An Empirical Investigation Of Hacking Behavior

Siew H. Chan, (E-mail: Siew.Chan@wmich.edu), Western Michigan University
Lee J. Yao, La Trobe University, Australia

ABSTRACT

Currently, very limited research is available to help researchers and firms understand the behavior of hackers. As a result, misconceptions about hackers are formed based on lack of understanding about technology and failure in recognizing the differences among hackers. We use addiction, intrinsic motivation (state), and self-monitoring (trait) theories to explain hacking. We obtained 62 usable responses from hackers who completed our online research instrument. Our findings showed that intrinsically motivated hackers were less discouraged by the possibility of being discovered and the rules imposed by regulatory authorities; however, no significant result was reported for rules imposed by the profession. Individuals with high motivation to hack were found to be less discouraged by all three deterrence measures. Participants who perceived hacking to be more consistent with their internal cues were less discouraged by the possibility of being discovered and the rules imposed by regulatory authorities; however, no significant difference was found for rules imposed by the profession. Finally, contrary to our expectation, low self-monitors were more discouraged by all three deterrence measures than high self-monitors. Additional research is needed to provide insight into this finding.

INTRODUCTION

The Department of Justice defines computer crimes as "any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution" (Benson et al. 1997). Hacking, in particular, is defined as "the process of accessing computer systems by persons who have no legitimate access to the systems" in Computer Misuse Executive Briefing (1990) by Coopers and Lybrand Deloitte (Mulhull 1999). Hacking can undermine the fundamentals of financial systems by exposing the flaws in these systems. Poorly designed systems are susceptible to security breaches that can compromise the quality of financial and operational information that resides on these systems. Decision makers who use information compromised by breaches may face adverse economic consequences such as impaired reputation, higher costs to detect or correct the breaches, and potential legal liability (Campbell et al. forthcoming). A survey of 500 U.S. companies by the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) indicated an increase in reported financial losses of 21 percent (or $456 million) for 2002; mostly a result of organized, planned cyber-attacks (Farber 2003). TruSecure, a security firm, found that a company suffered an average loss of $475,000 as a result of the Blaster Worm infection (Varghese 2003).

The information age has created an environment whereby information is a key asset and information security is a strategic variable that helps firms gain a competitive advantage (Gordon et al. forthcoming). Recognition of the role of IT and its accompanying budgetary demands for compliance with regulatory requirements is critical in maintaining a firm's competitiveness. An annual survey revealed that 40% of the chief financial officers polled believed that compliance with the requirements of the Sarbanes-Oxley Act (SOA) would not affect their IT budget (Gates 2003). This belief illustrates a disconnection between chief financial officers and chief information officers (Gates 2003). Besides chief executive officers and chief financial officers, chief information officers are also affected by SOA because assurance of compliance is provided by the systems that contain the financial information (Imhoff 2004). Firms are expected to increase spending to comply with the requirements of SOA. AMR Research projected that firms would spend about $5.5 billion in 2004 to comply with SOA (www.dmreview.com). Software packages (e.g., IDS Scheer's ARIS Sarbanes-Oxley Audit Manager, Preventsys Network Audit and Policy Assurance System,

HandySoft's Sarbanes-Oxley Accelerator, SAP Compliance Management for Sarbanes-Oxley Act, SAS Corporate Compliance for Sarbanes-Oxley, and Vignette V7) are now available to help firms achieve compliance with SOA.

Computer Insider, a newsletter for hackers, estimated that about 900 hackers were hired during the past few years by organizations that they once targeted. For instance, after a hacker successfully created a negative balance in a German bank account, he received job offers from several German companies desperate for his expertise in beefing up their security systems from external threats (Cushing 2001). A survey conducted by CSI/FBI showed that 68% of the security professionals indicated that they would not hire reformed hackers, 15% said they would, and 17% were unsure. In a survey of IT professionals, white hat hackers who hacked for intrinsic reasons and reformed hackers who hacked for extrinsic reasons were reported to be more likely to be hired (Chan and Yao forthcoming). "White hat" hackers conduct penetration tests to identify system vulnerabilities and inform the owners of these problems (Cushing, 2001). These individuals are likely former hackers who have moved on to become security professionals (Thomas 2002). A reformed hacker is one who no longer hacks to exploit for personal gains (Chan and Yao forthcoming).

