be directly used by online offenders to harm their target, whereas other information (e.g., names, email account, and birthdate) can be used in socially engineered attack vectors such as spear phishing (Halevi et al., 2003) to steal sensitive data. Additionally, and for the same reasons, individuals should avoid accepting friend requests from people they do not know. Yet, the majority of individuals active on social media post personal information on these sites (Halevi et al., 2003). This allows strangers, or potential scammers, access to the private information that, as stated above, can be stolen and used with malicious intent (Arachcilage & Love, 2014).

Connecting to public Wi-Fi also increases one's likelihood of experiencing victimization (Loukas & Patrikakis, 2016; Maimon et al., 2020), and therefore avoiding public Wi-Fi is a crucial, yet often ignored, element in self-protection. The danger of public Wi-Fi is that all information transferred between an individual's computer and the computer being accessed is available to everyone on the network. Cybercriminals are able to intercept this communication and gain access to sensitive data (e.g., usernames, passwords, credit card number, etc.) using open-source software. Although using a virtual proxy network is believed to reduce the risks of accessing public Wi-Fi by making it more difficult to decipher or intercept Internet traffic, it does not eliminate the risk (Karaymeh et al., 2019). Therefore, public Wi-Fi should be avoided when possible (Cain et al., 2018). Yet, the popularity of free Wi-Fi is soaring, and it can be found nearly everywhere (Henry & Luo, 2002).

Importantly, the behavioral safeguards that constitute cyber hygiene operate together to protect individuals while online. Similar to how maintaining good physical health requires individuals to engage in multiple self-protective behaviors (i.e., bathing, hand washing, teeth brushing, etc.) preventing cyber-victimization also requires the adoption of multiple behavioral safeguards. Thus, individuals who routinely engage in the self-protective behaviors outlined by Cain et al. (2018) are said to have high levels of cyber hygiene. Recall that cyber hygiene serves as a form of target hardening by restricting motivated offenders' opportunities to engage in crimes (Cohen & Felson, 1979; Cornish & Clarke, 2003). Accordingly, cyber hygiene should reduce victimization experiences. Various studies demonstrate that self-protection can be achieved by implementing computer security behaviors (Bossler & Holt, 2009; Choi, 2008; Holt & Bossler, 2013; Levesque et al., 2013, 2016; Wilsem, 2013), and multiple academic papers and industry reports discuss the importance of cyber hygiene in reducing risks associated with Internet connectivity (Maennel et al., 2018), yet no known study directly tests whether cyber hygiene reduces Internet users' experiences with victimization.

Moreover, it is unclear why some individuals choose not to implement self-protective behaviors (i.e., cyber hygiene) despite their target hardening capabilities. Developing a theoretical model capable of predicting engagement in self-protection is an area of academic inquiry with widespread theoretical and practical importance that spans across sub-field boundaries. Once Internet users who are most susceptible to victimization are identified, they can be nudged to make higher quality decisions that afford them some level of self-protection.

Preliminary evidence shows cognitive and behavioral differences can be used to explain variation in Internet users' adoption of good cyber hygiene practices (Neigel et al., 2020). For example, Whitty and colleagues (2015) found that older individuals and individuals who score high in "self-monitoring" are more likely to share their passwords. Similarly, Butler (2014) found knowledge, capability, and motivation are associated with password practices. Furthermore, Parsons et al., (2014; 2017) found knowledge and attitudes influence a variety of cyber hygiene practices including, but not limited to, password management and opening unfamiliar links. Additionally, myriad studies have shown that key theoretical variables derived from protection motivation theory (PMT) (i.e., threat and coping appraisals) explain variation in individuals' computer security behaviors (Sommestad et al., 2015). Lastly, and in direct relevance to the current study, Howell et al. (20021) demonstrated that cognitive decision-making capabilities are also a relevant predictor of computer security and privacy behaviors.

However, the cognitive decision-making process that leads to the adoption of online self-protective behaviors, which reduces the occurrence of victimization experiences, has not been adequately assessed. For starters, and as mentioned above, no known study has directly tested whether cyber hygiene reduces Internet users' victimization experiences. Moreover, both thoughtfully reflective decision making (TRDM) and PMT constructs are known correlates of computer security behaviors, but the processual relationship between TRDM, PMT, cyber hygiene, and victimization is yet to be explored. Thus, after demonstrating cyber hygiene reduces victimization experiences among a general sample of Internet users in the United States (Objective 1), the current study assesses a newly developed theoretical model in which TRDM operates through PMT constructs to predict variation in cyber hygiene engagement. In doing so, the current study serves as an attempt to develop a more robust theoretical model capable of explaining why some individuals fail to adopt recommended self-protective behaviors in the face of cyber threats despite their effectiveness at reducing victimization experiences (Objective 2).

Chapter Three:
Theoretical Framework

Chapter two provided literature relevant to the current study's first objective of determining whether engagement in cyber hygiene practices reduces Internet users' online victimization experiences. This chapter shifts focus to the current study's second objective of developing a theoretical model capable of explaining why some individuals fail to adopt good cyber hygiene practices in the face of cyber threats despite their purported effectiveness at reducing victimization experiences. In doing so, a newly developed theoretical model in which thoughtfully reflective decision making (TRDM) operates through protection motivation theory (PMT) constructs to explain variation in Internet users' engagement in cyber hygiene practices is introduced. The chapter begins by discussing key assumptions inherent within the rational choice approach to demonstrate that TRDM and PMT both operate on the assumption of human rationality and contend that decisions are the product of a cost-benefit analysis. Next, the propositional structure of TRDM and PMT are outlined, followed by a review of the empirical literature. Finally, an argument is made for the cross-disciplinary, end-to-end integration (Liska et al., 1989) of TRDM and PMT.

Rational Choice

Rational choice theory, which is more accurately described as a methodology or perspective (Wright & Decker, 1996), is grounded in the assumption of human agency, or the belief that individuals are capable of making choices and imposing those choices on the world. The depiction of man as rational beings, driven by an economical hedonistic calculus whereby they seek to maximize pleasure and minimize pain, is often traced to the writings of eighteenth and nineteenth century philosophers such as Cesare Beccaria and Jeremy Bentham. Operating on the assumption of human rationality, both Beccaria (1764) and Bentham (1781) believed decisions, such as the decision to engage in crime, are enacted out of self-interest and can be manipulated through changes to the anticipated outcomes. In *An introduction to the principles of morals and legislation*, Bentham (1781) outlined the principle of utility. He contended that "nature has placed mankind under the governance of two sovereign masters, pain and pleasure" (Bentham, (1781) and to ensure "the greatest happiness of the greatest number", it is the duty of the state to promote happiness through punishing and rewarding. Similarly, in *Dei delitti e delle pene* (*On crimes and punishments*), Beccaria (1764) argued that individuals will not engage in crime if the costs of crime (i.e., punishment) outweigh the benefits. Specifically, he believed it the responsibility of the state to deter crime by ensuring the associated punishments are swift, certain, and severe. Taken together, these early works painted an image of man as rational beings who make decisions based on anticipated outcomes (i.e., cost benefit analysis). This assumption is now central in the understanding of human behavior.

Importantly, and although Beccaria and Bentham discussed human agency in the context of offender decision making, the rational choice approach transcends academic disciplines. Rational choice has been used to model behavioral patterns in social, political, economic, and health behaviors. For example, rational choice is used by economists to explain purchasing behaviors, political scientists to explain voting behaviors, and by health scientists and information security researchers to explain the adoption of self-protective behaviors. Although the application of the approach varies based on the targeted population and dependent variable of interest, the basic tenants of the approach are invariant. McCarthy (2002, p. 419-422) conducted an interdisciplinary review of the rational choice literature outlining nine base assumptions.

The first assumption inherent within the rational choice approach is that “People have preferences for outcomes” (McCarthy, 2002, p. 418). Preference is a term used in relation to choosing between outcome alternatives. If an individual prefers A over B it simply means the individual would rather choose A than B. The second assumption states: “People’s preferences are complete, transitive, and stable” (McCarthy, 2002, p. 419). Completeness refers to an individual’s ability to rank outcome alternatives from most to least favorable. It is worth noting that not all outcomes are known, so completeness typically refers to the ranking of a subset of known outcomes. Transitivity refers to the coherence of the ordering. If a decision maker prefers A to B, and B to C, they must also prefer A to C. Stability refers to the consistency of the ranking over time. Although preferences can change over time as new information is acquired (Becker 1996; Frank 2000), they are believed to be stable throughout the decision-making process. The third assumption posits that “People’s preferences are influenced by their orientation to present versus future outcomes” (McCarthy, 2002, p. 419). Research on “time discounting” demonstrates that present rewards are often weighed more heavily than future rewards (Frederick et al., 2002).

The fourth assumption states: “Most outcomes are uncertain; there is typically no guarantee that they will be realized” (McCarthy, 2002, p. 419). Since outcomes are uncertain, decision makers’ risk tolerance affects their preferences. Individuals who are risk tolerant have a preference for taking gambles, whereas individuals who are risk-averse place greater emphasis on avoiding perils associated with a behavior, and thus an entirely different decision can be made based on the same set of facts. Additionally, and in accordance with the fifth assumption, “People base their assessments of costs and decisions on information they collect” (McCarthy, 2002, p. 420). Decisions are often made with incomplete information. Additionally, individuals are imperfect processors of information. Not all relevant information may be considered, and miscalculation often takes place. Importantly, information does not guarantee a rational choice will be made (Lupia & McCubbins 1998). However, the lack of information can hinder a decision maker's ability to make decisions based on their preferences. The sixth assumption is that "Rational actions are those that are consistent with the above assumptions" (McCarthy, 2002, p. 420). Paternoster and Pogarsky (2009, p. 105) express agreement with this notion, and state "persons are rational when they make choices that are consistent with their preferences and goals."

Importantly, and in accordance with the seventh assumption, "the rational choice approach does not preclude the possibility of people acting irrationally" (McCarthy, 2002, p. 421). Rational choice scholars do not believe that rational choice explains all behavior. An individual may choose an action that does not align with their preferences because the decision, or lack thereof, was made while in an emotional state. An example would include domestic homicide. Nonetheless, and as articulated in assumption eight, "People's choices can be examined with either a decision or game theory approach" (McCarthy, 2002, p. 421). Decision theory is used when an outcome is influenced by one individual's choice, whereas game theory is more applicable when an outcome results from more than one person's choices. Lastly, the ninth assumption states "The rational choice approach is not a theory of cognition" (McCarthy, 2002, p. 422). It does not assume people make literal calculations, but instead refers to the consistency between preferences and choices. Preferences vary based on a multitude of factors and, as a result, decision makers may make different choices based on the same set facts. Although individuals may not always be aware of their attempt to maximize interests while minimizing pain, useful predictions can be made on the assumption that most people act "as if" they engaged in a cost-benefit analysis (McCarthy, 2002, 422).

Rational choice has long been a dominant paradigm in economics (Gul, 2009) and, in recent decades, has also become widely used in the criminological literature. In accordance with the rational choice approach, the decision to engage in crime can be understood much like most other decisions (Becker, 1968; Ehrlich, 1974; Schmidt & Witte, 1984). To that end, criminal offending is shaped by a decision maker's preferences for outcomes, which are influenced by a host of factors including, but not limited to, risk tolerance, acquired information, time discounting, and cognitive decision-making capabilities (Paternoster & Pogarsky, 2009).

While many criminological theories attempt to explain criminal (e.g., strain theory) or non-criminal (e.g., social control theory) preferences, the rational choice approach treats preferences as a given and attempts to explain how these preferences alter the decision-making process. In other words, the rational choice approach focuses on individuals as decision makers who make choices (Nagin, 2007). Grounded in the above assumptions, a multitude of rational choice models have been developed in attempt to understand offender decision making. The first of these models was presented by the Nobel Prize winning economist, Gary Becker.

Becker (1968) contended that individuals engage in crime when the expected utility from engaging in a criminal act (i.e., monetary or psychic) is greater than the expected utility from refraining from engaging in a criminal act. Although Becker (1968) recognized psychic returns, and by extension myriad other costs and benefits associated with offending (McCarthy, 2002), his model is often boiled down to a deterrence model (Chiricos & Waldo, 1970; Loughran et al., 2011; Paternoster et al., 1983) similar to that offered by Beccaria (1764) over 200 years prior (Schmidt & Witte, 1984; Levitt & Lochner, 2001). However, Becker's (1968) economic model of crime and the rational choice approach are much more comprehensive than deterrence theory and take into account both formal and informal risks and rewards. The rational choice model, as presented by Becker (1968) and fully flushed out by Loughran et al. (2016) is expressed through the following equation: $\mathrm{EU} = pU\,(Y - f\,) + (1 - p)\;U\,(Y)$. Included in the equation are: “p, the offender’s probability of detection; f, the severity of the sanction one faces if apprehended; and Y, the utility benefits one accrues after the successful commission of the crime without apprehension” (Loughran et al., 2016).

Expanding upon Becker’s (1968) economic model of crime, and as discussed in chapter two, the rational choice approach has been employed to understand victimization patterns (Cohen & Felson, 1979) and provide practical solutions to aid in crime reduction (Clarke, 1983). Importantly, each of these models depict offenders as decision makers who act in accordance with their preferences and attempt to maximize pleasure while minimizing pain. The rational choice approach, as nested within the criminological literature, has generally shown to be relevant in modeling behavioral patterns in both offline (McCarthy, 2002) and online (Maimon & Louderback, 2019) environments.

In the cyber-environment, where the current study takes place, there exists a symbiotic relationship between offenders, guardians, targets, and enablers (Maimon & Louderback, 2019). Each of whom are decision makers who make choices (Nagin, 2007) and impose those choices on the world. Offenders, in attempt to maximize pleasure and avoid pain (Becker, 1968), choose targets deemed suitable and lacking capable guardianship (Bossler & Holt, 2009; Cohen & Felson, 1979). Consequently, and since law enforcement agencies (Burruss et al., 2019) and the cybersecurity industry (Holt, 2011; IC3, 2020; Maimon & Louderback, 2019; McAfee, 2017; Ponemon Institute, 2016) have proven ineffective in their role as guardians, Internet users (i.e., potential targets (Maimon & Louderback, 2019)) must restrict opportunities conducive to crime by means of target hardening (Newman & Clarke, 2013). Stated differently, Internet users must engage in self-protective behaviors (i.e., cyber hygiene) to avoid being victimized.

An abundance of evidence demonstrates cybercriminals act rationally when choosing their targets (Maimon & Louderback, 2019) and that implementing self-protective behaviors reduces victimization experiences (Cain et al., 2018), but it is less clear whether the rational choice approach can be used to explain variation in Internet users' adoption of self-protective behaviors (Ireland, 2020). In recent years, information security scholars have applied Rogers' (1975; 1983) PMT to explain variation in security related behaviors (Sommestad et al., 2015). Additionally, Howell et al. (2021) found TRDM (Paternoster & Pogarsky, 2009) to be relevant in predicting computer security and privacy behaviors. Both TRDM and PMT are rooted in the rational choice paradigm and thus share the assumption of human agency first depicted by eighteenth and nineteenth century enlightenment philosophers such as Beccaria (1764) and Bentham (1781).

The following sections will provide an overview of TRDM and PMT, detailing their underlying assumptions, propositions, and empirical support. After demonstrating that TRDM and PMT make the same assumptions regarding human behavior (i.e., humans are rational actors) and have complementary propositional structures, the chapter concludes by outlining arguments in support of a cross disciplinary, end-to-end theoretical integration (Liska et al., 1989) of the theories. The newly proposed theoretical model is a natural continuation of the rational choice approach and is useful in understanding the processual nature of human agency when deciding whether or not to engage in a particular behavior.

Thoughtfully Reflective Decision Making

The rational choice approach operates on the assumption of human agency (McCarthy, 2002) and, resultingly, rational choice scholars treat individuals as decision makers who make choices and impose those choices on the world (Nagin, 2007). Decisions are believed to be rational when they correspond with the decision maker's preferences for outcomes (McCarthy, 2002; Nagin, 2007; Paternoster & Pogarsky, 2009). However, not all individuals are equally equipped to make decisions that align with their preferences. "On average, some persons are better than others at collecting information or collecting more or better information, they are more careful in weighing the costs and benefits, more thoughtful in considering the information gathered, and more likely to ask themselves later if they could have made a better decision" (Paternoster & Pogarsky, 2009, p. 104).

Recognizing that not all actions are rational (McCarthy, 2002), and that not all individuals are equally capable of making decisions that result in desirable outcomes (Baron, 2008), Paternoster and Pogarsky (2009) introduced TRDM. In essence, the theorists contended that decision makers vary in their cognitive decision-making capabilities and that these capabilities are predictive of short-term and long-term life outcomes. TRDM, defined as the "tendency of persons to collect information relevant to a problem or decision they must make, to think deliberately, carefully, and thoughtfully about possible solutions to the problem, apply reason to the examination of alternative solutions, and reflect back upon both the process and the outcome of the choice in order to assess what went right and what went wrong" (Paternoster & Pogarsky, 2009, p.104-105), describes the process of quality decision making.

Inherent within this definition, Paternoster and Pogarsky (2009, p. 113) outlined the four components of TRDM: intentionality (i.e., "collecting information pertaining to a problem that requires a decision"), forethought (i.e., "thinking of alternative solutions to the problem"), self-reactiveness (i.e., "systematically deliberating over how to determine which alternative might be best"), and self-reflectiveness (i.e., "retrospectively analyzing how good a problem solver one was in the situation"). Importantly, these four components mirror the language Bandura (1989; 2001) used to describe human agency twenty years prior. If a rational action is one that aligns with a decision maker's preferences (McCarthy, 2002), human agency is intentionally acting to align actions with preferences (Paternoster & Pogarsky, 2009). Thus, TRDM captures the essence of human agency by depicting the process of reasoned decision making most likely to bring about the intended outcome.

TRDM varies between individuals and within individuals over time. Not all individuals are equal in their ability to make quality decisions and the ability to make quality decisions is not stable throughout the life course. TRDM is an "individual-level" (Paternoster & Pogarsky, 2009, p. 105) attribute reflective of an individual's biological capacity (i.e., differences in intelligence and executive functioning (Moffitt, 1990)) and socio-structural characteristics (i.e., human, social, and cultural capital (Becker, 1993)). Decision making capabilities can be improved throughout the life-course by means of deliberate training (Thaler & Sunstein, 2008) or through increased executive functioning. The development of the prefrontal cortex, a part of the brain largely responsible for executive functioning, is often not fully developed until age 25. Therefore, the ability to make quality decisions improves as youths advance into adulthood. Moreover, TRDM varies across contexts. Some decisions do not require thoughtful consideration, but are instead habitual (Kahneman, 2003). This is in sharp contrast to Gottfredson and Hirschi's (1990) notion of self-control, which, once established by age ten, is stable throughout the life course. Unlike self-control, TRDM is dynamic and can change based on lived events and experiences. Consequently, individuals can be trained or nudged to make decisions that will result in more prosperous outcomes, which is an important distinction when discussing policy implications aimed at changing behavioral patterns.

Those with higher levels of TRDM, or thoughtfully reflective decision makers, have an increased capacity to make choices that align with their preferences. Due to this increased capacity, Paternoster and Pogarsky (2009) convincingly argued that TRDM, as a measure of quality decision making, should be predictive of behavioral patterns, both criminal and conventional. Specifically, Paternoster and Pogarsky (2009, p. 106) contended that "thoughtfully reflective decision makers should be more effective agents and should make better quality decisions. This should be manifested in more successful life outcomes, the accumulation of social, personal, and cultural capital, and a reduced risk of anti-social and self-destructive behavior." Empirical examinations of TRDM have generally found support for this proposition (Howell et al., 2021; Louderback & Antonaccio, 2017; Maimon et al., 2012; Paternoster & Pogarsky, 2009; Paternoster et al., 2011; Timmer et al., 2020).