The question of whether former hackers should be hired is a controversial one. Firms may not hire former hackers because they are cautious of potential problems that may arise from hiring such individuals. Some firms prefer to play it safe than to risk hiring former hackers. Although preventive controls such as background checks are desirable in the hiring process, it is difficult to determine whether the former hackers are truly reformed and that they would not engage in activities to hack the systems of their prospective employers. A government agency hired a hacker to do research on its vulnerabilities but fired him later when he reported only one or two vulnerabilities each week and made these vulnerabilities known to his friends (Business Wire 2000). In another instance, upon interviewing a former hacker, a company found that the hacker still possessed a strong hacker mentality and had no choice but to disqualify him from further consideration for a job (Callaway 1996). On the other hand, it is possible that some hackers are reformed. For example, "Kuji", a former hacker, worked as a security consultant and was selected to head the marketing campaigns of some reputable companies (Cushing 2001). Another reformed hacker became a chief security officer of a security products company in Westboro (Weinstein 2002). Some believe that it takes a thief to catch a thief and that it may be appropriate to use a reformed hacker to simulate an attack (Bennett 2002). Thus, firms may hire hackers as part of their regular security control teams to combat information security breaches. Negative perceptions of hackers may be mitigated if these individuals can be reformed to assume the position of systems security officers and be assimilated into the firms' security control teams. Assimilation of reformed hackers into the workplace environment may increase the awareness of employees on the economic consequences of systems security breaches on business operations.

Law enforcement officials may be intimidated by hackers because they find technology too complicated to understand and the relationship between technology and punishment too difficult to discern (Thomas 2002). The paucity of research on hacking behavior impairs the ability of the judicial system in meting out effective deterrence measures for discouraging malicious attacks. The intentions of the perpetrators and the resultant damage or harm that they cause to a system or organization should be considered so that appropriate punishment can be imposed to deter malicious attacks. These actions may mitigate any misconceptions about unfair treatment of the perpetrators.[1] Knowledge of technology is what separates hackers from typical computer users and this increasingly wide gap poses a tremendous threat to security (Thomas 2002). People treat technology with hostility when systems are not perceived to be user friendly; as a result, expertise, control, and knowledge are needed for managing technology. Users' lack of understanding of technology contributes to their sense of helplessness with technology and this provides hackers with the opportunity to exert their authority with respect to their mastery and expertise in technology. This authority figure is usually a male because males dominate the computer industry. A layperson's lack of knowledge about technology leads to misconstrued conceptions about hackers and hacking.[2] Indeed, the media play a significant role in

[1] The hacking community expressed their outrage when they thought that the punishment imposed on Kevin Mitnick was harsh.

[2] A layperson's discomfort with her lack of knowledge of technology is demonstrated by our difficulty in getting this research study approved by a university's institutional review board. This research underwent three full board reviews over a period of several months. The first author had to attend the first meeting to explain the research to the board. A computer science faculty was asked to serve on the board as an adviser. We were not allowed to use our universities' systems. We were told to make sure that all identifying information that linked us to our respective universities be removed from our instrument housed at a website rented from an external web hosting company. We were not supposed to use our universities' email accounts. Instead, we had to set up email accounts with hotmail.com without identifying information that would link us to our respective

contributing to the misconceptions that the general public has about hackers. For example, the media portrayed Kevin Mitnick as a dangerous criminal and a "darkside hacker" despite the fact that no financial gains or damage to computer systems, files, or codes resulted from his hacking. Although these stories were later retracted, the labels attached to Mitnick stuck and had a lasting impact on his life (Thomas 2002). Thus, the stories that the media tell the public have a tremendous impact on their impression about hackers in general.

Prior research (e.g., Gordon and Loeb 2002; Gordon et al. forthcoming; Campbell et al. forthcoming) has examined the impact of systems security on the accounting, financial, and economic sectors. Using economics as a framework, these studies looked at variables such as the economic cost of publicly announced information security breaches and return on investment in information security. The market reacted negatively to security breaches involving unauthorized access to confidential information; however, no market reaction was reported for breaches that did not involve confidential information (Campbell et al. forthcoming). These findings suggest that the economic consequences of a security breach vary in accordance with the nature of the assets compromised by the breach (Campbell et al. forthcoming). Since substantial amounts of money are invested in information security activities, it is not surprising that chief financial officers are demanding a rational approach to such expenditures. This includes increased adoption of return on security investments as a measure to capture the cost-beneficial aspect of information security (Gordon and Loeb 2002). Although security systems may be effective at preventing security breaches with severe economic consequences, the breaches that do occur are often nuisances with inconsequential economic impact on firms (Anders 2000; Smith 2000). Thus, it may be rational to take a "wait-and-see" approach toward spending some of the funds earmarked for information security because of the uncertain occurrence of security breaches (Gordon et al. forthcoming). This reactive, as opposed to proactive, approach toward a significant portion of information security expenditures is consistent with the capital investment decisions frequently made by management. We contribute to the stream of research developed by Gordon and Loeb and their colleagues by examining the systems security problem from a behavioral perspective. The paucity of research on the behavior of a hacker may explain why the tremendous amount of resources committed to contain the hacking problem has resulted in somewhat little success.

The objectives of our study are to increase understanding on the behaviors of hackers by examining hacking as a state and trait, and to provide insight into whether deterrence measures would discourage hacking. We use addiction, intrinsic motivation (state), and self-monitoring (trait) theories to explain hacking. Addiction theory provides a framework for understanding the behaviors of hackers. We consider hacking as an addictive behavior because the interviews conducted by Thomas (2002) and Verton (2002) suggest that hackers are so engrossed in the activity that they frequently stay up all night to hack. These individuals indicated that they hacked for the sake of interest/enjoyment. Thus, we believe that it is appropriate to use intrinsic motivation theory to facilitate understanding on the hacking behavior. Intrinsic motivation is a state variable because it varies with respect to the type of activity or over a period of time. Since intrinsically motivated individuals hack for the sake of interest/enjoyment, deterrence measures such as the possibility of being discovered, and the rules imposed by regulatory authorities or the profession may not deter hacking. The positive affect[3] derived from interest/enjoyment in hacking may outweigh the negative affect associated with the deterrence measures. In addition, we modified the Perception of Task Value scale (developed by Eccles et al. 1983) to obtain a perception of hacking scale to measure a person's motivation to hack. In particular, we examine whether individuals with a high motivation to hack would be more discouraged by the deterrence measures than those with a low motivation to hack. Our perception of hacking scale (i.e., motivation to hack construct) includes four components: interest, importance, utility, and opportunity cost. The interest component is similar to the intrinsic motivation factor (i.e., interest/enjoyment). The purpose of our perception of hacking scale is to address the strength and intensity of the combined factors (i.e., interest, importance, utility, and opportunity cost) on the effectiveness of the deterrence measures in discouraging hacking. Finally, we use self-monitoring theory to provide insight into the individual characteristics of hackers. We use the self-monitoring scale (Snyder 1974, 1979, 1987) to classify our hacker participants into two categories: high or low self-monitors, and investigate whether the deterrence measures are effective at discouraging hackers with different personality traits.

---

universities. We were specifically instructed to print out, not forward via email, any emails received from our hacker participants to an administrator on the board.

[3] Affect is defined as our "liking, disliking, preference, evaluation, or the experience of pleasure or displeasure" (Zajonc 1980, p. 151).

The next section discusses the theoretical framework and the hypotheses posed in our study. The third section explains the research method used to address our hypotheses. The statistical results are presented in the fourth section. Finally, the contributions and limitations of our study, and suggestions for future research are discussed.