The first test of TRDM was conducted by Paternoster and Pogarsky (2009) using data from the National Longitudinal Study of Adolescent to Adult Health. The authors made three key empirical contributions. First, they demonstrated TRDM can be effectively operationalized. Second, they illustrated the conceptual and empirical differences between TRDM and self-control. Third, they found TRDM to be predictive of both short- and long-term behavioral patterns. In the short-term (6-18 months), thoughtfully reflective decision makers were more likely to graduate from college and less likely to be involved in delinquency, drug use, and heavy drinking. In the long-term (5-7 years), thoughtfully reflective decision makers were more likely to be involved in community and civic groups and less likely to be involved in criminal offending and drug use (Paternoster & Pogarsky, 2009).

Using the same data source, Paternoster et al. (2011) and Maimon et al. (2012) generated two additional contributions central to the development of the theory. Paternoster et al. (2011) linked TRDM to successful life outcomes. Specifically, the authors found that thoughtfully reflective decision makers accumulate more resources (i.e., social, human, and cultural capital) due to their ability to formulate a "rationally arrived at life plan" (Paternoster et al., 2011). Additionally, they found that resource accumulation partially mediates the relationship between TRDM and crime. Maimon et al. (2012) demonstrated the contextual nature of the relationship between decision making and criminal behavior. Specifically, Maimon et al. (2012) found TRDM is associated with a decrease in youth violent offending and that the effect of TRDM on violence is conditioned by school-authorized sanctions. Timmer et al. (2020), corroborating the existence of a conditional relationship between TRDM and crime, found the effect of TRDM on crime is moderated by "hot triggers" such as sleep problems, depression, and straining conditions. Taken together, these studies demonstrate that TRDM is associated with both positive (Paternoster et al., 2011) and negative (Paternoster & Pogarsky, 2009) life outcomes, and that contextual factors alter the decision-making process (Maimon et al., 2012; Timmer et al., 2020).

The next major theoretical contributions to the development of TRDM were made by Louderback and Antonaccio (2017), who conducted the first test of TRDM using data not derived from the National Longitudinal Study of Adolescent to Adult Health. Using survey data gathered from a large private university, the authors examined the relationship between TRDM and criminal behavior in the cyber-environment. Moreover, they were the first to assess the relationship between TRDM and victimization. Findings demonstrated that thoughtfully reflective decision makers were less likely to engage in, or fall victim to, cybercrime incidents than their less thoughtfully reflective counterparts. The effect of TRDM on cybercrime involvement highlights the importance of decision making in the cyber-environment and is consistent with past examinations of TRDM on crime (Maimon et al., 2012; Paternoster et al., 2011; Paternoster et al., 2011). The effect of TRDM on victimization demonstrates that quality decision making is pertinent to the discussion of self-protection. The authors also estimated the interaction effects between TRDM and respondents' gender and age. They found the effects of TRDM on offending and victimization did not differ between males and females. However, the effects do vary by age as theorized by Paternoster and Pogarsky (2009).

Importantly, Louderback and Antonaccio (2017) believed the observed effect between TRDM and online victimization occurred because those with lower levels of TRDM "are less likely to engage in thoughtful cognitive decision-making processes when taking steps to protect their computers against potential victimization" (Louderback & Antonaccio, 2017, p. 645). Although untested, the authors suggested that thoughtfully reflective decision makers are more likely to engage in self-protective behaviors, which reduces their experience with online victimization. Stated differently, Louderback and Antonaccio (2017) posited that engagement in self-protective behaviors (i.e., cyber hygiene) mediates the effect of TRDM on online victimization.

In a recent study, Howell et al. (2021) sought to test the assertion that TRDM is associated with the adoption of self-protective behaviors. Specifically, the authors conducted two application experiments using a general sample of Internet users in Israel to test whether thoughtfully reflective decision makers are more likely to engage in computer privacy and security behaviors. As hypothesized, they found thoughtfully reflective decision makers are more likely to engage in computer privacy behaviors. TRDM was only associated with online security behaviors for participants who were warned of the potential consequences of not engaging in the security behaviors. In other words, TRDM interacted with implication disclosure to predict engagement in security behaviors. Thus, thoughtfully reflective decision makers who are made aware of the potential implications associated with not engaging in computer security behaviors are more likely to engage in security behaviors. Taken together, Howell and colleagues' (2021) study demonstrates TRDM's predictive efficacy on Internet users' engagement in self-protective behaviors (i.e., privacy and security) and illustrates how Internet users can be nudged to adopt behavioral recommendations through environmental configurations aimed to trigger greater levels of cognition.

However, it is worth noting that Howell et al.'s (2021) study only focused on a limited number of specific behaviors, rather than holistically examining engagement in cyber hygiene practices. This is problematic, because as discussed in chapter two, cyber hygiene serves as the best form of target hardening (Cain et al., 2018). Additionally, they failed to test whether the adoption of these behavioral safeguards reduces victimization experiences. Lastly, and although the authors provided insight into the relationship between TRDM and the adoption of computer security and privacy behaviors, they failed to consider the cognitive mediating process that underlies this nexus. Consequently, the true nature of the relationship between TRDM and engagement in self-protective behaviors is unclear. It is possible that TRDM has a direct effect on engagement in self-protective behaviors as documented by Howell et al. (2021). However, even Howell et al. (2021) alluded to a processual relationship in which TRDM is mediated by constructs derived from PMT by noting that thoughtfully reflective decision makers, when confronted with the threat of a potential negative outcome, develop higher and more accurate threat and coping appraisals, which results in the adoption of self-protective behaviors. The following section provides a detailed overview of Rogers' (1975; 1983) PMT.

Protection Motivation Theory

One of the leading causes of death in the United States is cardiovascular disease. Although hereditary factors are certainty important, susceptibility to heart disease can be reduced through the adoption of established self-protective behaviors such as routine physical examinations, monitoring blood pressure, eating a well-balanced diet, abstaining from smoking, and exercising. These behavioral safe-guards are well-known by the general public, yet some individuals choose not to adopt them, thus increasing their risk of cardiovascular disease. The same problem has emerged in cyberspace. The general public is constantly warned about the threat of cyber-victimization and relayed the importance of adopting cyber hygiene practices (Maennel et al., 2018), yet some individuals choose not to engage in self-protection, thus increasing their risk of being victimized (Cain et al., 2018). Rogers' (1975; 1983) PMT, which originated in the health sciences to explain variation in persons' intent to adopt recommended health behaviors, is now used to model variation in persons' intent to adopt, and actual adoption of, a variety of self-protective behaviors including those in the cyber-environment (Sommestad et al., 2015).

PMT contends that when confronted with the threat of a potential negative outcome (i.e., fear appeal) two parallel independent cognitive processes are triggered: threat appraisals and coping appraisals. The stronger the appraisals, the higher one's protection motivation, and thus the more likely an individual is to actually adopt the recommended behaviors (Rogers, 1975; 1983). Protection motivation is best defined as a decision maker's "behavioral intention," or their intent to adopt the behavioral recommendation(s) believed to prevent the occurrence of the negative outcome (Rogers, 1983, p. 170). Importantly, Rogers (1983) theorized that behavioral intention (i.e., protection motivation) and behavioral adoption are strongly correlated, a proposition that has garnered overwhelming support (Floyd et al., 2000; Milne et al., 2000; Sommestad et al., 2015). Resultingly, examinations of PMT, especially in the information security literature, often examine the direct effects of PMT constructs on behavioral adoption (Sommestad et al., 2015).

Threat appraisals result in more protection motivation when individuals view the occurrence of a negative outcome to be probable and severe. Additionally, an individual's threat appraisal in the face of risk may spark fear, which in turn, may push a decision maker to decide that the future outcomes from engaging in protective behaviors outweigh the maladaptive rewards earned from not adopting protective behaviors (Boss et al., 2015). Maladaptive rewards include any perceived reward (both intrinsic and extrinsic) for the response of not protecting oneself (Floyd et al., 2000). If an individual's perceived maladaptive rewards outweigh the perceived threat, the individual may choose the maladaptive route of not adopting the protective behavior. However, maladaptive rewards are rarely considered in examinations of PMT (Boss et al., 2015; Norman et al., 2005; Sommestad et al., 2015) due to the conceptual overlap with response costs, which is discussed in the following paragraph.

Fear appeals also trigger a decision maker's coping appraisals. Coping appraisals result in more protection motivation when an individual has faith in the behavioral recommendation proposed to thwart the occurrence of a negative outcome (i.e., response efficacy) and their own ability to carry out the recommendation (i.e., self-efficacy), but does not perceive the response cost associated with adopting the recommended behavior to be too high. Response costs are any cost (i.e., monetary, time, level on difficulty, etc.) associated with adopting the recommended behavior. Response costs and maladaptive rewards are nearly indistinguishable, and researchers often struggle to differentiate the concepts (Boss et al., 2015; Norman et al., 2005; Sommestad et al., 2015). In other words, the costs of adopting a behavioral recommendation are often the same as the rewards of not adopting the behavior. For instance, if an individual believes purchasing anti-virus software is expensive, the response cost is the money spent and the maladaptive reward is the money saved, thus making the concepts two sides of the same coin. See Figure 1 for an illustration of Roger's (1983) theoretical model.

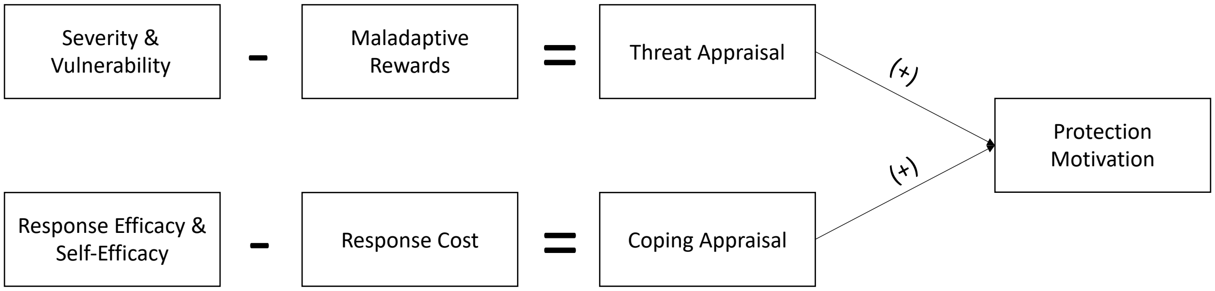

Figure 1. Protection Motivation Theory Model.

Stated precisely, PMT posits the motivation to protect oneself from danger is a "positive linear function of four beliefs: (1) the threat is severe, (2) one is personally vulnerable to the threat, (3) one has the ability to perform the coping response, and (4) the coping response is effective in averting the threat" and, "a negative linear function of: (1) the reinforcements associated with the maladaptive response, and (2) the response costs" (Rogers, 1983, p. 170). More loosely put, PMT is a cost-benefit model where risks associated with experiencing a negative outcome are compared to the costs of trying to prevent the negative outcome from occurring (Sommestad et al., 2015). Importantly, and although PMT is presented as a general theory of persuasive communication, the cognitive mediating process is conditioned by age, race, and gender (Allen et al., 2008; Chou et al., 2017; Guo et al., 2015). It is also likely that intraindividual differences in quality decision making capabilities alter the cognitive mediating processes that result in protection motivation, a point that will be expanded upon in the following section.

A litany of research has amassed over the course of 45 years evaluating the propositions set forth by Rogers (1975; 1983), generating support for PMT across several disciplines (Milne et al., 2000; Floyd et al., 2000). Although a large majority of studies examine PMT in the context of the health sciences (Norman et al., 2005), PMT began to emerge as a dominate theoretical framework in the information security literature in the early 2000s (Sommestad et al., 2015). Given the sheer volume of empirical examinations of the theory, the current study will only review literature as it relates to self-protection in the cyber-environment. However, an interested reader is encouraged to review the meta-analytic studies put forth by Milne et al. (2000) and Floyd et al. (2000), who find general support for PMT in predicting the intent to adopt, and actual adoption of, health-related behaviors.

In a recent review of the literature, Sommestad et al. (2015) identified 28 studies which sought to assess the predictive efficacy of one or more of the components of PMT (i.e., severity, maladaptive rewards, vulnerability, response efficacy, self-efficacy, response cost) on information security behavior (Anderson & Agarwal, 2010; Arachchilage & Love, 2013; Boss & Galletta, 2008; Bulgurcu et al., 2010; Chan & Woon, 2005; D'Arcy & Hovav, 2008; Dinev et al., 2009; Guo et al., 2011; Herath & Rao, 2009; Herath et al., 2012; Hu et al., 2012; Ifinedo, 2012; Johnston & Warkentin, 2010; Johnston et al., 2010; Kumar et al., 2008; Lee et al., 2008; Li et al., 2010; Liang & Xue, 2010; Liao et al., 2009; Posey et al., 2011; Rhee et al., 2009; Siponen et al., 2010; Tamjidyamcholo et al., 2013; Vance et al., 2012; Xue et al., 2010; Zhang et al., 2009; Zhang et al., 2013). Of these 28 studies, 24 included measures for self-efficacy, 18 included measures for response efficacy, 11 included measures for vulnerability and severity, 10 included measures for response cost, and only 1 included a measure for maladaptive rewards.

The first of these studies was conducted by Chan and Woon (2005). The authors demonstrated that self-efficacy (i.e., an individual's belief in their own ability to perform a specific task (Bandura, 1977)) influences employees' willingness to comply with security procedures. However, the first real test of PMT on Internet users' engagement in self-protective behaviors was offered by Lee et al. (2008), who, unlike Chan and Woon (2005), included measures for self-efficacy, response efficacy, response cost, severity, and vulnerability. The authors, using a sample of college students, found that all of the PMT constructs, with the exception of perceived severity, are predictive of Internet users' intent to adopt anti-virus software. Self-efficacy had the largest effect, followed by response efficacy. Interestingly, and as reported by Sommestad et al. (2015), self-efficacy has since remained, on average, the strongest predictor of information security behavior.

Each of the PMT constructs, however, have garnered overwhelming support across various contexts. For example, the constructs have been applied to mandatory (i.e., following protocol) (e.g., Bulgurcu et al., 2010; Chan & Woon, 2005; Galletta, 2008) and voluntary (e.g., Anderson & Agarwal, 2010; Arachchilage & Love, 2013; Boss & Galletta, 2008) behavior examining general (e.g., I intend to protect my computer) (e.g., Posey et al., 2011; Rhee et al., 2009; Siponen et al., 2010) and specific (e.g., I intend to change my password) (e.g., Johnston & Warkentin, 2010; Johnston et al., 2010; Kumar et al., 2008) forms of protection using samples of employees (e.g., Bulgurcu et al., 2010; Chan & Woon, 2005; D'Arcy & Hovav, 2008) and students (e.g., Dinev et al., 2009; Kumar et al., 2008; Lee et al., 2008). On average, PMT constructs are more predictive of voluntary than mandatory behavior, with the exception of vulnerability, which is more strongly correlated when the behavior is mandatory (0.28 vs 0.18) (Sommestad et al., 2015). Additionally, PMT constructs are more predictive of protection motivation when the behavioral recommendation is specific rather than general (Sommestad et al., 2015). This is likely due to Internet users' ability to adopt the behavior. Being prompted to "update a password" is easier to understand and implement than being asked to "secure a computer". Moreover, the effect of PMT constructs in the cyber-environment also seem to be conditioned by demographic characteristics (Chou et al., 2017).

Interesting patterns also emerged when assessing the effect of threat appraisals in the cyber-environment. First, the effect of both perceived severity (0.30 vs 0.17) and perceived vulnerability (0.22 vs 0.18) are more likely to increase Internet users' willingness to adopt recommended security behaviors when the threat of victimization is targeted at them, rather than an organization (Arachchilage & Love, 2013; Boss & Galletta, 2008; Guo et al., 2011; Herath & Rao, 2009; Ifinedo, 2012; Johnston et al., 2010; Lee et al., 2008; Liang & Xue, 2010; Posey et al., 2011; Zhang et al., 2013). Additionally, and although depicted as two separate constructs (Rogers, 1983), the average correlation between perceived severity and perceived vulnerability is .50, indicating that Internet users may not view the constructs as distinctly different (Sommestad et al., 2015).

Taken together, the aforementioned studies (1) highlight the effectiveness of PMT constructs in modeling protection motivation and self-protection in the cyber-environment, (2) demonstrate that PMT is most applicable when the behavior is voluntary, (3) illustrate that fear appeals are more likely to elicit protection motivation when the individual is being personally threatened, and (4) cast doubt on the empirical distinction between the perceived severity and perceived vulnerability of online victimization. Although PMT is consistently shown to be correlated with security related behaviors (Sommestad et al., 2015), it is worth noting that none of the individual constructs are able to explain more than a small portion of the variance in individual's intent to adopt, or actual adoption of, security behaviors. However, and as noted by Rogers' (1983), the variables operate together to influence a decision makers' willingness to adopt self-protective behaviors. In the seven studies that included all six variables of PMT, or all key variables except maladaptive rewards, the variance explained is between 0.34 and .50 (Sommestad et al., 2015), which is respectable when compared to competing theories within the information sciences (Sommestad & Hallberg, 2013).

As depicted above, PMT has become a dominate theoretical framework in the information security literature and, considering the model's "respectable explanatory ability" (Sommestad et al., 2015, p. 11), it will likely remain central to the understanding of self-protection in the cyber-environment. However, since PMT posits a cost-benefit analysis in which decision makers must weigh the risks associated with experiencing a negative outcome against the costs of trying to prevent the negative outcome from occurring (Sommestad et al., 2015), the next logical step toward theoretical development is determining the environmental or intrapersonal factors that shape this decision-making process. Drawing from a relatively new concept from the criminological literature, TRDM (Paternoster & Pogarsky, 2009), the current study posits that quality decision makers, when confronted with the threat of a potential negative outcome, will develop higher and more accurate threat and coping appraisals, which will result in the adoption of self-protective behaviors that prevent victimization experiences. This newly expanded theoretical model, which is discussed in more depth in the following section, describes the processual nature of human agency by illustrating the cognitive mediating process that links quality decision making with self-protection.

Theoretical Integration

While it is possible that a decision maker's threat and coping appraisals may influence their decision to adopt computer security behaviors as shown in the empirical research reviewed above (Sommestad et al., 2015), it is important to note that changes in one's cognitive attitudes and behaviors occur within a field of bounded rationality (Gigerenzer & Selten, 2002). In other words, individuals have varying levels of information available to accurately predict the overall costs and benefits of their actions (Clarke & Cornish, 1985), as well as varying levels of cognitive decision-making skills to successfully make effective decisions—including the decision to develop protection motivation in the first place (Paternoster & Pogarsky, 2009).

In the original formulation of PMT, Rogers (1975; 1983) noted that protection motivation likely varies based on environmental and intrapersonal factors but was "vague" in his operationalization (Clubb & Hinkle, 2015). Given that PMT posits a cost-benefit analysis where persons must decide whether or not to engage in security behaviors (Sommestad et al., 2015), and since not all persons are equally capable of making decisions that result in desirable outcomes (Baron, 2008), intraindividual variation in quality decision making capabilities, as measured through TRDM, likely shapes the context in which the cognitive mediating process (i.e., threat and coping appraisals) takes place. Stated differently, in the face of cyber threats, thoughtfully reflective decision makers may develop higher and more accurate threat and coping appraisals, leading to the adoption of cyber hygiene practices and ultimately reducing victimization experiences. To examine such a relationship requires the cross-disciplinary, end-to-end integration (Liska et al., 1989) of the interrelated propositions set forth by Paternoster and Pogarsky (2009) and Rogers (1983).

Theoretical integration, as defined by Thornberry (1989), is the act of combining two or more sets of logically interrelated propositions into one larger set of interrelated propositions, in order to provide a more comprehensive explanation of a particular phenomenon" (p. 52). Theoretical integration is not new to the field of criminology. In fact, many theorists have employed integrative practices including Shaw and McKay (1942), Merton (1938), Burgess and Akers (1966), and Akers (1973). However, the logical ability to integrate such theories resulted in a heated debate among some of the most influential scholars in the field at a conference held on the Albany campus of the State University of New York in May of 1987, which is presented in *Theoretical integration in the study of deviance and crime, problems and prospects.* Although some scholars have argued forcefully for the integration of theories (Elliott et al., 1979; 1985), others have raised serious concerns (Hirschi 1979; 1989; Short, 1979). For example, Elliott et al. (1985), a proponent of integration, argued the "oppositional tradition," in which theories are pitted against each other, has failed. As a result, the level of explained variance in most theories is "embarrassing low" (Elliott et al., 1985, p. 125), with some leading theories (e.g., self-control) explaining less than 30%, on average, of the observed variance in patterns of crime and deviance (Weisburd & Piquero, 2008). Additionally, Akers (1989) argued that if integration is not pursued we miss important commonalities among seemingly incompatible theories. Thus, for Elliott et al. (1985) and Akers (1989), integration is a necessary path for the development of a more comprehensive view of human behavior.

Conversely, Hirschi (1989), one of the most vocal critics of theoretical integration, argued most criminological theories are by design oppositional, possessing incompatible assumptions of human behavior. Enlightenment scholars, for example, depicted man as rational calculators and argued criminal incidents could be thwarted by making the cost of crime outweigh the benefits (Beccaria, 1764; Bentham, 1781). Cesare Lombroso rejected the assumption of human rationality and argued criminality was inherited and that a “born criminal” could be identified based on physical defects (Lombroso-Ferrero & Lombroso, 1911). Sutherland (1947) rejected the assumption that criminals are defective at birth and depicted man as a social animal who engages in learned behaviors. The Freudian image of defective socialization was then replaced with theories prioritizing social sources as the root cause of crime. Finally, control theories were developed in direct opposition to purely social theories of crime.

When discussing whether theories with opposing assumptions can be integrated, Hirschi (1989) correctly argued “If theory A asserts X and theory B asserts not X, it would seem impossible to bring them together in a way pleasing and satisfactory to both, and also pointless to try” (p. 39). In other words, by ignoring the assumptions on which the competing theories were built, the clarity and internal consistency of the traditional theory is lost, and we are left with “theoretical mush” (Thornberry, 1989). Swayed by Hirschi’s (1989) arguments, I too find attempts to integrate oppositional theories inappropriate. However, Hirschi (1989) did concede that theories can be integrated if they have the same assumptions and are making similar predictions. Similarly, Thornberry (1989) argued past integration efforts are faulty because propositions rather than concepts are the building blocks of a theory, and therefore successful integration is only possible when propositions are linked. Thus, integration efforts should not simply borrow concepts from incompatible theories, such as social learning theory (Akers, 1973) and self-control theory (Gottfredson & Hirschi, 1990), but should instead demonstrate how interrelated propositions overlap to provide a more robust explanation of a particular behavior.

The above sections went to great lengths to demonstrate that TRDM and PMT are rooted in the rational choice paradigm, depicting humans as decision makers who impose their will on the world. Adopting self-protective behaviors is itself a choice shaped by a cost-benefit analysis in which decision makers weigh the risks of a negative outcome against the costs of engaging in protective behaviors (Rogers, 1983). Since not all persons are equally equipped in their ability to make quality decisions, this choice is likely altered by decision makers' cognitive decision-making capabilities. By asserting that TRDM shapes the cognitive mediating process depicted in PMT, the propositional structures can be logically linked to demonstrate the processual nature of human agency. Stated differently, in the face of a credible threat, it is hypothesized that PMT constructs are a function of TRDM. Thoughtfully reflective decision makers will: (1) recognize the seriousness of a threat, (2) recognize they are personally vulnerable, (3) believe in their ability to adopt the recommended behavior, (4) believe in the effectiveness of the recommended behavior, (5) associate less costs with adopting the behavior, and (6) associate less rewards with adopting the maladaptive response. Consequently, it is hypothesized that TRDM will both increase self-protection and PMT constructs. Specifically, TRDM will have both a direct effect on cyber hygiene and indirect effect through PMT constructs.

Now that it has been established that TRDM and PMT have the same assumptions of human behavior, and can be linked based on their propositional structure, the various methods of theoretical integration will be outlined to identify which, if any, method is most appropriate. The three types of theoretical integration outlined by Liska, Krohn, and Messner (1989) are as followed: side-by-side, up-and-down, and end-to-end. Each type is defined by a principle that links different theories together.

Side-by-side integration involves partitioning behavioral patterns based on the theory that best explains them. This type of integration is the most straightforward and operates on the notion that not all theories can be used to explain all forms of behavior. Successful side-to-side integration requires theorists to specify the conditions for which the integrated theories can be applied. Consider the effect punishment has on recidivism. Deterrence theory (Becker, 1968) posits that punishment decreases the occurrence of future criminal incidents. Conversely, labeling theory (Becker, 1963) posits that punishment increases the occurrence of future criminal incidents. Title (1975) suggests that punishment may have both a deterrent and labeling effect on recidivism depending on the crime type. Being convicted of prostitution, and the societal stigma associated with such a label, would likely provide additional opportunities to engage in the practice, while closing opportunities for engagement in more conventional relationships and employment. Conversely, being convicted of shoplifting would not lead to public shaming, nor would it necessarily block opportunities for conventional employment, but it would likely increase the offender's perception of sanction certainty. Thus, the side-by-side approach could be used to integrate deterrence theory and labeling theory despite their oppositional nature if the conditions under which each theory can be applied is specified by the newly integrated theoretical model. Rather than TRDM and PMT being used "side-by-side" (Liska et al., 1989) to predict security behavior, the current study proposes a processual relationship in which TRDM operates indirectly through PMT constructs. Therefore, the side-by-side approach is inappropriate for achieving the objectives set forth by the current study.

Up-and-down integration, also known as deductive integration, involves "identifying a level of abstraction or generality that will incorporate some of the conceptualization of the constituent theories" (Liska et al., 1989, p. 10). This method requires theorists to deduce the propositions of theory B from the premise of theory A. This can be accomplished by equating terminology among the two theories. For example, Burgess and Akers (1966) equated concepts from differential association theory (theory B) with those contained in the premise of learning theory (theory A) by arguing learning that takes place within a peer group is a special form of operant conditioning and by reconceptualizing definitions favorable to deviance as a form of discriminative stimuli (Liska et al., 1989). This method of integration has been referred to as theoretical imperialism because the deduced theory, which in this case is differential association theory, loses its original identity. The current study does not attempt to equate concepts from TRDM and PMT, making this approach inappropriate.

Lastly, end-to-end integration "refers to conceptualizing a dependent variable in one theory as an independent variable in another, an independent variable in one theory as a dependent variable in another, or both" (Liska et al., 1989, p. 8). This form of integration occurs when a processual relationship is believed to exist between two or more theories and the dependent variable of interest. Causal conditions of behavior range on a continuum from immediate (i.e., direct cause) to remote (i.e., indirect cause) (Jessor & Jessor, 1973). In the context of the current study, TRDM is used to predict key independent variables derived from PMT. Stated differently, independent variables from PMT are conceptualized as dependent variables to be predicted by TRDM. Thus, in the full processual model in which TRDM operates through PMT constructs to predict engagement in cyber hygiene behaviors, TRDM is conceptualized as a remote cause of self-protection and PMT constructs are conceptualized as immediate causes of self-protection. This method can also be referred to as theoretical elaboration (Liska et al., 1989; Wagner & Berger, 1985). Although the newly developed theoretical model incorporates theoretical insights from both TRDM and PMT (integration), it also uses those insights to further specify the causal explanations contained in PMT (elaboration). Semantics aside, this method of model building is generally preferred by theorists

(Hirschi, 1989; Thornberry, 1989; Wagner & Berger, 1985) and results in "what most sociologists consider as growth and development (Liska et al., 1989, p. 10)."

Despite the potential for theoretical growth and development, past end-to-end integration attempts have failed to consider assumptive differences between the integrated theories. For example, Elliott and colleagues (1985) attempted to integrate differential association theory (Sutherland, 1947) and Hirschi's (1969) control theory, but merely "use the terms and ignore the claims of control theory" (Hirschi, 1979, p. 34). Unlike learning and control theories, which have competing assumptions of human behavior, TRDM and PMT both operate on the assumption of human rationality and contend that decisions are the product of a cost-benefit analysis. Since both theories have the same assumption of human behavior, and since the propositional structures overlap, the theoretical models can be logically integrated into a singular, processual theoretical model, which should increase the amount of explained variance in cybersecurity related behaviors, help gain a more nuanced understanding of the processual nature of human agency, and, most importantly, provide a more comprehensive theoretical model capable of predicting whether an individual will adopt recommended self-protective behaviors in the face of cyber threats (Muftic, 2009). The following chapter provides a detailed description of the aims and scope of the current study and puts forth testable hypotheses.

Chapter Four:
Current Study

The current study has two primary objectives: (1) determine whether engagement in cyber hygiene practices reduces Internet users' online victimization experiences, and if so, (2) develop a theoretical model capable of explaining why some individuals fail to adopt good cyber hygiene practices despite their now proven effectiveness at reducing victimization experiences.

A review of the literature, as presented in chapter two, demonstrates that motivated offenders, who seek to maximize pleasure and avoid pain (Becker, 1968), choose targets deemed as suitable and lacking capable guardianship (Cohen & Felson, 1979; Maimon & Louderback, 2019). Thus, to reduce susceptibility to online victimization, Internet users must increase capable guardianship and/or decrease suitability by engaging in acts of target hardening (Clarke, 1983). Myriad studies have demonstrated the effectiveness of specific target hardening measures at reducing susceptibility to certain forms of victimization (Bossler & Holt, 2009; Choi, 2008; Holt & Bossler, 2013; Levesque et al., 2013, 2016; Wilsem, 2013). However, to achieve self-protection in the cyber-environment, Internet users must engage in a multitude of preventative behaviors. For example, anti-virus software can protect against computer infections, whereas a strong password is necessary to protect against brute force attacks (i.e., password guessing) (Weir et al., 2010). Cain et al. (2018) outline the preventative behaviors widely believed to be the best practices in achieving self-protection. The amalgamation of these behavioral safe-guards can be referred to as cyber hygiene (Cain et al., 2018). Although cyber hygiene has been advertised as an effective means to reduce susceptibility to victimization experiences, this claim has never been directly tested. Therefore, the current study seeks to examine whether engagement in cyber hygiene practices reduces Internet users' experiences with online victimization. Stated as a hypothesis:

H1: Higher levels of engagement in cyber hygiene practices will decrease Internet users' experiences with victimization.

Next, the current study shifts to examining why some Internet users choose not to implement good cyber hygiene practices despite their now proven effectiveness at preventing victimization experiences. In doing so, a newly developed theoretical model in which thoughtfully reflective decision making (TRDM) operates through protection motivation theory (PMT) constructs to explain variation in Internet users' engagement in cyber hygiene practices is introduced. PMT can be viewed as a cost-benefit model where risks associated with experiencing a negative outcome are compared to the costs of trying to prevent the negative outcome from occurring (Rogers, 1983; Sommestad et al., 2015). Importantly, not all persons are equally capable of making decisions that result in desirable outcomes. Thus, as hypothesized in chapter three, protection motivation is believed to be a function of TRDM. When considering the threat of online victimization, thoughtfully reflective decision makers will develop higher and more accurate threat and coping appraisals than their less thoughtfully reflective counterparts. As two hypotheses:

H2: Higher levels of TRDM will increase Internet users' coping appraisals.

H3: Higher levels of TRDM will increase Internet users' threat appraisals.

Moreover, threat appraisals are theorized to elicit the emotional response referred to as fear, which in turn, pushes a decision maker to decide that the future outcomes from engaging in protective behaviors (i.e., cyber hygiene) outweigh the maladaptive rewards earned from not adopting protective behaviors (Boss et al., 2015). Thus, Internet users' threat appraisals are believed to increase their fear of victimization, which in turn, should increase their engagement in cyber hygiene practices. Stated as hypotheses:

> *H4: Higher threat appraisals will increase Internet users' fear of victimization.*

> *H5: Higher fear appraisals will increase Internet users' adoption of cyber hygiene practices.*

Since past studies have found direct effects between TRDM (Howell et al., 2021) and PMT constructs (Sommestad et al., 2015) on engagement in online protective behaviors, it is believed TRDM and PMT constructs will also have direct effects on cyber hygiene engagement. Stated as hypotheses:

> *H6: Higher levels of TRDM will increase Internet users' adoption of cyber hygiene practices.*

> *H7: Higher coping appraisals will increase Internet users' adoption of cyber hygiene practices.*

> *H8: Higher threat appraisals will increase Internet users' adoption of cyber hygiene practices.*

Provided that thoughtfully reflective decision makers develop higher coping (hypothesis 2) and threat (hypothesis 3) appraisals, and that TRDM (hypothesis 6) and PMT constructs (hypotheses 7 and 8) have a direct effect on cyber hygiene engagement, the current study takes the next logical step to assess the processual relationship between TRDM, PMT, and cyber hygiene. Specifically, the current study posits that PMT constructs will partially mediate the effect of TRDM on cyber hygiene and that TRDM will operate indirectly through PMT constructs to increase engagement in cyber hygiene practices. Stated as hypotheses:

> *H9: PMT constructs will partially mediate the effect of TRDM on Internet users' adoption of cyber hygiene practices.*

> *H10: The indirect effect of TRDM through coping appraisals will increase Internet users' adoption of cyber hygiene practices.*

H11: The indirect effect of TRDM through threat appraisals will increase Internet users' adoption of cyber hygiene practices.

The aforementioned hypotheses and full processual model are depicted in Figure 2.

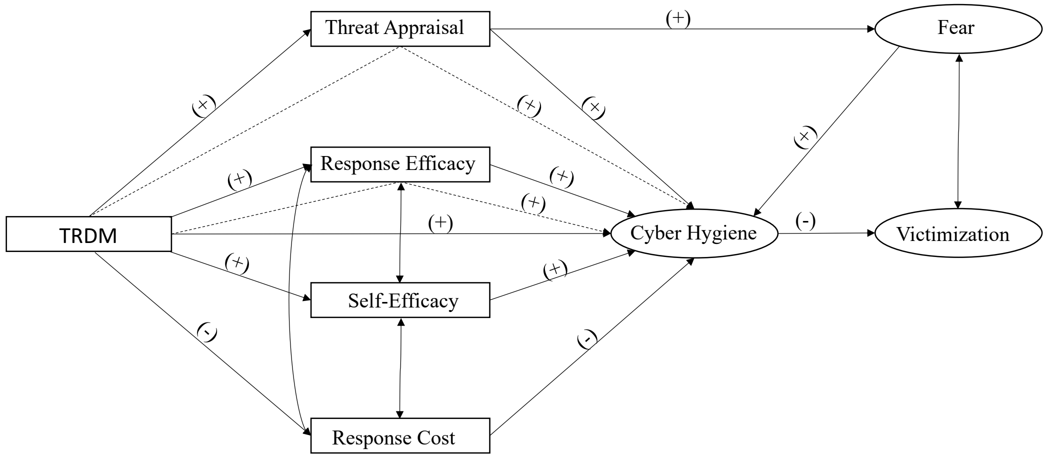

Figure 2. Proposed Structural Model Examining the Processual Relationship Between Thoughtfully Reflective Decision Making, Protection Motivation Theory Constructs, Cyber Hygiene, and Victimization.

Note. Error terms not depicted in the figure; TRDM=thoughtfully reflective decision making; Control variables include: low self-control, computer skill, education, White, age, male.

Chapter Five:
Methodology

Data Collection

The data collection strategy described below was approved by The University of South Florida's Institutional Review Board (Pro00041929). Data for the current study were gathered using Amazon's Mechanical Turk, a popular surveying platform that recruits and pays individuals to complete online tasks, such as surveys. Although Mechanical Turk allows for a general sample of Internet users residing in the United States in terms of demographic characteristics (i.e., age, race, sex), not all Internet users in the United States (the sampling frame) have an equal chance of inclusion, thus resulting in a purposive, non-random sample. Importantly, recent research demonstrates that non-random online samples (e.g., Mechanical Turk) yield relationships that are often in the same direction, though magnitude may vary, as those found using national probability samples (e.g., Thompson & Pickett, 2020).

An online survey was designed to assess thoughtfully reflective decision making (TRMD) and theoretical constructs derived from protection motivation theory (PMT) to model persons' adoption of cyber hygiene practices and past victimization experiences. The survey was administered via Mechanical Turk in March 2020. Those who participated in the survey were first presented with informed consent documentation, followed by the questionnaire. Once respondents completed the survey, they were paid through Mechanical Turk. In total, 356 individuals accessed the survey, but only 311 individuals (13% attrition) responded to each of the questions used in the final structural model.

There are notable limitations with the aforementioned data collection strategy. First, and as noted above, not all Internet users in the United States have an equal chance of being included in the survey. It is possible, and even probable, that those who complete surveys for pay differ from those who do not. Additionally, response rates for the items gradually declined as the survey progressed (95.51%-91.85%), meaning respondents were more likely to answer questions at the beginning, rather than the end, of the survey. Those who dropped out before completion may systematically differ from the final sample. Therefore, missing data cannot be assumed to be random. These issues introduce bias into the sample and threaten the generalizability of findings derived using these data. These limitations, among others, are discussed in chapter seven.

Variables of Interest

Victimization – To assess past online victimization experiences, respondents were asked whether the following events transpired over the past 12 months: (1) My computer was infected with a virus; (2) I received messages from someone that threatened, insulted, or harassed me; (3) I was notified 1 or more of my online account(s) had been hacked and personal data was at risk. Response options included yes (which was coded as 1) and no (which was coded as 0). Confirmatory factor analysis was conducted based on responses to these questions to create the first-order latent factor, *victimization*. Since the victimization measurement model only includes three items, it is a saturated model (i.e., the number of free parameters exactly equals the number of known values) with perfect model fit: $\chi 2 = 0.000$, df=0, p = NA; CFI = 1.000; TLI = 1.000; RMSEA = 0.000; SRMR = 0.000. Importantly, each of the factor loadings are significant and above the minimum threshold, indicating good local fit (0.577-0.785) (Nunnally, 1998). Summary statistics for the three items used to create the latent factor are presented in Table 1.

Cyber Hygiene – *Cyber hygiene* consists of 7 ordinal measures regarding Internet users' computer security behaviors in the past 12 months. Specifically, respondents were asked how often they engaged in the following behaviors in the past 12 months: (1) I used complex passwords (including random letters, numbers, and symbols); (2) I shared geographic information on social media; (3) I shared account information on social media; (4) I downloaded something from a non-secure source; (5) I shared my password with someone; (6) I used the same password for multiple accounts; (7) I clicked or opened unfamiliar links. Response options ranged from 1 (never) to 5 (always). Responses for items 2-7 were reverse coded so higher scores correspond with higher levels of cyber hygiene. Lastly, confirmatory factor analysis was conducted based on responses to the questions to create a first-order latent factor. Error terms for items 1 and 6 were correlated because both questions related to password management and error terms for items 2 and 3 were correlated because both questions related to social media engagement. The cyber hygiene measurement model proved to be a good fit to the data: $\chi2$ = 19.638, df=12, p = 0.074; CFI = 0.989; TLI = 0.982; RMSEA = 0.045; SRMR = 0.046. The p-value indicated good absolute fit (i.e., the model chi-square was nonsignificant), and the remaining relative fit indicators all showed that the model fit the data well. Additionally, all of the factor loadings are significant and above the minimum threshold (0.332-0.796) (Nunnally, 1998). Summary statistics for the 7 items used to create the latent factor, *cyber hygiene*, are presented in Table 1. It should be noted the latent factor, *cyber hygiene*, does not include all computer security behaviors Internet users can implement to increase self-protection. Most notably, the measure does not include "anti-virus software" due to issues concerning model fit. Specifically, the inclusion of the item reduced model fit on all observed indices. Anti-virus software differs both conceptually (i.e., technical rather than behavioral) and empirically from the items used to create the final latent construct.

Thoughtfully Reflective Decision Making (TRDM) – In line with past research (Paternoster & Pogarsky, 2009), *TRDM* is measured using the following items: (1) When you have a problem to solve, one of the first things you do is get as many facts about the problem as possible; (2) When you are attempting to find a solution to a problem, you usually try to think of as many different approaches to the problem as possible; (3) When making decisions, you generally use a systematic method for judging and comparing alternatives; (4) After carrying out a solution to a problem, you usually try to analyze what went right and what went wrong. Participants reported their level of agreement to each item using a 4-point Likert scale ranging from 1 (strongly disagree) to 4 (strongly agree). Responses to the four items were then summated to create the final measure, *TRDM* (α=0.768). Higher scores on the index correspond with higher individual-level cognitive decision-making capabilities. Descriptive statistics for the summated scale and individual items used to comprise the scale are presented in Table 2.

Protection Motivation Theory (PMT) Constructs – In essence, PMT posits that when confronted with the threat of future negative outcomes, two parallel cognitive processes are triggered: threat appraisals and coping appraisals. The higher the appraisals, the more likely an individual will engage in self-protective behaviors. Additionally, higher threat appraisals lead to the emotional response of fear, which may also push a decision maker to adopt the behavioral recommendation.

Threat appraisals result in the adoption of recommended behaviors when the perceived threat outweighs the maladaptive route of not adopting the protective behavior. Thus, a decision maker's threat appraisal is the summation of their perception of the threat's severity and their own vulnerability minus the rewards associated with not engaging in the recommended behavior (i.e., maladaptive rewards). The current study, like the majority of examinations of PMT (Boss et al., 2015), operationalize threat appraisals as severity and vulnerability, and exclude maladaptive rewards. Thus, the current study is only a partial test of PMT. This decision, and the corresponding bias it introduces to the current study, is discussed in the chapter seven.

To measure severity, participants were asked to rate their level of agreement to the following statement: “Online victimization is a serious threat.” To measure vulnerability, participants were asked to rate their level of agreement to the following statement: “Online victimization is a probable threat.” Response options ranged from 0 to 100, with higher scores indicating higher levels of agreement with the items. In accordance with PMT, perceived vulnerability and perceived severity are conceptually distinct, but together form what is referred to as the threat appraisal. However, in a recent review of the literature, Sommestad et al. (2015) found Internet users’ perceptions of vulnerability and severity to be highly correlated. The items are also highly correlated in the current study ($r=0.756$, $p=0.000$). Due to issues concerning multicollinearity, these items cannot be included in the same structural model. Thus, severity and vulnerability are summated to create the scale *threat appraisal* ($\alpha=0.855$).

Coping appraisals result in the adoption of recommended behaviors when an individual has faith in the behavioral recommendation proposed to thwart the occurrence of a negative outcome (i.e., *response efficacy*), and their own ability to carry out the recommendation (i.e., *self-efficacy*), but does not perceive the *response cost* associated with adopting the recommendation to be too high. To measure *response efficacy*, participants were asked to rate their level of agreement to the following statement: “Adopting recommended security behaviors will prevent online victimization.” To measure *self-efficacy*, participants were asked to rate their level of agreement to the following statement: “I can prevent online victimization.” Lastly, to measure *response cost*, participants were asked to rate their level of agreement to the following statement: “Protecting myself online is difficult.” Response options ranged from 0 to 100, with higher scores indicating higher levels of agreement with the aforementioned items. Descriptive statistics for the key components central to PMT are presented in Table 2.

Fear – As noted above, an individual’s threat appraisal in the face of a potential negative outcome may spark the emotional response referred to as fear, which in turn, may push a decision maker to engage in protective behaviors (Boss et al., 2015). To measure the emotional response of *fear*, respondents were asked to rate their fear of the following events occurring in the next 12 months: (1) A major data breach where my customer information is stolen; (2) I open a phishing e-mail message that runs malicious code; (3) My computer’s data become locked in a ransomware scheme; (4) My computer will become infected with a virus; (5) I receive a Distributed Denial of Service attack. Response options ranged from 1 (not at all fearful) to 4 (very fearful). Confirmatory factor analysis was conducted based on responses to the aforementioned items to create a first-order latent factor. The fear measurement model proved to be a good fit to the data: $\chi2 = 12.418$, df=5, p = 0.029; CFI = 0.997; TLI = 0.995; RMSEA = 0.069; SRMR = 0.021. Although the p-value indicated a poor absolute fit (i.e., the model chi-square was significant), the remaining relative fit indicators showed that the model fit the data well. Additionally, all of the factor loadings are significant and above the minimum threshold (0.743-0.925) (Nunnally, 1998). Summary statistics for the 5 items used to create the latent factor, *fear*, are presented in Table 1.

Control Variables

Since the current study does not employ a randomized control trial, it is impossible to rule out all alternative hypotheses (Campbell & Stanley, 2015). However, the inclusion of control variables can reduce the occurrence of omitted variable bias. Therefore, respondents were asked a series of questions concerning their level of self-control, computer skill, education, race, age, and sex. A correlation matrix and list of survey items are provided in Appendices A and B, respectively.

Low Self-Control – Low self-control has been found to increase Internet users' probability of experiencing online victimization (Reyns et al., 2019). The relationship between low self-control and victimization experiences is likely mediated by the adoption of self-protective behaviors. Thus, individuals with low self-control may adopt lower levels of cyber hygiene practices leading to increased victimization experiences. For this reason, *low self-control* is included as a control variable. An abridged self-control questionnaire taken from the Personal and Relationships Profile (Straus et al., 1999) and validated by Rebellon et al. (2008) was used to measure respondents' self-control, or the lack thereof. The questionnaire consists of six items to measure each of the six dimensions of self-control specified in *The general theory of crime* (Gottfredson & Hirschi, 1990): impulsivity, a preference for simple tasks, risk-seeking, physicality, self-centeredness, and a bad temper.

Specifically, respondents were asked to report their level of agreement to the following statements: (1) I don't think about how what I do will affect other people; (2) I often do things that other people think are dangerous; (3) There is nothing I can do to control my feelings when someone hassles me; (4) I often get hurt by things that I do; (5) I have trouble following the rules at work or in school; (6) I have goals in life that I try to reach. Response options ranged from 1 (strongly disagree) to 4 (strongly agree). Item 6 was reverse coded so higher scores represent lower levels of self-control. Lastly, confirmatory factor analysis was conducted based on responses to the six survey items to create a first-order latent factor. The low self-control measurement model proved to be a good fit to the data: $\chi 2 = 46.114$, df= 9, p = 0.000; CFI = 0.957; TLI = 0.928; RMSEA = 0.115; SRMR = 0.054. Although the p-value indicated a poor absolute fit (i.e., the model chi-square was significant), the remaining relative fit indicators showed that the model fit the data well. Additionally, all of the factor loadings are significant and above the minimum threshold (0.541-0.844) (Nunnally, 1998). Summary statistics for the six items used to create the latent factor are presented in Table 1.

Computer Skill – It is also plausible that higher levels of computer skill increase engagement in cyber hygiene practices and reduce victimization experiences (Yucedal, 2010). Thus, *computer skill* is included as a control variable. To assess computer skill, respondents were asked to rank how skilled they are at using the following technologies on a range from novice (1) to expert (100): (1) Dealing with software problems; (2) Removing malware from your computing devices (e.g., computer viruses); (3) Dealing with computer hardware problems; (4) Modifying the firewall on your computing devices; (5) Establishing a virtual proxy network on your computing devices; (6) Storing digital information on a cloud-based platform (e.g., Dropbox, OneDrive, Box, iCloud). Responses to the questions were then summated to create the final measure, *computer skill* (α=0.889). Higher scores on the index correspond with higher levels of computer skill. Descriptive statistics for the scale are presented in Table 2.

Demographic Characteristics – Demographic characteristics (i.e., education, race, age, and sex) have also been shown to explain variation in computer security behaviors (Chua et al., 2018) and victimization experiences (Bunch et al., 2015). Thus, respondents were asked questions pertaining to their educational attainment, racial identity, age, and sex. *Education* is coded as an ordinal variable ranging from 1 (high school diploma or GED) to 6 (graduate degree). Race was transformed into a dummy variable (*White*), and those who self-reported as White were given a score of 1 and those who did not were given a score of 0. *Age* is coded as an ordinal variable ranging from 1 (18-24 years old) to 7 (75 years or older). Lastly, the dummy variable, *male,* was generated based on respondents' self-reported sex. Admittedly, this is an imperfect measure. Respondents should have been asked to self-report their gender identity, with more options available to them. However, given the limited variation that would have existed based on the relatively small sample size, it is probable that a dummy variable with the same (or similar) distribution would have been generated. Descriptive Statistics for the demographic control variables are presented in Table 2 and a brief description of the sample is presented directly below.

In total, 12.86% of respondents reported having a high school diploma or GED, 17.04% reported having "some college, but no degree," 16.72% reported having an associate degree, 40.51% reported having a bachelor's degree, 1.93% reported having "some graduate courses but no graduate degree," and finally, 10.93% reported having a graduate degree (e.g., MA, JD, PHD). Of the respondents, 82.96% of were White and 17.04% were non-White. In total, less than 1% of the respondents (0.64%) were between the ages of 18-24, 28.30% were between the ages of 25-34, 33.44% were between the ages of 35-44, 20.90% were between the ages of 45-54, 11.25% were between the ages of 55-64, 5.14% were between the ages of 65-74, and finally, less than 1% (0.32%) were 75 years of age or older. Lastly, 44.69% self-identified as male and 55.31% identified as female.

Data Analysis

Structural equation modeling (SEM) is a multivariate statistical analysis technique that combines factor analysis and multiple regression analysis to analyze the structural relationship between measured variables and latent constructs. SEM is believed to be the most appropriate method for assessing mediation and indirect effects (Gunzler et al., 2013). Since the current study includes latent constructs, tests for mediation (hypothesis 9), and estimates indirect effects (hypotheses 10 and 11), SEM is the appropriate data analytic technique. Therefore, SEM is used to test the eleven hypotheses and evaluate the measurement models. Data are analyzed using the weighted least squares mean and variance (WLSMV) estimator through the R package, Lavaan version 0.6-7. The WLSMV estimator is appropriate for models with categorical predictors and outcomes (Bollen, 1989). Each model is assessed using the following goodness-of-fit indices, with acceptable threshold levels presented in parentheticals: the chi-square test (p>0.050), the comparative fit index (CFI>0.950), the Tucker-Lewis index (TLI>0.950), the root mean square error approximation (RMSEA<0.070), and the standardized root mean square residual (SRMR<0.080) (Hooper et al., 2008; Hu & Bentler, 1999).

Table 1. Summary Statistics and Factor Loadings of Indicator Variables for Latent Factors (n=311).

Measure	Percent	Estimate	SE	p-value	Factor Loading
Victimization					
Victimization 1					
Yes	10.61	1.000			0.577
No	89.39				
Victimization 2					
Yes	10.29	1.049	0.312	0.001	0.605
No	89.71				
Victimization 3					
Yes	32.15	1.360	0.526	0.010	0.785
No	67.85				
Cyber Hygiene					
Cyber Hygiene 1					
Always	25.72	1.000			0.332
Often	38.91				
Sometimes	22.83				
Rarely	10.29				
Never	2.25				
Cyber Hygiene 2					
Never	52.09	1.555	0.332	0.000	0.516
Rarely	28.62				
Sometimes	13.18				
Often	4.18				
Always	1.93				
Cyber Hygiene 3					
Never	84.24	1.877	0.395	0.000	0.623
Rarely	9.32				
Sometimes	2.89				
Often	2.57				
Always	0.96				
Cyber Hygiene 4					
Never	63.02	2.149	0.427	0.000	0.713
Rarely	22.83				
Sometimes	10.61				
Often	2.25				
Always	1.29				

Table 1. (continued).

Measure	Percent	Estimate	SE	p-value	Factor Loading
Cyber Hygiene 5					
Never	85.21	1.962	0.397	0.000	0.651
Rarely	10.29				
Sometimes	2.57				
Often	1.61				
Always	0.32				
Cyber Hygiene 6					
Never	37.62	1.649	0.305	0.000	0.547
Rarely	20.58				
Sometimes	26.37				
Often	11.58				
Always	3.86				
Cyber Hygiene 7					
Never	73.31	2.399	0.451	0.000	0.796
Rarely	17.68				
Sometimes	6.75				
Often	1.93				
Always	0.32				
Fear					
Fear 1					
Not at all Fearful	10.29	1.000			0.743
Somewhat not Fearful	33.44				
Somewhat Fearful	45.66				
Very Fearful	10.61				
Fear 2					
Not at all Fearful	36.33	1.190	0.056	0.000	0.884
Somewhat not Fearful	32.15				
Somewhat Fearful	25.08				
Very Fearful	6.43				
Fear 3					
Not at all Fearful	36.66	1.244	0.057	0.000	0.925
Somewhat not Fearful	30.55				
Somewhat Fearful	21.54				
Very Fearful	11.25				
Fear 4					
Not at all Fearful	16.40	1.106	0.053	0.000	0.822
Somewhat not Fearful	35.37				
Somewhat Fearful	38.59				
Very Fearful	9.65				

Table 1. (continued).

Measure	Percent	Estimate	SE	p-value	Factor Loading
Fear 5					
Not at all Fearful	46.30	1.068	0.055	0.000	0.794
Somewhat not Fearful	30.55				
Somewhat Fearful	14.79				
Very Fearful	8.36				
Low Self-Control					
Low Self-Control 1					
Strongly Disagree	44.37	1.000			0.617
Disagree	48.23				
Agree	5.78				
Strongly Agree	1.61				
Low Self-Control 2					0.704
Strongly Disagree	62.70	1.142	0.100	0.000	
Disagree	27.33				
Agree	8.04				
Strongly Agree	1.93				
Low Self-Control 3					
Strongly Disagree	43.73	0.999	0.098	0.000	0.616
Disagree	41.16				
Agree	12.86				
Strongly Agree	2.25				
Low Self-Control 4					
Strongly Disagree	54.34	1.313	0.107	0.000	0.810
Disagree	39.87				
Agree	5.14				
Strongly Agree	0.64				
Low Self-Control 5					
Strongly Disagree	63.99	1.368	0.114	0.000	0.844
Disagree	29.90				
Agree	4.50				
Strongly Agree	1.61				
Low Self-Control 6					
Strongly Agree	43.41	0.877	0.098	0.000	0.541
Agree	51.13				
Disagree	2.89				
Strongly Disagree	2.57				

Note. The ‘Estimate’ column reports unstandardized regression coefficients; The ‘SE’ column reports the standard error of the estimate.

Table 2. Summary Statistics for Observed Variables (n=311).

Measure	Alpha	Percent	Mean	Standard Deviation	Range	
TRDM	0.768		13.251	2.095	4	16
TRDM 1			3.441	0.592	1	4
Strongly Disagree		0.96				
Disagree		2.55				
Agree		48.55				
Strongly Agree		48.23				
TRDM 2			3.328	0.692	1	4
Strongly Disagree		1.93				
Disagree		7.07				
Agree		47.27				
Strongly Agree		43.73				
TRDM 3			3.251	0.687	1	4
Strongly Disagree		1.29				
Disagree		10.29				
Agree		50.48				
Strongly Agree		37.94				
TRDM 4			3.232	0.748	1	4
Strongly Disagree		2.25				
Disagree		12.22				
Agree		45.66				
Strongly Agree		39.87				
Threat Appraisal	0.855		151.707	42.374	14	200
Response Efficacy			75.830	19.653	1	100
Self-Efficacy			68.135	24.295	0	100
Response Cost			31.415	27.135	0	100
Computer Skill	0.889		343.804	141.793	16	600

Table 2. (continued).

Measure	Alpha	Percent	Mean	Standard Deviation	Range	
Education			3.444	1.428	1	6
High school diploma or GED		12.86				
Some college, but no degree		17.04				
Associate degree		16.72				
Bachelor’s degree		40.51				
Some graduate courses but no graduate degree		1.93				
Graduate degree		10.93				
White		82.96			0	1
Age			3.305	1.180	1	7
18-24 years old		0.64				
25-34 years old		28.30				
35-44 years old		33.44				
45-54 years old		20.90				
55-64 years old		11.25				
65-74 years old		5.14				
75 years or older		0.32				
Male		44.69			0	1

Note. TRDM=thoughtfully reflective decision making.

Chapter Six:
Results

As noted above, the measurement models and aforementioned hypotheses are assessed using structural equation modeling. The final structural model, as depicted in Figure 2, includes seven regressions assessing variation in *victimization*, *threat appraisal*, *response efficacy*, *self-efficacy*, *response cost*, *fear*, and *cyber hygiene*. In the final structural model, error terms are correlated for the following variables: *fear* and *victimization*, *response efficacy* and *self-efficacy*, and *response efficacy* and *response cost*. Error terms for *fear* and *victimization* are correlated because of the established correlation between the constructs (e.g., Tseloni & Zarafonitou, 2008). Although correlated error terms account for unexplained variation between the two latent constructs, *fear* is not included in the regression equation predicting victimization because it would create a non-recursive model that is more appropriately assessed using longitudinal data. This of course introduces the possibility of omitted variable bias, which is discussed in the following chapter. Error terms for *response efficacy*, *self-efficacy*, and *response cost* are correlated because together they form the coping appraisal (Rogers, 1983) and have been found to be highly correlated when examining computer security behaviors (Sommestad et al., 2015). The overall structural model, depicted in Figure 2, proved to be a good fit to the data: $\chi2$ = 579.969, df=367, p = 0.000; CFI = 0.944; TLI = 0.954; RMSEA = 0.043; SRMR = 0.076. Although the p-value indicated a poor absolute fit (i.e., the model chi-square was significant), the remaining relative fit indicators showed that the model fit the data well.

The current study has two primary objectives, the first of which is to determine whether engagement in cyber hygiene practices reduces Internet users' online victimization experiences.

Table 3, panel 1, presents the results of the regression equation assessing the effect of *cyber hygiene* on *victimization* while controlling for the following rival explanations: *TRDM*, *low self-control*, *computer skill*, *education*, *White*, *age*, *male*. Providing support of the first hypothesis, higher levels of engagement in cyber hygiene practices is associated with a decrease in Internet users' victimization experiences (b=-0.514, *p*=0.023). Interestingly, *cyber hygiene* is the only significant predictor of *victimization*.

Since the adoption of cyber hygiene practices is associated with a reduction in victimization experiences, the current study shifts to the second objective of developing a theoretical model capable of explaining why some individuals fail to adopt good cyber hygiene practices in the face of cyber threats despite their now proven effectiveness at reducing victimization experiences. In doing so, a newly developed theoretical model in which thoughtfully reflective decision making (TRDM) operates through protection motivation theory (PMT) constructs to explain variation in Internet users' engagement in cyber hygiene practices is introduced. The first step in evaluating this processual model is to determine whether TRDM is associated with key PMT constructs.

Table 3, panels 2-4, present the regression equations estimating the direct effects of *TRDM* on the three components that comprise one's coping appraisal (i.e., *response efficacy*, *self-efficacy*, and *response cost*). As depicted in panel 2, *TRDM* is positively associated with *response efficacy* (b=1.451, *p*=0.002). In other words, thoughtfully reflective decision makers are more likely to have faith in cyber hygiene as a means to prevent online victimization. Additionally, *low self-control* is negatively associated (b=-5.161, *p*=0.007) and *computer skill* positively associated (b=0.027, *p*=0.001) with *response efficacy*. Stated differently, individuals with low levels of self-control have less faith in cyber hygiene, while those with increased computer skill have more faith in cyber hygiene, to prevent the occurrence of online victimization.

TRDM, however, is not significantly associated with *self-efficacy* (b=0.194, *p*=ns) or *response cost* (b=-0.983, *p*=ns), which is illustrated in Table 3, panels 3 and 4, respectively. Interestingly, *low self-control* is negatively associated with *self-efficacy* (b=-6.197, *p*=0.010) and positively associated with *response cos*t (b=10.486, *p*=0.00). In other words, individuals with low self-control do not have faith in their ability to engage in the cyber hygiene practices required to reduce victimization experiences and have higher perceptions of the costs associated with good cyber hygiene. Conversely, *computer skill* is associated with an increase in individual's faith in their ability to prevent victimization experiences (i.e., *self-efficacy*) (b=0.049, *p*=0.000) and a decrease in their perceptions of the costs associated with engaging in cyber hygiene practices (i.e., *response cost*) (b=-0.054, *p*=0.000). Lastly, *education* is positively associated with *response cost* (b=3.391, *p*=0.002). More educated persons have higher perceptions of the costs associated with self-protection in the cyber-environment. Taken together, hypothesis 2 is only partially supported since TRDM is only associated with one of the three components that comprise one's coping appraisal. Additionally, findings provide support for Gottfredson and Hirschi's (1990) *A general theory of crime*, in that self-control is associated with all three components that comprise one's coping appraisal.

Recall that severity and vulnerability are highly correlated (r=0.756, *p*=0.000), presenting issues with multicollinearity when included in the same structural model. Thus, a summated scale, *threat appraisal*, is included as an endogenous variable in the final structural model. Table 3, panel 5, demonstrates that *TRDM* is positively associated with *threat appraisal* (b=2.613, *p*=0.004). In other words, thoughtfully reflective decision makers have higher threat appraisals when confronted with the threat of a potential negative outcome, thus providing support for hypothesis 3. Moreover, *age* (b=6.407, *p*=0.007) is positively associated with *threat appraisal* whereas being *male* (b=-11.465, *p*=0.015) and *White* (b= -14.647, *p*=0.030) is negatively associated with respondents' *threat appraisal*.

In accordance with PMT, threat appraisals are hypothesized to elicit the emotional response referred to as fear (Boss et al., 2015). Findings, as presented in Table 3, panel 6, indicate that *threat appraisal* is positively associated with *fear* (b=0.006, *p*=0.000) in a manner consistent with the theory and hypothesis 4. L*ow self-control* is also positively and significantly associated with *fear* (b=0.455, *p*=0.000).

Three regression models were employed to assess the direct effects of TRDM and PMT constructs on cyber hygiene and the indirect effects of TRDM on cyber hygiene through PMT constructs. These three models are also used to assess whether PMT constructs partially mediate the effect of TRDM on cyber hygiene. Table 3, panel 7, presents the results from the structural model assessing the effect of *both* TRDM and PMT constructs on cyber hygiene. Table 4 presents the results from identical structural models, with the omission of TRDM (model 1[1]) and PMT constructs (model 2[2]) in the regression equation predicting cyber hygiene.

Table 4, model 1, illustrates the direct effect of *TRDM* on *cyber hygiene* in the absence of PMT constructs. Findings demonstrate that higher levels of TRDM are associated with increased adoption of cyber hygiene practices (b=0.039, *p*=0.007), providing support for hypothesis 6. Additionally, *age* (b=0.091, *p*=0.002) and *computer skill* (b=0.001, *p*=0.008) are associated with an increase in cyber hygiene engagement, whereas *low self-control* is associated with a decrease

[1] Model fit indices: $\chi2$ = 599.522, df=368, p = 0.000; CFI = 0.939; TLI = 0.950; RMSEA = 0.045; SRMR = 0.077.

[2] Model fit indices: $\chi2$ = 585.855, df=368, p = 0.000; CFI = 0.943; TLI = 0.953; RMSEA = 0.044; SRMR = 0.076.

in cyber hygiene engagement (b=-0.366, *p*=0.000). Model 1, which only includes TRDM and relevant control variables, explains about 38% of the latent categorical response variable (y*).

Table 4, model 2, depicts the direct effects of key theoretical constructs derived from PMT on *cyber hygiene* in the absence of *TRDM*. Findings demonstrate that *threat appraisal* (b=0.003, *p*=0.000) and *response efficacy* (b=0.009, *p*=0.003) are associated with *cyber hygiene* and statistically significant at the conventional p-value < 0.050. Both *threat appraisal* and *response efficacy* operate in the anticipated direction and increase Internet users' cyber hygiene engagement. Conversely, *self-efficacy*, which is marginally not-significant (b=-0.005, *p*=0.051), operates in a manner inconsistent with PMT and is associated with a decrease in Internet users' adoption of cyber hygiene practices. The final PMT construct included in the model, *response cost*, is nonsignificant (b=-0.000, *p*=ns) but operates in the hypothesized direction. The effect of *low self-control* (b=-0.269, *p*=0.000), *computer skill* (b=0.001, *p*=0.030), and *age* (b=0.083, *p*=0.003) remain significant and operate in the same direction as they did in model 1. Taken together, hypothesis 7 is partially supported since one (i.e., *response efficacy*) of the three components that comprise one's coping appraisal is associated with cyber hygiene adoption. Hypothesis 8, however, is supported since threat appraisals increase Internet users' adoption of cyber hygiene practices. Model 2, which only includes PMT constructs and relevant control variables, explains about 44% of the latent categorical response variable (y*).

Table 3, panel 7, presents the direct effects of both *TRDM* and PMT constructs on *cyber hygiene* simultaneously, in addition to the indirect effects of *TRDM* on cyber *hygiene* through PMT constructs (i.e., *threat appraisal* and *response efficacy*). Interestingly, the full model only explains about 42% of the latent categorical response variable (y*), which is less than the amount of explained variance in Table 4, model 2. In regard to the control variables, *low self-control* (b=-0.269, *p*=0.000), *computer skill* (b=0.000, *p*=0.048), and *age* (b=0.082, *p*=0.004) remain significant and operate in the same direction depicted in Table 4. Interestingly, low self-control remained significant in all three models, providing additional support for Gottfredson and Hirschi's (1990) theory. Note that *fear* is not associated with *cyber hygiene*, thus support for hypothesis 5 is not found. *Threat appraisal* (b=0.003, *p*=0.000) and *response efficacy* (b=0.005, *p*=0.007), which were the only PMT constructs associated with Internet users' adoption of cyber hygiene practices at the conventional level of p-value < 0.050 in Table 4, remain the only two significant predictors.

Additionally, the direct effect of *TRDM* on *cyber hygiene* remains significant and in the hypothesized direction (b=0.031, *p*=0.034), thus PMT constructs do not fully mediate the effect of TRDM on Internet users' adoption of self-protective behaviors. However, there is a reduction in the amount of variation in cyber hygiene adoption explained by TRDM in Table 3, panel 7, compared to Table 4, model 1, which, coupled with the indirect effects reported below, provide support for hypothesis 9 in that PMT constructs partially mediate the effect of TRDM on cyber hygiene.

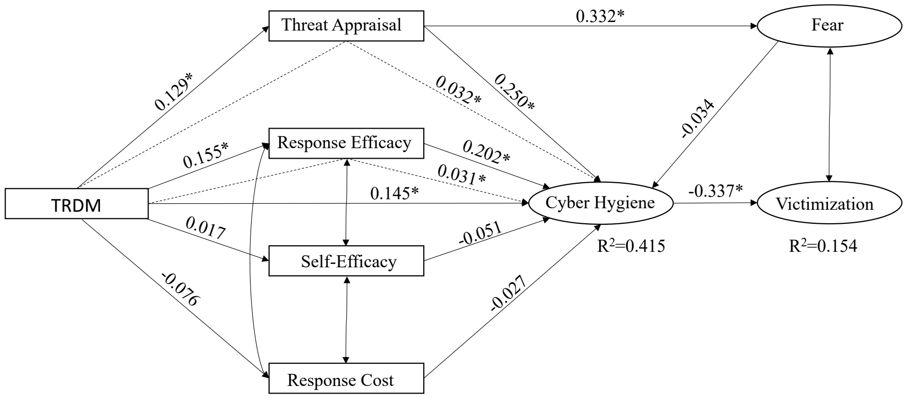

Figure 3. Structural Model Examining the Processual Relationship Between Thoughtfully Reflective Decision Making, Protection Motivation Theory Constructs, Cyber Hygiene, and Victimization.

Note. Error terms not depicted in the figure and nonsignicant indirect paths have been removed for ease of presentation; Standardized coefficents are reported; TRDM=thoughtfully reflective decision making; Control variables include: low self-control, computer skill, education, White, age, male; Model fit indices: $\chi 2$ = 579.969, df=367, p = 0.000; CFI = 0.944; TLI = 0.954; RMSEA = 0.043; SRMR = 0.076.
**p*<0.050.

Finally, *TRDM* was found to have indirect effects on *cyber hygiene* through both *threat appraisal* (b=0.007, *p*=0.016) and *response efficacy* (b=0.007, *p*=0.037). Two additional models examining the indirect effects of *TRDM* on *cyber hygiene* through *self-efficacy* and *response cost* were estimated, but the indirect effects were nonsignificant. Therefore, hypothesis 11 (i.e., the indirect effect of TRDM through threat appraisals will increase Internet users' adoption of cyber hygiene practices) is fully supported. However, since indirect effects were only observed when examining the effect of *TRDM* through *response efficacy*, hypothesis 10 (i.e., the indirect effect of TRDM through coping appraisals will increase Internet users' adoption of cyber hygiene practices) is only partially supported. A path model of the processual relationship between TRDM, PMT constructs, cyber hygiene, and victimization is depicted in Figure 3.

Table 3. Structural Model Results (n=311).

	Estimate	SE	p-value	β
Panel 1				
Victimization				
Cyber Hygiene	-0.514*	0.225	0.023	-0.337
TRDM	0.014	0.034	0.689	0.043
Low Self-Control	0.091	0.122	0.458	0.078
Computer Skill	0.000	0.001	0.432	0.088
Education	-0.012	0.042	0.771	-0.026
White	-0.249	0.163	0.126	-0.139
Age	0.043	0.058	0.455	0.075
Male	-0.169	0.132	0.200	-0.125
R^2		0.154		
Panel 2				
Response Efficacy				
TRDM	1.451*	0.471	0.002	0.155
Low Self-Control	-5.161*	1.898	0.007	-0.153
Computer Skill	0.027*	0.008	0.001	0.198
Education	-0.078	0.813	0.924	-0.006
White	-1.874	3.450	0.587	-0.036
Age	0.906	0.888	0.307	0.055
Male	-1.153	2.228	0.605	-0.029
R^2		0.100		
Panel 3				
Self-efficacy				
TRDM	0.194	0.691	0.779	0.017
Low Self-Control	-6.197*	2.418	0.010	-0.148
Computer Skill	0.049*	0.010	0.000	0.285
Education	0.027	0.971	0.978	0.002
White	0.195	3.651	0.957	0.003
Age	1.986	1.150	0.084	0.097
Male	-0.189	2.734	0.945	-0.004
R^2		0.106		
Panel 4				
Response Cost				
TRDM	-0.983	0.683	0.150	-0.076
Low Self-Control	10.486*	2.883	0.000	0.225
Computer Skill	-0.054*	0.012	0.000	-0.285
Education	3.391*	1.082*	0.002	0.179
White	5.853	4.437	0.187	0.081
Age	-1.784	1.272	0.161	-0.078
Male	-1.124	3.074	0.715	-0.021
R^2		0.173		

Table 3. (continued).

	Estimate	SE	p-value	β
Panel 5				
Threat Appraisal				
TRDM	2.613*	0.897	0.004	0.129
Low Self-Control	-7.111	3.859	0.065	-0.098
Computer Skill	0.009	0.015	0.563	0.029
Education	-0.752	1.867	0.687	-0.025
White	-14.647*	6.768	0.030	-0.130
Age	6.407*	2.367	0.007	0.179
Male	-11.465*	4.696	0.015	-0.135
R^2			0.093	
Panel 6				
Fear				
Threat Appraisal	0.006*	0.001	0.000	0.332
TRDM	0.025	0.023	0.271	0.067
Low Self-Control	0.455*	0.081	0.000	0.337
Computer Skill	-0.001	0.000	0.064	-0.111
Education	0.017	0.033	0.602	0.031
White	-0.163	0.125	0.195	-0.078
Age	0.036	0.041	0.378	0.054
Male	-0.128	0.094	0.174	-0.082
R^2			0.263	
Panel 7				
Cyber Hygiene				
TRDM	0.031*	0.014	0.034	0.145
Threat Appraisal	0.003*	0.001	0.000	0.250
Response Efficacy	0.005*	0.002	0.007	0.202
Self-Efficacy	-0.001	0.001	0.434	-0.051
Response Cost	-0.000	0.001	0.664	-0.027
Fear	-0.019	0.039	0.623	-0.034
Low Self-Control	-0.269*	0.067	0.000	-0.352
Computer Skill	0.000*	0.000	0.048	0.151
Education	-0.021	0.021	0.320	-0.068
White	0.026	0.076	0.729	0.022
Age	0.082*	0.028	0.004	0.217
Male	-0.045	0.062	0.466	-0.051
R^2			0.415	
Indirect effects of TRDM on Cyber Hygiene through the mediator variables Threat Appraisal and Response Efficacy				
TRDM via Threat Appraisal	0.007*	0.003	0.016	0.032
TRDM via Response Efficacy	0.007*	0.003	0.037	0.031

Note. Model fit indices: $\chi 2$ = 579.969, df=367, p = 0.000; CFI = 0.944; TLI = 0.954; RMSEA = 0.043; SRMR = 0.076; The 'Estimate' column reports unstandardized regression coefficients; The 'SE' column reports the standard error of the estimate; The 'β' column reports the standardized regression coefficients; TRDM=thoughtfully reflective decision making.
**p*<0.050.

Table 4. Structural Model Results for Assessing Mediation (n=311).

	Model 1.				**Model 2.**			
	TRDM on Cyber Hygiene				**PMT on Cyber Hygiene**			
Measures	**Estimate**	**SE**	**p-value**	**β**	**Estimate**	**SE**	**p-value**	**β**
TRDM	0.039*	0.014	0.007	0.194	-	-	-	-
Threat Appraisal	-	-	-	-	0.003*	0.001	0.000	0.267
Response Efficacy	-	-	-	-	0.009*	0.003	0.003	0.411
Self-Efficacy	-	-	-	-	-0.005	0.002	0.051	-0.253
Response Cost	-	-	-	-	-0.000	0.001	0.666	-0.027
Fear	0.057	0.035	0.100	0.106	-0.020	0.038	0.595	-0.037
Low Self-Control	-0.366*	0.073	0.000	-0.498	-0.269*	0.068	0.000	-0.359
Computer Skill	0.001*	0.000	0.008	0.203	0.001*	0.000	0.030	0.168
Education	-0.024	0.022	0.268	-0.083	-0.020	0.021	0.342	-0.067
White	-0.002	0.073	0.983	-0.001	0.038	0.080	0.635	0.033
Age	0.091*	0.029	0.002	0.256	0.083*	0.028	0.003	0.227
Male	-0.060	0.061	0.324	-0.071	-0.038	0.063	0.544	-0.044
R^2	0.384				0.443			

Note. The 'Estimate' column reports unstandardized regression coefficients; The 'SE' column reports the standard error of the estimate; The 'β' column reports the standardized regression coefficients; TRDM=thoughtfully reflective decision making; PMT=protection motivation theory; Model 1 fit indices: $\chi2$ = 599.522, df=368, p = 0.000; CFI = 0.939; TLI = 0.950; RMSEA = 0.045; SRMR = 0.077; Model 2 fit indices: $\chi2$ = 585.855, df=368, p = 0.000; CFI = 0.943; TLI = 0.953; RMSEA = 0.044; SRMR = 0.076.
**p*<0.050.

Chapter Seven: Discussion

Regardless the metric or report used, cybercrime is among the greatest threats to the national security interests of the United States and developed countries around the globe (Department of Homeland Security, 2020). It is estimated that cybercrime incidents cost the global economy billions of dollars annually (McAfee, 2017) and nearly all businesses have attacks launched against them (Ponemon Institute, 2016). Additionally, cyber-attacks against individuals are on the rise (IC3, 2020) with no evidence of a downward trend (Holt, 2011) in the absence of proactive mitigation efforts that consider both the human and technical components of a cybercrime incident (Maimon & Louderback, 2019). Understanding the behavioral patterns of the individuals constituting the cyber-environment is the first step in developing evidence-based policies and strategies aimed to protect Internet users.

It is believed that a symbiotic relationship exists between offenders, guardians, targets, and enablers within the cyber-environment (Maimon & Louderback, 2019). The literature has overwhelming demonstrated that (motivated) cyber-offenders, in attempt to maximize pleasure while avoiding pain (Becker, 1968), choose their targets based on suitability and the lack of capable guardianship (Bossler & Holt, 2009; Choi, 2008; Choi & Lee, 2017; Holt & Bossler, 2013; Holt et al., 2018; Howell et al., 2019; Kigerl, 2012; Maimon et al., 2013; Marcum et al., 2010; Perkins et al., 2020; Pratt et al., 2010; Song et al., 2015; Van Wilsem, 2011; Wilsem, 2013), in a manner consistent with the propositions set forth by Cohen and Felson (1979).

Since cybersecurity companies have been unsuccessful at keeping Internet users safe from cyber-attacks (Holt, 2011; IC3, 2020; Maimon & Louderback, 2019; McAfee, 2017;

Ponemon Institute, 2016), and since law enforcement officers are unable to prevent cybercrime incidents (Burruss et al., 2019), Internet users (i.e., targets (Maimon & Louderback, 2019)) are responsible for their own self-protection. Reducing motivated offenders' opportunities to offend is the overarching goal of situational crime prevention (SCP) (Clarke, 1983), and in accordance with the perspective, "the most obvious way to reduce criminal opportunities is to obstruct or target harden" (Clarke, 1983, p. 241). The current study posits cyber hygiene as analogous to target hardening in the cyber-environment. Cyber hygiene can be thought of as a set of best practices, that when combined, reduce the risks of Internet connectivity. Although some of these practices have been found to reduce susceptibility to victimization, (Bossler & Holt, 2009; Choi, 2008; Holt & Bossler, 2013; Levesque et al., 2013, 2016; Wilsem, 2013), and although multiple academic papers and industry reports discuss the importance of cyber hygiene in achieving self-protection in the cyber-environment (Maennel et al., 2018), the current study is the first to empirically assess whether cyber hygiene reduces Internet users' online victimization experiences.

After assessing whether cyber hygiene reduces victimization experiences in a manner consistent with SCP, the current study shifts to developing a theoretical model capable of predicting self-protection in the cyber-environment. Specifically, the current study developed and assessed a cross-disciplinary integrated model in which thoughtfully reflective decision making (TRDM) has a direct and indirect effect on cyber hygiene through protection motivation theory (PMT) constructs. Several interesting findings, supporting the existence of a processual relationship between TRDM, PMT constructs, cyber hygiene, and victimization emerge. Key findings are summarized in Table 5.

Firstly, garnering support for hypothesis 1 and the SCP perspective, Internet users' adoption of cyber hygiene practices is negatively and significantly associated with experiencing online victimization. As established by SCP scholars (Clarke, 1983, 1997, 1999; Cornish & Clarke, 2003), and embedded in the rational choice framework more generally (Becker, 1968; McCarthy, 2002), offenders act with agency and seek suitable targets lacking capable guardianship (Cohen & Felson, 1979) to maximize pleasure and minimize pain. By adopting cyber hygiene practices, Internet users are engaging in an act the SCP literature refers to as "target hardening" (Clarke, 1983). Target hardening simultaneously increases guardianship and decreases suitability, reducing opportunities for potential offenders to engage in crimes to or against the Internet user.

After establishing self-protection in the form of cyber hygiene reduces Internet users' likelihood of experiencing victimization, the current study assessed why some individuals choose not to engage in self-protective behaviors despite their now proven effectiveness at preventing cybercrime incidents. Findings indicate that when confronted with a cyber threat, thoughtfully reflective decision makers have higher threat appraisals: they view the repercussions of a cyber-attack as severe and believe themselves to be vulnerable, which is an accurate assessment given online victimization is indeed both probable and severe (Maimon & Louderback, 2019). Thus, hypothesis 3 is fully supported. Additionally, and in support of hypothesis 4, Internet users' threat appraisals elicit the emotional response, fear. Stated differently, higher threat appraisals are associated with increased fear of victimization.

Only partial support is garnered for hypothesis 2, which states: higher levels of TRDM will increase Internet users' coping appraisals. Specifically, TRDM is associated with increased response efficacy, but not associated with self-efficacy or response cost. Perhaps thoughtfully reflective decision makers are more likely to have faith in the behavioral recommendations proposed to thwart the occurrence of a negative outcome (i.e., response efficacy) due to their increased ability to evaluate empirical evidence. Individuals with lesser cognitive decision-making capabilities may struggle to identify and discern credible sources of information. Conversely, self-efficacy and response cost relate to Internet users' trust in their own ability to prevent cyber-attacks and the personal costs of doing so, respectively. Perhaps thoughtfully reflective decision makers recognize the probability of being victimized (as supported in hypothesis 2) and as a result believe victimization to be inevitable regardless of their personal attempts to prevent it. A similar explanation can be used to explain the lack of a relationship between response cost and TRDM. In the current study, response cost is operationalized as the difficulty associated with self-protection. Due to thoughtfully reflective decision makers assessment of their own vulnerability, they may believe self-protection to be difficult if not impossible to achieve. Given the probability of being victimized, this may be an accurate assessment.

Next, the direct effects of TRDM and PMT constructs on cyber hygiene engagement were assessed. Fear is not associated with increased cyber hygiene, thus hypothesis 5 is not supported. Fear, which is intended to serve as an emotional response elicited by the threat appraisal (Rogers, 1983), may have less relevance given the hypothetical nature of the survey design. A proper examination of the propositions inherent within PMT would require the introduction of a fear appeal (i.e., a warning regarding the threat of a negative outcome), which then triggers two independent parallel cognitive processes: threat appraisals and coping appraisals. Persons' threat appraisals would then elicit the emotional response of fear, which in turn should have a direct effect on protection motivation. Although respondents' threat appraisals were associated with fear in a manner consistent with theory (and hypothesis 4), it is possible the direct effect of fear on cyber hygiene was not observed because respondents gauged fear objectively (rather than emotionally) based on their perceptions of threat. In other words, the latent construct fear, due to the survey design, was not operationalized in a manner consistent with PMT.

Conversely, support was garnered for hypotheses 6 and 8, respectively, in finding that TRDM and threat appraisals are positively and significantly associated with Internet users' level of engagement in cyber hygiene practices. These findings are consistent with past studies examining the direct effects of TRDM (Howell et al., 2021) and threat appraisals (Sommestad et al., 2015) on online protective behaviors. Hypothesis 7 (i.e., higher coping appraisals will increase Internet users' adoption of cyber hygiene practices) however, is only partially supported. Specifically, response efficacy increases internet users' engagement in self-protective behaviors, whereas self-efficacy and response cost are not significant predictors of cyber hygiene engagement. It is possible the inclusion of other variables in the regression equation, such as computer skill, explained away the direct effects self-efficacy and response cost typically have on computer security behaviors. Internet users with greater computer skill are more likely to believe in their ability to thwart victimization attempts (self-efficacy), less likely to view self-protection as "difficult" (response cost), and more likely to engage in cyber hygiene practices. Findings presented here suggest that computer skill, not self-efficacy and response cost, predict engagement in online security behaviors. If true, tests of PMT that fail to consider computer skill suffer from omitted variable bias, casting doubt on the meta-analytic findings presented by Sommestad et al. (2015). Future studies must parse out the relationship between computer skill and PMT constructs.

Findings also demonstrate the existence of a processual relationship in which TRDM operates indirectly through Internet users' response efficacy (hypothesis 10) and threat appraisals (hypothesis 11) to explain variation in the adoption of cyber hygiene practices and in which key theoretical constructs derived from PMT partially mediate the direct effect of TRDM on cyber hygiene (hypothesis 9). Thus, thoughtfully reflective decision makers are more likely to engage in self-protective behaviors as: (1) a direct result of their increased cognitive functioning; (2) an indirect result of their ability to accurately assess the probability and severity (threat appraisal) of a cyber-attack; and (3) an indirect result of their faith in cyber hygiene's effectiveness at reducing victimization experiences.

Taken together, findings largely support the cross-disciplinary integration of TRDM and PMT, depicting the processual relationship linking quality decision making to victimization. Specifically, the adoption of cyber hygiene, in the current study, is the only significant predictor of victimization. Adopting cyber hygiene practices is a direct result of an Internet users' cognitive decision-making capabilities, and an indirect result of TRDM through the cognitive mediating processes depicted in PMT.

Theoretical Implications

The results presented in Chapter six, and discussed directly above, have myriad theoretical implications that span academic disciplines. For too long, theoretical developments have struggled to cross sub-field boundaries, causing scientific advancements to occur in a vacuum. The occurrence of a cybercrime incident, however, often includes human, technical, political, and economic components, making the study of cybercrime and cybersecurity related issues inherently interdisciplinary. Thus, attempts to develop theoretical insight into behavioral patterns observable in the cyber-environment should draw upon theoretical perspectives from a variety of academic disciplines. The current study draws from TRDM and PMT, which originated in the criminological and health sciences literature respectively, to explain the adoption of online self-protective behaviors, an endogenous variable of particular interest in the information security literature. Therefore, the findings presented above have direct bearing on the criminological, information security, and cyber-criminological literature.

The criminological literature, through the application of the rational choice framework within the cyber-environment, has demonstrated: (1) online offenders choose targets viewed as suitable and lacking capable guardianship (Maimon & Louderback, 2019); (2) target hardening can be used to reduce victimization experiences (Newman & Clarke, 2013); and (3) individuals' decision-making capabilities (TRDM) are associated with victimization experiences (Louderback & Antonaccio, 2017). Absent in the criminological literature, however, was a theoretical model designed to assess why some individuals choose not to engage in self-protective behaviors despite their known effectiveness at reducing victimization experiences (but see Burruss, Jaynes, Moule & Fairchild, in press, for a discussion of the link between rational choice and PMT). Additionally, measures of capable guardianship and suitability have been vague, inconsistent, and underdeveloped. With a lack of understanding surrounding the behaviors associated with self-protection, it creates uncertainty among Internet users pertaining to which target hardening behavior(s) to adopt to thwart victimization attempts. Lastly, documenting a correlation between decision making capabilities and victimization (Louderback & Antonaccio, 2017) without understanding the processual nature of such a relationship does little to inform theory.

Therefore, the current study promotes theoretical development in the field of criminology by (1) conceptualizing target hardening in cyberspace as the adoption of cyber hygiene practices; (2) operationalizing cyber hygiene through the development and assessment of a measurement model; (3) providing empirical support for the existence of a relationship between cyber hygiene and victimization; (4) parsing out the processual relationship linking decision making and victimization; and (5) expanding the scope of TRDM by illustrating the direct and indirect effects of TRDM on the adoption of online security behaviors.

The current study also promotes theoretical development in the information security literature. Information security scholars are increasingly adopting PMT as a preferred theoretical framework in explaining variation in information security behaviors (Sommestad et al., 2015). Rogers (1983), in his development of PMT, theorized that intraindividual differences likely shape the cognitive mediating processes leading to protection motivation, but was "vague" in his operationalization (Clubb & Hinkle, 2015). The current study, which serves as a logical extension of PMT, finds variation in threat and coping appraisals can be explained by persons' cognitive decision-making capabilities. Stated differently, TRDM shapes the cognitive mediating processes (i.e., threat and coping appraisals) depicted in PMT. Given that TRDM influences both PMT constructs and the adoption of security behaviors, the omission of such a construct when examining security behaviors creates omitted variable bias. Thus, information security scholars must incorporate decision making capabilities in current or future theories attempting to explain self-protection.

Policy Implications

In addition to aiding in theoretical development, the current study aids in the development of an evidence-based approach to cybersecurity. It was established that victimization stems from the lack of cyber hygiene, and that cyber hygiene is the byproduct of a cost-benefit analysis. Thus, if individuals can be nudged to engage in cyber hygiene practices, or if cyber-architectural modifications are made to automate cyber hygiene engagement, a reduction in the frequency of cybercrime incidents will follow suit. The former approach would require identifying those least likely to engage in cyber-hygiene and nudging them to adopt self-protective behaviors. Since TRDM has both a direct and indirect effect on cyber hygiene engagement, and since TRDM can be increased through educational training (Paternoster & Pogarsky, 2009), persons with low levels of TRDM could be provided targeted educational training which could increase engagement in cyber hygiene through increasing their decision-making capabilities. Another approach may involve nudging all Internet users, regardless of their cognitive decision-making capabilities, to make higher quality choices. For example, Internet users entering a public shop could be warned of the dangers associated with using private Wi-Fi networks; social media users could be presented with warnings pertaining to the dangers of sharing sensitive information; Email service providers could display banners encouraging users to approach unfamiliar emails with caution. These, and similar, warnings may elicit behavioral change by making cyber hygiene engagement, and the risks of non-engagement, focal to a decision maker's decision-making process.

Alternatively, the decision to engage in self-protective behaviors could be taken away from Internet users. By automating the process of target hardening, Internet users would receive protection by default. Internet providers, for example, could restrict Internet access on devices lacking anti-virus software. Strong passwords could be mandated to access an account or networked device. Social media sites could restrict the posting of personal information. Email service providers could develop better filtration systems to monitor for phishing attempts. This approach may increase security, but it would be at the cost of privacy. Security through cyber-environmental alterations would result in increased monitoring and restrictions. Thus, Internet users, and policy makers, must decide how many freedoms and how much privacy should be sacrificed to achieve security. Although such philosophical, or legal, debate is outside the scope of the current study, the section will conclude with a quote from Benjamin Franklin (1756): “Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.”

Limitations and Future Research

Although the current study provides theoretical insight into the correlates of engaging in self-protective behaviors, which have now proven to reduce victimization experiences, notable limitations exist. The most problematic of these limitations spawn from the reliance on a cross-sectional survey design. Cross-sectional designs do not allow for an accurate assessment of temporal ordering or reciprocal relationships. The inability to accurately test for reciprocal effects is of particular concern given that TRDM and PMT constructs may influence self-protective behaviors, but experiences with self-protective behaviors may in turn influence TRDM and PMT constructs. Moreover, and although cyber hygiene was found to reduce victimization experiences, it is possible that victimization also influences engagement in cyber hygiene practices. Testing such relationships can be more accurately accomplished using longitudinal survey designs.

Importantly, survey designs, both cross-section and longitudinal, are open to various forms of bias. Respondents may lie on the survey, not recall past experiences, or misinterpret questions. Additionally, since it was not possible to gather a random sample, in which all Internet users residing in the United States (the sampling frame) had an equal chance of inclusion, it is not clear whether the findings presented in the current study can be generalized to the population at large. Persons who use Mechanical Turk, or any online opt-in survey platform, differ from those who do not. Specifically, Mechanical Turk users must have access to the Internet, which not all who reside in the United States have. Given the current study examines online behavior, this is not particularly problematic. If individuals aren't online, they can't engage in cyber hygiene practices, meaning they are not the focus of the study. More problematically, the sample used in the current study significantly ($p<0.05$) differs from the United States population on various demographic characteristics. See Appendix C for comparisons. Therefore, it is also likely the sample differs from the general population in other, unobserved, ways which may influence the results discussed in the study in unknown ways. However, research has shown that findings derived from non-random online surveys do yield results that are similar in direction (Thompson & Pickett, 2020), though the magnitude of the effects may vary. Furthermore, it is possible those who accessed but did not complete the survey differ from those who accessed and completed the survey. Fortunately, the study did not suffer from high levels of attrition.

Lastly, and like most studies in the field of criminology (Mustard, 2003), the current study suffers from omitted variable bias. Most problematically, the measure *maladaptive rewards* was not included in the final structural model making the study an incomplete test of PMT. Since the bulk of examinations of PMT do not include the measure (Sommestad et al., 2015), it is unclear how omitting the theoretical construct biases the results. Differentiating response costs from maladaptive rewards both empirically and conceptually in cyberspace is central to the development of PMT. It is also possible other theoretical constructs, derived from any number of academic disciplines, could alter the decision-making process leading to self-protection. Control variables were added to the model in attempt to reduce bias, but with the inability to control for all observed and unobserved characteristics through the process of randomization (Campbell & Stanley, 2015), bias likely prevailed. Although this is certainly a limitation that future research should address, the current study established the existence of a processual relationship between TRDM, PMT, cyber hygiene, and victimization. It is now up to future studies to assess the possibility of alternative hypotheses.

In fact, the bulk of these limitations can, and should, be addressed in future studies. Firstly, two of the most notable limitations (i.e., generalizability and temporal ordering) can be remedied by gathering longitudinal data using a random sample. By randomly selecting participants from the population of interest (i.e., sampling frame), the findings can be generalized to the population at large. Additionally, employment of longitudinal data allows researchers to more accurately assess causal statements. The processual model introduced here would be best assessed by gathering four waves of data. TRDM at wave one would be used to predict PMT constructs at wave two and cyber hygiene at wave three, PMT constructs at wave two would be used to predict cyber hygiene engagement at wave three, cyber hygiene engagement at wave three would be used to predict victimization experiences at wave four. Moreover, victimization at wave two could be used to predict cyber hygiene at wave three to determine if a reciprocal relationship between cyber hygiene and victimization exists. Reciprocal relationships between TRDM, PMT constructs, and cyber hygiene could also be assessed in a similar manner. Since TRDM varies based on lived experiences (Paternoster & Pogarsky, 2009), such data could be used to determine whether TRDM is altered based on the accuracy of one’s appraisals and experiences with victimization and victimization avoidance. Ideally, a fear appeal would also be introduced to participants between wave one and wave two, which would allow for a more accurate assessment of the propositions set forth by Rogers (1983). The fear appeal would directly warn participants of the dangers associated with Internet connectivity. Of course, future studies should also include measures for maladaptive rewards.

Although longitudinal data allows for the assessment of temporal ordering, and researchers often make false claims of causality based on these data, it should be noted that only randomized control trials truly allow for the assessment of causality (Campbell & Clarke, 2015). Unfortunately, however, the processual model presented here cannot be tested using such a method since TRDM and the cognitive processes depicted in PMT (i.e., threat and coping appraisals) cannot be randomly assigned. That said, participants could be randomly assigned to a treatment or control group. Those in the treatment group could be given educational training to strengthen their cognitive decision-making capabilities, while those in the control group receive no such training. TRDM could be measured before and after successful completion of the training. This would allow researchers to determine if TRDM can be improved through educational training as suggested by Paternoster and Pogarsky (2009) and develop insight into whether such improvements alter the cognitive decision-making processes (as measured through PMT constructs) that lead to cyber hygiene and a reduction in victimization experiences.

Future research should also consider conducting various forms of invariance testing (see Cheung et al., 2002). Measurement invariance is the statistical property of measurement that indicates the same underlying construct is being measured across groups. It is unclear whether the measurement models and path analyses presented in the current study are invariant across groups (e.g., age, race, gender identity, etc.). It is unknown, for example if the same items measure the latent construct, cyber hygiene, for both men and women (i.e., configural invariance). Additionally, it is unclear whether the factor loadings (i.e., metric invariance), item intercepts (i.e., scalar invariance), and error terms (i.e., strict invariance) vary across groups. Understanding how the cognitive decision-making processes that promote self-protection varies based on demographic characteristics will allow for the development of a more general theory and more nuanced policy recommendations.

Lastly, the purpose of the current study was to assess the processual relationship between TRDM, PMT constructs, cyber hygiene, and victimization. Although partial support was garnered for the existence of such a relationship, self-control also demonstrated its relevance in predicting both PMT constructs and cyber hygiene engagement. In fact, low self-control was predictive of each of the PMT constructs included in the current study with the exception of *threat appraisal*, which was marginally not-significant (b=-7.111, p=0.065). Thus, future research should consider evaluating the predicative efficacy of Gottfredson and Hirschi's (1990) theory of self-control on information security behaviors. Specifically, the processual relationship between self-control, PMT constructs, cyber hygiene, and victimization should be assessed.

Conclusion

Although notable limitations exist, and although much work is yet to be done, the current study serves as an early attempt to bridge cross-disciplinary theoretical perspectives to garner insight into behavioral patterns in the cyber-environment. The study of cybercrime and cybersecurity does not belong to a singular academic discipline, but instead is inherently interdisciplinary with human, technical, political, and economic components. The current study employed theories derived from the criminological and health sciences literature to explain variation in information security behavior. Future research should continue in this tradition, drawing from other relevant disciplines where possible. Moreover, scholars must engage in translation research practices, working with law enforcement agencies and the cybersecurity industry to introduce an evidence-based approach to cybersecurity. Only together can academics, industry leaders, and government agencies create a safer cyber-environment.

Table 5. Summary of Findings.

	Victimization	
Hypothesis 1	Higher levels of engagement in cyber hygiene practices will decrease Internet users' experiences with victimization.	**Supported**
	PMT Constructs	
Hypothesis 2	Higher levels of TRDM will increase Internet users' coping appraisals.	**Partially Supported**
Hypothesis 3	Higher levels of TRDM will increase Internet users' threat appraisals.	**Supported**
	Fear	
Hypothesis 4	Higher threat appraisals will increase Internet users' fear of victimization.	**Supported**
	Cyber Hygiene	
Hypothesis 5	Higher fear appraisals will increase Internet users' adoption of cyber hygiene practices.	**Not Supported**
Hypothesis 6	Higher levels of TRDM will increase Internet users' adoption of cyber hygiene practices.	**Supported**
Hypothesis 7	Higher coping appraisals will increase Internet users' adoption of cyber hygiene practices.	**Partially Supported**
Hypothesis 8	Higher threat appraisals will increase Internet users' adoption of cyber hygiene practices.	**Supported**
Hypothesis 9	PMT constructs will partially mediate the effect of TRDM on Internet users' adoption of cyber hygiene practices.	**Supported**
Hypothesis 10	The indirect effect of TRDM through coping appraisals will increase Internet users' adoption of cyber hygiene practices.	**Partially Supported**
Hypothesis 11	The indirect effect of TRDM through threat appraisals will increase Internet users' adoption of cyber hygiene practices.	**Supported**

Note. TRDM=thoughtfully reflective decision making; PMT=protection motivation theory.

Chapter Eight:
References

Allen, R. S., Phillips, L. L., Pekmezi, D., Crowther, M. R., & Prentice-Dunn, S. (2008). Living well with living wills: Application of protection motivation theory to living wills among older Caucasian and African American adults. *Clinical Gerontologist*, *32*(1), 44-59.

Anandarajan, M., & Malik, S. (2018). Protecting the Internet of medical things: A situational crime-prevention approach. *Cogent Medicine*, *5*(1).

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643.

AOL/NCSA. (2004). AOL/NCSA online safety study. America Online and National Cyber Security Alliance. http://www.staysafeonline.info/news/ safety_study_v04.pdfO

Akers, R. L. (1973). *Deviant behavior: A social learning approach*. Belmont, Calif: Wadsworth Pub. Co.

Akers, R. L. (1989). A social behaviorist's perspective on integration of theories of crime and deviance. In Messner, S. F., Krohn, M. D., & Allen, L. E. (Eds.), *Theoretical integration in the study of deviance and crime: Problems and prospects* (pp. 23-36). SUNY Press.

Akers, R. L., Sellers, C. S., & Jennings, W. G. (2017). *Criminological Theories: Introduction, Evaluation, and Application (*7th ed.). Oxford University Press.

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, *29*(3), 706-714.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Ashford, W. (2009). Millions of web users at risk from weak passwords. *ComputerWeekly*. https://www.computerweekly.com/news/1280096996/Millions-of-web-users-at-risk-from-weak-passwords

Back, S., & LaPrade, J. (2020). Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions. *International Journal of Cybersecurity Intelligence & Cybercrime*, *3*(2), 25-47.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191-215.

Bandura, A. (1989). Human agency in social cognitive theory. *American Psychologist*, *44*(9), 1175-1184.

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology*, *52*(1), 1-26.

Baron, J. (2008). *Thinking and deciding* (4th ed.). Cambridge University Press.

Beccaria, C. (1764). *On crimes and punishments.* Bobbs-Merrill.

Becker, H. S. (1963). *Outsiders; studies in the sociology of deviance*. Free Press of Glencoe.

Becker, G. S. (1993). *Human capital: A theoretical and empirical analysis with special reference to education* (3rd ed.). University of Chicago Press.

Becker, G. S. (1968). Crime and punishment: An economic approach. In Fielding, N. G., Clarke, A., & Witt, R. (Eds.), *The economic dimensions of crime* (pp. 13-68). Palgrave Macmillan.

Becker, G. S. (1996). *Accounting for tastes.* Harvard University Press

Beebe, N. L., & Rao, V. S. (2005, December). Using situational crime prevention theory to explain the effectiveness of information systems security. *SoftWars Conference, Las Vegas, NV* (pp. 1-18).

Bentham, J. (1781). *An introduction to the principles of morals and legislation*. McMaster University Archive for the History of Economic Thought.

Bidgoli, M., & Grossklags, J. (2016, June). End user cybercrime reporting: what we know and what we can do to improve it. *International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, Canada* (pp. 1-6). IEEE.

Bollen, K. A. (1989). *Structural equations with latent variables*. John Wiley.

Boss, S., & Galletta, D. (2008). Scared straight: An empirical comparison of two major theoretical models explaining user backups. *International Research Symposium on Accounting Information Systems Conference, Paris, France* (pp. 1–17).

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837-864.

Bossler, A. M. (2017). Need for debate on the implications of honeypot data for restrictive deterrence policies in cyberspace. *Criminology & Public Policy, 16*(3), 681-688.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400-420.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly,* 523-548.

Bunch, J., Clay-Warner, J., & Lei, M. K. (2015). Demographic characteristics and victimization risk: Testing the mediating effects of routine activities. *Crime & Delinquency*, *61*(9), 1181-1205.

Burgess, R. L., & Akers, R. L. (1966). A differential association-reinforcement theory of criminal behavior. *Social Problems*, *14*(2), 128-147.

Burruss, G., Howell, C. J., Bossler, A., & Holt, T. J. (2019). Self-perceptions of English and Welsh constables and sergeants preparedness for online crime. *Policing: An International Journal*, *43*(1), 105-119.

Burruss, G.W., Jaynes, C.M., Moule R., Fairchild, R. (in Press). Modeling individual non-compliance with covid-19 pandemic mitigation behaviors insights from the expanded model of deterrence and protection motivation theories. *Criminal Justice & Behavior*.

Butler, M. J. (2014). Towards online security: Key drivers of poor user behaviour and recommendations for appropriate interventions. *South African Journal of Business Management*, *45*(4), 21-32.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36-45.

Campbell, D. T., & Stanley, J. C. (2015). *Experimental and quasi-experimental designs for research*. Ravenio Books.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, *12*(1), 28-38.

Center for Strategic and International Studies (CSIS). (2018). Space Threat Assessment 2018. https://www.csis.org/analysis/space-threat-assessment-2018

Chan, M., & Woon, I. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security, 1*(3), 18-41.

Cheung, G. W., & Rensvold, R. B. (2002). Evaluating goodness-of-fit indexes for testing measurement invariance. *Structural Equation Modeling*, *9*(2), 233-255.

Chiricos, T. G., & Waldo, G. P. (1970). Punishment and crime: An examination of some empirical evidence. *Social Problems*, *18*(2), 200-217.

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308-333.

Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394-402.

Chou, H. L., & Sun, J. C. Y. (2017). The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers. *Computers & Education*, *112*, 83-96.

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics*, *35*(6), 1770-1780.

Clarke, R. V. (1980). Situational crime prevention: Theory and practice. *British Journal of Criminology*, *20*(2), 136-147.

Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. *Crime and Justice*, *4*, 225-256.

Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice*, *19*, 91-150.

Clarke, R. V. (2004). Technology, criminology and crime science. *European Journal on Criminal Policy and Research*, *10*(1), 55-63.

Clarke, R. V., Cody, R. P., & Natarajan, M. (1994). Subway slugs: tracking displacement on the London Underground. *The British Journal of Criminology*, *34*(2), 122-138.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice*, *6*, 147-185.

Clarke, R. V., Field, S., & McGrath, G. (1991). Target hardening of banks in Australia and displacement of robberies. *Security Journal*, *2*(2), 84-90.

Clarke, R. V. G., & Newman, G. R. (2006). *Outsmarting the terrorists*. Greenwood Publishing Group.

Clubb, A. C., & Hinkle, J. C. (2015). Protection motivation theory as a theoretical framework for understanding the use of protective measures. *Criminal Justice Studies*, *28*(3), 336-355.

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

Collins, J. D., Sainato, V. A., & Khey, D. N. (2011). Organizational data breaches 2005-2010: Applying SCP to the healthcare and education sectors. *International Journal of Cyber Criminology*, *5*(1), 794-810.

Corcoran, J., Zahnow, R., & Higgs, G. (2016). Using routine activity theory to inform a conceptual understanding of the geography of fire events. *Geoforum*, *75*, 180-185.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies*, *16*, 41-96.

Cornish, D. B., & Clarke, R. V. (2014). *The reasoning criminal: Rational choice perspectives on offending*. Transaction Publishers.

Coupe, T., & Blake, L. (2006). Daylight and darkness targeting strategies and the risks of being seen at residential burglaries. *Criminology*, *44*(2), 431-464.

D'Arcy, J., & Hovav, A. (2008). Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. *Journal of Business Ethics, 89*, 59–71.

Dawson, L. A., & Stinebaugh, J. (2010). *Methodology for prioritizing cyber-vulnerable critical infrastructure equipment and mitigation strategies* (No. SAND2010-1845). Sandia National Laboratories.

Decker, J. F. (1972). Curbside Deterrence? An analysis of the effect of a slug-rejector device, coin-view window, and warning labels on slug usage in New York City parking meters. *Criminology*, *10*(2), 127-142.

Denning, D. E., & Baugh Jr, W. E. (1999). Hiding crimes in cyberspace. *Information, Communication & Society*, *2*(3), 251-276.

Department of Homeland Security. (2020). Homeland Threat Assessment. https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal, 19,* 391–412.

Dodge, R., Toregas, C., & Hoffman, L. J. (2012). Cybersecurity workforce development directions. *HAISA*, 1-12.

Ehrlich, I. (1974). *Participation in illegitimate activities: An economic analysis* (No. c3627). National Bureau of Economic Research.

Ekblom, P. (1988). Preventing post office robberies in London: Effects and side effects. *Journal of Security Administration*, *11*(1), 36-43.

Elliott, D. S., Ageton, S. S., & Canter, R. J. (1979). An integrated theoretical perspective on delinquent behavior. *Journal of Research in Crime and Delinquency*, *16*(1), 3-27.

Elliott, D. S., Huizinga, D., & Ageton, S. S. (1985). *Explaining delinquency and drug use*. Sage Publications.

Fedler, R., Schütte, J., & Kulicke, M. (2013). On the effectiveness of malware protection on android. *Fraunhofer AISEC*, 1-35.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407-429.

Frank, R. H. (2000*). Microeconomics and behavior.* McGraw-Hill

Franklin, B. (1755). Those who would give up Essential Liberty to purchase a little Temporary Safety, deserve neither Liberty nor Safety. *Speech to the Pennsylvania Assembly.*

Frederick, S., Loewenstein, G., & O'Donoghue, T. (2002). Time discounting and time preference: A critical review. *Journal of Economic Literature, 40*, 351-401.

Furnell, S. (2005). Why users cannot use security. *Computers & Security*, *24*(4), 274-279.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence.* Elsevier.

Gigerenzer, G., & Selten, R. (2002). *Bounded rationality: The adaptive toolbox*. MIT press.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), 256-267.

Gul, S. (2009). An evaluation of the rational choice theory in criminology. *Girne American University Journal of Social and Applied Science*, *4*(8), 36-44.

Gunzler, D., Chen, T., Wu, P., & Zhang, H. (2013). Introduction to mediation analysis with structural equation modeling. *Shanghai Archives of Psychiatry*, *25*(6), 390.

Guo, X., Han, X., Zhang, X., Dang, Y., & Chen, C. (2015). Investigating m-health acceptance from a protection motivation theory perspective: gender and age differences. *Telemedicine and E-Health*, *21*(8), 661-669.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203–236.

Halevi, T., Lewis, J., & Memon, N. (2013, May). A pilot study of cyber security and privacy related behavior and personality traits. *International Conference on World Wide Web, Rio de Janeiro, Brazil* (pp. 737-744).

Harknett, R. J., Callaghan, J. P., & Kauffman, R. (2010). Leaving deterrence behind: War-fighting and national cybersecurity. *Journal of Homeland Security and Emergency Management*, *7*(1), 1-24.

Henry, P. S., & Luo, H. (2002). WiFi: What's next?. *IEEE Communications Magazine*, *40*(12), 66-72.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2012). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24,* 61-84.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125.

Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal*, *26*(4), 383-402.

Hirschi, T. (1969). Causes of delinquency. University of California Press.

Hirschi, T. (1979). Separate and unequal is better. *Journal of Research in Crime and Delinquency*, *16*(1), 34-38.

Hirschi, T. (1989). Exploring alternatives to integrated theory. In Messner, S. F., Krohn, M. D., & Allen, L. E. (Eds.), *Theoretical integration in the study of deviance and crime: Problems and prospects* (pp. 37-49). SUNY Press.

Hoonakker, P., Bornoe, N., & Carayon, P. (2009, October). Password authentication from a human factors perspective: Results of a survey among end-users. *Human Factors and Ergonomics Society Annual Meeting, Los Angeles, CA*, (pp. 459-463). SAGE Publications.

Hooper, D., Coughlan, J., & Mullen, M. (2008, June). Evaluating model fit: a synthesis of the structural equation modelling literature. *7th European Conference on Research Methodology for Business and Management Studies, Aveiro, Portugal,* (pp. 195-200).

Holt, T. J. (2011). *Crime on-line: correlates, causes, and context.* Carolina Academic Press.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1-25.

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420-436.

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2018). Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology*, *62*(6), 1720-1741.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, *46*(1), 189-220.

Howell, C. J., Burruss, G. W., Maimon, D., & Sahani, S. (2019). Website defacement and routine activities: Considering the importance of hackers' valuations of potential targets. *Journal of Crime and Justice*, *42*(5), 536-550.

Howell, C. J., Maimon, D., Berenbulm, T., Carmel, T., & Steinfeld, N. (2021). *Pocket Security.* Evidence-Based Cybersecurity Research Group. ebcs.gsu.edu

Howell, C. J., Maimon, D., Cochran, J. K., Jones, H. M., & Powers, R. A. (2017). System trespasser behavior after exposure to warning messages at a Chinese computer network: An examination. *International Journal of Cyber Criminology, 11*(1), 63–77.

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Dournal*, *6*(1), 1-55.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615–660.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Internet Crime Complaint Center. (2019). *2018 Internet Crime Report*. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2018-internet-crime-report#:~:text=The%20FBI's%20Internet%20Crime%20Complaint,extortion%2C%20and%20personal%20data%20breach.

Ireland, L. (2020). Predicting online target hardening behaviors: An extension of routine activity theory for privacy-enhancing technologies and techniques. *Deviant Behavior*, 1-17.

Jeffery, C. R. (1971). *Crime prevention through environmental design*. Sage Publications.

Jessor, R., & Jessor, S. L. (1973). The perceived environment in behavioral science: Some conceptual issues and some illustrative data. *American Behavioral Scientist*, *16*(6), 801-828.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549 -66.

Johnston, A. C., Wech, B., Jack, E., & Beavers, M. (2010). Reigning in the remote employee: Applying social learning theory to explain information security policy compliance attitudes. *Americas Conference on Information Systems, Lima, Peru,* (pp. 2217–2230).

Kahneman D (2003) Maps for bounded rationality: psychology for behavioral economics. *American Economic Review, 93*(5), 1449–1475.

Karaymeh, A., Ababneh, M., Qasaimeh, M., & Al-Fayoumi, M. (2019, October). Enhancing data protection provided by VPN connections over ppen WiFi networks. *International Conference on new Trends in Computing Sciences, Amman, Jordan,* (pp. 1-6). IEEE.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review, 30*(4), 470-486.

Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems, 46*, 254-264.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour and Information Technology, 27*(5), 445-454.

Levesque, F. L., Nsiempba, J., Fernandez, J. M., Chiasson, S., & Somayaji, A. (2013, November). A clinical study of risk factors related to malware infections. *ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany,* (pp. 97-108).

Levesque, F. L., Fernandez, J. M., Batchelder, D., & Young, G. (2016). Are they real? Real-life comparative tests of ´ antivirus products. *Virus Bulletin Conference, Abingdon, UK,* (pp. 1–11). Virus Bull.

Levitt, S. D., & Lochner, L. (2001). The determinants of juvenile crime. In Gruber, J. (Eds.), *Risky behavior among youths: An economic analysis* (pp. 327-374). University of Chicago Press.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association of Information Systems, 11*(7), 394–413.

Liao, Q., Luo, X., Gurung, A., & Li, L. (2009). Workplace management and employee misuse: does punishment matter? *Journal of Computer Information Systems, 50*, 49-60.

Liska, A. E., Krohn, M. D., & Messner, S. F. (1989). Strategies and requisites for theoretical integration in the study of crime and deviance. In Messner, S. F., Krohn, M. D., & Allen, L. E. (Eds.), *Theoretical integration in the study of deviance and crime: Problems and prospects* (pp. 1-19). SUNY Press.

Lombroso-Ferrero, G., & Lombroso, C. (1911). *Criminal man, according to the classification of Cesare Lombroso*. Putnam.

Louderback, E. R., & Antonaccio, O. (2017). Exploring cognitive decision-making processes, computer-focused cyber deviance involvement and victimization: The role of thoughtfully reflective decision-making. *Journal of Research in Crime and Delinquency*, *54*(5), 639-679.

Loughran, T. A., Paternoster, R., Chalfin, A., & Wilson, T. (2016). Can rational choice be considered a general theory of crime? Evidence from individual-level panel data. *Criminology*, *54*(1), 86-112.

Loughran, T. A., Paternoster, R., Piquero, A. R., & Pogarsky, G. (2011). On ambiguity in perceptions of risk: Implications for criminal decision making and deterrence. *Criminology*, *49*(4), 1029-1061.

Loukas, G., & Patrikakis, C. (2016). Cyber and physical threats to the Internet of Everything. *Cutter IT Journal*, *29*(7), 5-11.

Lupia, A. McCubbins, M. D. (1998). *The democratic dilemma: Can citizens learn what they need to know?* Cambridge University Press.

Maennel, K., Mäses, S., & Maennel, O. (2018, November). Cyber hygiene: The big picture. *Nordic Conference on Secure IT Systems, Oslo, Norway,* (pp. 291-305). Springer, Cham.

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33-59.

Maimon, D., Antonaccio, O., & French, M. T. (2012). Severe sanctions, easy choice? Investigating the role of school sanctions in preventing adolescent violent offending. *Criminology*, *50*(2), 495-524.

Maimon, D., Becker, M., Patil, S., & Katz, J. (2017). Self-protective behaviors over public WiFi networks. *The {LASER} Workshop: Learning from Authoritative Security Experiment Results, Arlington, VA,* (pp. 69-76).

Maimon, D., Howell, C. J., Jacques, S., Perkins, R. C. (2020) Situational awareness and public Wi-Fi users' self-protective behaviors. *Security Journal, 1-21.*

Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network: An application of the routine-activities and lifestyle perspective. *British Journal of Criminology*, *53*(2), 319-343.

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: an interdisciplinary review. *Annual Review of Criminology*, 191-216.

Mansfield-Devine, S. (2017). Meeting the needs of GDPR with encryption. *Computer Fraud & Security*, 9, 16-20.

Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2010). Policing possession of child pornography online: Investigating the training and resources dedicated to the investigation of cyber crime. *International Journal of Police Science & Management*, *12*(4), 516-525.

Martini, B., & Choo, K. K. R. (2014, June). Building the next generation of cyber security professionals. *European Conference on Information Systems (ECIS), Tel Aviv, Israel*, (pp.1-13).

Maybury, M. T. (2015). Toward principles of cyberspace security. *Cybersecurity policies and strategies for cyberwarfare prevention* (pp. 1-12). IGI Global.

McAfee. (2017). The economic impact of cybercrime— no slowing down. https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf.

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology*, *28*(1), 417-442.

McNeeley, S., & Wilcox, P. (2015). Street codes, routine activities, neighbourhood context and victimization. *British Journal of Criminology*, *55*(5), 921-943.

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review*, *3*(5), 672-682.

Messner, S. F., & Tardiff, K. (1985). The social ecology of urban homicide: An application of the “routine activities” approach. *Criminology*, *23*(2), 241-267.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106-143.

Mitchell, W. J. (1996). *City of bits: space, place, and the infobahn*. MIT press.

Moffitt, T. E. (1990). The neuropsychology of juvenile delinquency: A critical review. *Crime and Justice*, *12*, 99-169.

Muftić, L. R. (2009). Macro-micro theoretical integration: An unexplored theoretical frontier. *Journal of Theoretical & Philosophical Criminology*, *1*(2), 33-37.

Mustard, D. B. (2003). Reexamining criminal behavior: the importance of omitted variable bias. *Review of Economics and Statistics*, *85*(1), 205-211.

Mustaine, E. E., & Tewksbury, R. (1998). Predicting risks of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology*, *36*(4), 829-858.

Mustaine, E. E., & Tewksbury, R. (2002). Sexual assault of college women: A feminist interpretation of a routine activities analysis. *Criminal Justice Review*, *27*(1), 89-123.

Nagin, D. S. (2007). Moving choice to center stage in criminological research and theory: The American Society of Criminology 2006 Sutherland Address. *Criminology: An Interdisciplinary Journal, 45* (2), 259–272.

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*, *92*, 101731.

Newman, O. (1972). *Defensible space*. Macmillan.

Newman, G. R., & Clarke, R. V. (2013). *Superhighway robbery*. Routledge.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773-793.

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. *Predicting health Behaviour*, *81*, 126.

Nunnally, J. C. (1978). *Psychometric theory*. McGraw-Hill

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40-51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, *42*, 165-176.

Paternoster, R., & Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology*, *25*(2), 103-127.

Paternoster, R., Pogarsky, G., & Zimmerman, G. (2011). Thoughtfully reflective decision making and the accumulation of capital: Bringing choice back in. *Journal of Quantitative Criminology*, *27*(1), 1-26.

Paternoster, R., Saltzman, L. E., Waldo, G. P., & Chiricos, T. G. (1983). Perceived risk and social control: Do sanctions really deter?. *Law and Society Review*, *17*(3), 457-479.

Perkins, R. C., Howell, C. J., Dodge, C. E., Burruss, G. W., & Maimon, D. (2020). Malicious spam distribution: A routine activities approach. *Deviant Behavior*, 1-17.

Ponemon Institute. (2016). Cost of cyber crime study & the risk of business in- novation. Ponemon Institute. http://www.ponemon.org/ library/2016-cost-of-cyber-crime-study-the-risk-of-business-innovation

Posey, C., Roberts, T., Lowry, P. B., Courtney, J., & Bennett, R. J. (2011). Motivating the insider to protect organizational information assets: Evidence from protection motivation theory and rival explanations. *Dewald Roode Workshop in Information Systems Security* Blacksburg, Virginia, (pp. 1–51).

Poyner, B. (1993). What works in crime prevention: An overview of evaluations. *Crime Prevention Studies*, *1*, 7-34.

Pratt, T. C., & Cullen, F. T. (2005). Assessing macro-level predictors and theories of crime: A meta-analysis. *Crime and Justice*, *32*, 373-450.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

Privacy rights Clearinghouse (PRCH). (2017). Privacy rights clearinghouse. https://privacyrights.org

Rebellon, C. J., Straus, M. A., & Medeiros, R. (2008). Self-control in global perspective: An empirical assessment of Gottfredson and Hirschi's general theory within and across 32 national settings. *European Journal of Criminology*, *5*(3), 331-361.

Rege, A. (2014). A criminological perspective on power grid cyber attacks: Using routine activities theory to rational choice perspective to explore adversarial decision-making. *Journal of Homeland Security and Emergency Management*, *11*(4), 463-487.

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety*, *12*(2), 99-118.

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization?. *American Journal of Criminal Justice*, *44*(1), 63-82.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149-1169.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security, 28*(8), 816–826.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology: A Sourcebook*, 153-176.

Sasse, M. A., & Flechais, I. (2005). *Usable security: Why do we need it? How do we get it?*. O'Reilly.

Schmidt, P., & Witte, A. D. (1984). *An economic analysis of crime and justice: Theory, methods, and applications.* MIT Press.

Shaw, C. R., & McKay, H. D. (1942). *Juvenile delinquency and urban areas*. University of Chicago Press.

Short Jr, J. F. (1979). On the etiology of delinquent behavior. *Journal of Research in Crime and Delinquency*, *16*(1), 28-33.

Siponen, M. T., Pahnila, S., & Mahmood, A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer, 43*(2), 64–71.

Smith, W. R., Frazee, S. G., & Davison, E. L. (2000). Furthering the integration of routine activity and social disorganization theories: Small units of analysis and the study of street robbery as a diffusion process. *Criminology*, *38*(2), 489-524.

Sommestad, T., & Hallberg, J. (2013, July). A review of the theory of planned behaviour in the context of information security policy compliance. *IFIP International Information Security Conference, Heidelberg, Berlin,* (pp. 257-271). Springer.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy*, *9*(1), 26-46.

Song, H., Lynch, M. J., & Cochran, J. K. (2016). A macro-social exploratory analysis of the rate of interstate cyber-victimization. *American Journal of Criminal Justice*, *41*(3), 583-601.

Spano, R., & Nagy, S. (2005). Social guardianship and social isolation: An application and extension of lifestyle/routine activities theory to rural adolescents. *Rural Sociology*, *70*(3), 414-437.

Stewart, E. A., Elifson, K. W., & Sterk, C. E. (2004). Integrating the general theory of crime into an explanation of violent victimization among female offenders. *Justice Quarterly*, *21*(1), 159-181.

Straus, M. A., Hamby, S. L., Boney-McCoy, S., & Sugarman, D. (1999). Manual for the personal and relationships profile (PRP). *University of New Hampshire, Family Research Laboratory. Available in: http://pubpages. unh.edu/~ mas2*.

Sutherland, E. H. (1947). *Principles of criminology*. J. B. Lippincott.

Talib, S., Clarke, N. L., & Furnell, S. M. (2010, February). An analysis of information security awareness within home and work environments. *International Conference on Availability, Reliability and Security, Krakow, Poland,* (pp. 196-203). IEEE.

Testa, A., Maimon, D., Sobesto, B., & Cukier, M. (2017). Illegal roaming and file manipulation on target computers: Assessing the effect of sanction threats on system trespassers' online behaviors. *Criminology & Public Policy*, *16*(3), 689-726.

Tewksbury, R., Mustaine, E. E., & Stengel, K. M. (2008). Examining rates of sexual offenses from a routine activities perspective. *Victims and Offenders*, *3*(1), 75-85.

Tewksbury, R., & Mustaine, E. E. (2000). Routine activities and vandalism: A theoretical and empirical study. *Journal of Crime and Justice*, *23*(1), 81-110.

Thaler, R. H., Sunstein, C. R. (2008. *Nudge: improving decisions and health, wealth, and happiness.* Yale University Press.

Thompson, A. J., & Pickett, J. T. (2020). Are relational inferences from crowdsourced and opt-in samples generalizable? Comparing criminal justice attitudes in the GSS and five online samples. *Journal of Quantitative Criminology*, *36*, 907-932.

Thornberry, T. P. (1989). Reflections on the advantages and disadvantages of theoretical integration. In Messner, S. F., Krohn, M. D., & Allen, L. E. (Eds.), *Theoretical integration in the study of deviance and crime: Problems and prospects* (pp. 51-60). SUNY Press.

Tittle, C. (1985). The assumption that general theories are not possible. In Meir R. F. (Eds.), *Theoretical methods in criminology* (pp.93-121). Sage Publications.

Timmer, A., Antonaccio, O., & French, M. T. (2020). Hot or cool processing? Adolescent decision-daking and Delinquency. *Justice Quarterly*, 1-34.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers & Security*, *79*, 68-79.

Tseloni, A., & Zarafonitou, C. (2008). Fear of crime and victimization: A multivariate multilevel analysis of competing measurements. *European Journal of Criminology*, *5*(4), 387-409.

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2), 115-127.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

Vidal, C., & Choo, K. K. R. (2017, October). Situational Crime Prevention and the Mitigation of Cloud Computing Threats. *International Conference on Security and Privacy in Communication Systems*, Niagara Falls, Canada, (pp. 218-233). Springer.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160.

Wagner, D. G., & Berger, J. (1985). Do sociological theories grow?. *American Journal of Sociology*, *90*(4), 697-728.

Webb, B. (1994). Steering column locks and motor vehicle theft: Evaluations from three countries. *Crime Prevention Studies*, *2*, 71-89.

Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010, October). Testing metrics for password creation policies by attacking large sets of revealed passwords. *Proceedings of the 17th ACM Conference on Computer and Communications Security*, Chicago, IL, (pp. 162-175).

Weisburd, D., & Piquero, A. R. (2008). How well do criminologists explain crime? Statistical modeling in published studies. *Crime and Justice*, *37*(1), 453-502.

Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly*, *26*(4), 716-745.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3-7.

Willison, R., & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM*, *52*(9), 133-137.

Wilsem, J. V. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437-453.

Wilson, T., Maimon, D., Sobesto, B., & Cukier, M. (2015). The effect of a surveillance banner in an attacked computer system: Additional evidence for the relevance of restrictive deterrence in cyberspace. *Journal of Research in Crime and Delinquency*, *52*(6), 829-855.

Wright, R. T., & Decker, S. H. (1996). *Burglars on the job: Streetlife and residential break-ins*. UPNE.

Xue, Y., Liang, H., & Wu, L. (2010). Punishment, Justice, and Compliance in Mandatory IT Settings. *Information Systems Research, 22*(2), 400–414.

Yar, M. (2005). The novelty of 'cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407-427.

Yucedal, B. (2010). *Victimization in cyberspace: An application of Routine Activity and Lifestyle Exposure theories* (Doctoral dissertation, Kent State University).

Zhang, L., Messner, S. F., & Liu, J. (2007). A multilevel analysis of the risk of household burglary in the city of Tianjin, China. *The British Journal of Criminology*, *47*(6), 918-937.

Zhang, L., Pavur, R. J., York, P., & Amos, C. (2013). Testing a model of users' web risk information seeking intention. *Informing Science: The International Journal of an Emerging Transdiscipline, 16*, 1-18.

Zhang, J., Reithel, B., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management and Computer Security, 17*(4), 330–34.

Appendices

Appendix A: Correlation Matrix

Table A1. Correlation Matrix (n=311).

Variables	Victim 1	Victim 2	Victim 3	Cyber Hygiene 1	Cyber Hygiene 2	Cyber Hygiene 3	Cyber Hygiene 4	Cyber Hygiene 5
Victim 1	1.000							
Victim 2	0.158	1.000						
Victim 3	0.232	0.243	1.000					
Cyber Hygiene 1	-0.112	0.009	0.023	1.000				
Cyber Hygiene 2	-0.088	-0.087	-0.055	0.097	1.000			
Cyber Hygiene 3	-0.104	-0.007	-0.060	0.047	0.518	1.000		
Cyber Hygiene 4	-0.212	-0.026	-0.048	0.155	0.316	0.347	1.000	
Cyber Hygiene 5	-0.138	-0.020	-0.040	0.130	0.277	0.247	0.265	1.000
Cyber Hygiene 6	-0.126	-0.022	-0.108	0.398	0.299	0.243	0.230	0.257
Cyber Hygiene 7	-0.149	-0.084	-0.083	0.269	0.250	0.320	0.438	0.256
TRDM	0.024	0.040	-0.033	0.231	0.057	0.140	0.143	0.028
Threat Appraisal	-0.028	0.070	0.089	0.259	0.118	0.245	0.251	0.031
Response Efficacy	0.032	-0.077	-0.092	0.260	0.093	0.160	0.158	0.056
Self-Efficacy	-0.034	-0.049	-0.125	0.228	0.023	0.074	0.077	0.068
Response Cost	0.121	0.105	0.068	-0.253	-0.031	-0.011	-0.060	-0.082
Fear 1	-0.009	0.129	0.164	0.116	0.026	0.016	0.125	-0.073
Fear 2	0.039	0.142	0.150	0.062	0.031	-0.027	0.043	-0.098
Fear 3	0.006	0.111	0.106	0.049	0.027	-0.056	0.077	-0.075
Fear 4	0.052	0.118	0.067	-0.002	0.000	-0.013	0.039	-0.106
Fear 5	0.086	0.206	0.128	0.029	-0.061	-0.089	0.001	-0.235
Low Self-Control 1	-0.005	0.005	0.014	-0.099	-0.129	-0.069	-0.048	-0.087
Low Self-Control 2	0.025	-0.069	0.036	-0.055	-0.192	-0.234	-0.217	-0.119
Low Self-Control 3	0.010	0.034	0.120	-0.157	-0.086	-0.121	-0.131	-0.117
Low Self-Control 4	0.097	0.073	0.098	-0.138	-0.192	-0.169	-0.210	-0.182
Low Self-Control 5	0.120	0.048	0.024	-0.076	-0.186	-0.282	-0.226	-0.153
Low Self-Control 6	-0.037	-0.075	0.056	-0.132	0.046	-0.076	-0.104	-0.087
Computer Skill	0.002	-0.031	0.030	0.316	0.044	-0.001	-0.049	-0.033
Education	-0.003	-0.008	0.027	0.001	-0.027	-0.020	0.052	0.042
White	-0.094	-0.015	-0.073	-0.117	0.099	0.010	0.063	0.109
Age	-0.027	-0.052	0.014	-0.045	0.165	0.201	0.124	0.135
Male	0.047	-0.070	-0.065	-0.026	-0.003	-0.080	-0.166	0.054

Table A1. (continued).

Variables	Cyber Hygiene 6	Cyber Hygiene 7	TRDM	Threat Appraisal	Response Efficacy	Self-Efficacy	Response Cost	Fear 1	Fear 2	Fear 3
Cyber Hygiene 6	1.000									
Cyber Hygiene 7	0.327	1.000								
TRDM	0.047	0.174	1.000							
Threat Appraisal	0.199	0.191	0.147	1.000						
Response Efficacy	0.200	0.193	0.199	0.309	1.000					
Self-Efficacy	0.153	0.124	0.073	0.150	0.644	1.000				
Response Cost	-0.163	-0.123	-0.108	0.101	-0.287	-0.281	1.000			
Fear 1	0.068	0.040	0.088	0.350	-0.014	-0.076	0.167	1.000		
Fear 2	0.024	-0.015	0.070	0.229	0.021	-0.009	0.159	0.551	1.000	
Fear 3	0.068	-0.036	0.084	0.241	0.005	-0.057	0.133	0.549	0.754	1.000
Fear 4	-0.015	-0.049	0.114	0.248	0.010	-0.067	0.237	0.565	0.631	0.634
Fear 5	-0.005	-0.095	0.084	0.187	-0.030	-0.097	0.097	0.481	0.569	0.659
Low Self-Control 1	-0.098	-0.081	-0.161	-0.085	-0.138	-0.027	0.071	0.085	0.129	0.053
Low Self-Control 2	-0.113	-0.198	-0.083	-0.140	-0.092	-0.095	0.031	-0.025	0.055	0.051
Low Self-Control 3	-0.100	-0.193	-0.115	-0.059	-0.085	-0.130	0.153	0.152	0.091	0.096
Low Self-Control 4	-0.135	-0.234	-0.139	-0.046	-0.142	-0.050	0.140	0.072	0.140	0.102
Low Self-Control 5	-0.145	-0.236	-0.185	-0.104	-0.085	-0.021	0.055	0.078	0.135	0.072
Low Self-Control 6	-0.016	-0.148	-0.230	-0.077	-0.138	-0.150	0.121	0.091	0.134	0.158
Computer Skill	0.161	0.160	0.208	0.011	0.218	0.272	-0.287	0.012	-0.118	-0.105
Education	-0.091	-0.053	0.182	0.005	0.038	0.020	0.133	-0.026	0.039	0.047
White	-0.032	-0.015	-0.105	-0.096	-0.058	-0.006	0.072	-0.074	-0.066	-0.068
Age	0.148	0.092	-0.027	0.167	0.016	0.052	-0.018	0.121	0.086	0.086
Male	-0.019	-0.088	-0.055	-0.162	-0.005	0.037	-0.055	-0.156	-0.119	-0.098

Table A1. (continued).

Variables	Fear 4	Fear 5	Low Self- Control 1	Low Self- Control 2	Low Self- Control 3	Low Self- Control 4	Low Self- Control 5	Low Self- Control 6
Fear 4	1.000							
Fear 5	0.567	1.000						
Low Self-Control 1	0.042	0.125	1.000					
Low Self-Control 2	-0.002	0.058	0.321	1.000				
Low Self-Control 3	0.087	0.104	0.253	0.355	1.000			
Low Self-Control 4	0.093	0.139	0.359	0.442	0.475	1.000		
Low Self-Control 5	0.082	0.143	0.421	0.526	0.325	0.541	1.000	
Low Self-Control 6	0.131	0.165	0.322	0.188	0.247	0.289	0.362	1.000
Computer Skill	-0.183	0.021	0.038	0.069	-0.022	-0.009	0.077	-0.134
Education	0.087	0.021	0.050	0.057	-0.047	-0.003	-0.071	-0.119
White	-0.049	-0.123	-0.048	-0.011	0.079	0.022	-0.037	0.055
Age	0.109	0.060	0.015	-0.044	-0.028	-0.068	-0.077	0.035
Male	-0.138	-0.144	0.099	0.175	-0.011	0.068	0.258	-0.028

Table A1. (continued).

Variables	Computer Skill	Education	White	Age	Male
Computer Skill	1.000				
Education	0.073	1.000			
White	-0.101	-0.167	1.000		
Age	-0.160	-0.049	0.219	1.000	
Male	0.208	0.064	-0.057	-0.178	1.000

Note. TRDM= thoughtfully reflective decision making.

Appendix B: Survey Items

Table A2. List of Survey Items.

	Victimization
Victim 1	My computer was infected with a virus.
Victim 2	I received messages from someone that threatened, insulted, or harassed me.
Victim 3	I was notified 1 or more of my online account(s) had been hacked and personal data was at risk.
	Cyber Hygiene
Cyber Hygiene 1	I used complex passwords (including random letters, numbers, and symbols).
Cyber Hygiene 2	I shared geographic information on social media.
Cyber Hygiene 3	I shared account information on social media.
Cyber Hygiene 4	I downloaded something from a non-secure source.
Cyber Hygiene 5	I shared my password with someone.
Cyber Hygiene 6	I used the same password for multiple accounts.
Cyber Hygiene 7	I clicked or opened unfamiliar links.
	TRDM
TRDM 1	When you have a problem to solve, one of the first things you do is get as many facts about the problem as possible.
TRDM 2	When you are attempting to find a solution to a problem, you usually try to think of as many different approaches to the problem as possible.
TRDM 3	When making decisions, you generally use a systematic method for judging and comparing alternatives.
TRDM 4	After carrying out a solution to a problem, you usually try to analyze what went right and what went wrong.
	PMT Constructs
Severity	Online victimization is a serious threat.
Vulnerability	Online victimization is a probable threat.
Response Efficacy	Adopting recommended security behaviors will prevent online victimization.
Self-Efficacy	I can prevent online victimization.
Response Cost	Protecting myself online is difficult.
	Fear
Fear 1	A major data breach where my customer information is stolen.
Fear 2	I open a phishing e-mail message that runs malicious code.
Fear 3	My computer's data become locked in a ransomware scheme.
Fear 4	My computer will become infected with a virus.
Fear 5	I receive a Distributed Denial of Service attack.
	Low Self-Control
Low Self-Control 1	I don't think about how what I do will affect other people.
Low Self-Control 2	I often do things that other people think are dangerous.
Low Self-Control 3	There is nothing I can do to control my feelings when someone hassles me.
Low Self-Control 4	I often get hurt by things that I do.
Low Self-Control 5	I have trouble following the rules at work or in school.
Low Self-Control 6	I have goals in life that I try to reach.
	Computer Skill
Computer Skill 1	Dealing with software problems.
Computer Skill 2	Removing malware from your computing devices (e.g., computer viruses).
Computer Skill 3	Dealing with computer hardware problems.
Computer Skill 4	Modifying the firewall on your computing devices.
Computer Skill 5	Establishing a virtual proxy network on your computing devices.
Computer Skill 6	Storing digital information on a cloud-based platform (e.g., Dropbox, OneDrive, Box, iCloud).
	Demographic Characteristics
Education	What is the highest level of formal education that you have completed?
White	How would you identify yourself with regard to race?
Age	What is your age?
Male	How do you identify yourself with regard to sex?

Note. TRDM=thoughtfully reflective decision making; PMT=protection motivation theory.

Appendix C: Sample Comparisons

Table A3. Z Tests Comparing Sample to United States Population.

	Population	Current Sample		
Variables	(percentage)	(percentage)	z-value	p-value
Education				
High school diploma or GED	27.00	12.86	5.6*	0.000
Some college or Associate degree	26.50	33.76	2.9*	0.004
Bachelor’s degree	20.20	42.44	9.8*	0.000
Advanced degree	11.40	10.93	0.3	0.794
Race				
White	76.30	82.96	2.8*	0.006
Black	13.40	5.81	3.9*	0.000
Asian	5.90	7.95	1.5	0.125
Native Hawaiian or Pacific Islander	0.20	0.31	0.4	0.664
Sex				
Male	49.20	44.69	1.6	0.112
Age				
25-34 years old	13.80	28.30	7.4*	0.000
35-44 years old	12.60	33.44	11.1*	0.000
45-54 years old	12.60	20.90	4.4*	0.000
55-64 years old	12.80	11.25	0.8	0.413
65-74 years old	9.90	5.14	2.8*	0.005
75 years or older	6.60	0.32	4.5*	0.000

Note. United States population measures taken from U.S. Census (2019).