THEORETICAL FRAMEWORK AND HYPOTHESES

Using addiction theory as a framework, we examine hacking both as a state (intrinsic motivation) and trait (self-monitoring) to facilitate understanding on the behaviors of hackers. Intrinsic motivation and self-monitoring theories propose that internal (values, beliefs, and self-image) or external cues (recognition of achievements by and identification with social groups, financial incentives, or prestige) may impact a person's motivation to hack. Although individuals may experience interest or enjoyment in the performance of a specific activity (e.g., hacking), they may not perceive performance of activities in general to be interesting or enjoyable. Personality trait can help explain a person's predisposition or attitude toward an activity such as hacking.

Addiction Theory

Addicts lack self-identity and inner stability; therefore, they are prone to extreme experiences ranging from rigid self-control to total lack of control (Hirschman 1992). Addicts may possess an emotionally inadequate self and a false identity in early childhood, and may view addictive behaviors as essential to their daily functioning (Hirschman 1992). As a result, they may become dependent on frequently performed activities for intrinsic (i.e., interest or enjoyment) or extrinsic (i.e., recognition of achievements by and identification with social groups, financial incentives, or prestige) reasons. Addictive behaviors are difficult to change because they are performed frequently and automatically, and are habitual in nature (Tomer 2001). Addicts feel controlled by the commodity or activity because they treat the commodity or activity as the underlying reason for their existence (Tomer 2001).

We use addiction theory as a framework for explaining the behavior of hackers. We view hacking as an addictive behavior. This contention can be supported by the judicial system's treatment of hacking as a case of "substance abuse" (Thomas 2002). Indeed, one hacker described hacking as an obsessive behavior (Thomas 2002). Most hackers turn to hacking during their early adolescent years as a means to avoid problems at home or at school (Verton 2002). These individuals spend countless number of hours hacking because they not only derive interest or enjoyment from engaging in the act but also feel a sense of superiority in their ability to exercise control over the computer (Verton 2002). Addictive behaviors are compulsive and addicts experience craving for the given commodity or activity (Tomer 2001). It is difficult to deter addictive behaviors such as hacking. To counteract this problem, judges impose penalties that restrict hackers from accessing telephones, computers, and modems (Thomas 2002). In general, deterrence measures are imposed to discourage individuals from performing acts that are either socially undesirable or criminal in nature. However, limited research is available to help us understand circumstances where these deterrence measures will not be effective in deterring such acts.

Intrinsic Motivation

One's inherent motivation to perform an activity is considered an intrinsic motivation. In contrast to extrinsic motivation such as monetary reward, intrinsic motivation exists when an activity satisfies a person's need for competence and control (e.g., Lepper and Henderlong 2000; Ryan and Deci 2000). Intrinsic motivation occurs when "individuals are motivated to experience interest and … that a variety of goals may be associated with interest for different people and/or in different contexts" (Sansone and Smith 2000, p. 445). Individuals experience interest when their needs and desires are integrated with the activity. From this perspective, interest is the driving mechanism for all actions, including cognitive activity (Piaget 1981). In other words, an individual is said to be experientially interested when a certain quality of attention and sense of delight is present. Interest leads to the performance of intrinsically motivated behaviors (Deci 1998).

Intrinsic motivation has been examined as an outcome of an activity (i.e., a dependent variable) or as a process of engagement in the activity (i.e., an independent variable that predicts some dependent variable such as performance) (Sansone and Harackiewicz 2000). We examine intrinsic motivation (i.e., interest/enjoyment) as a

process of engagement in an activity where intrinsic motivation determines whether hackers who hack for the sake of interest/enjoyment would be discouraged by deterrence measures.

Motivation to Hack (Perception of Hacking Scale)

The motivation to hack construct is derived from motivation theory. We modified the Perception of Task Value scale (developed by Eccles et al., 1983) to obtain the perception of hacking scale to measure a person's motivation to hack. The value components of a person's motivation in a task include her goals for the task and beliefs about the importance, utility or interest of the task (Pintrich and De Groot 1990). These components can influence the strength or intensity of a behavior (Pintrich and Schrauben 1992). An individual's needs, goals, or values can interact with the characteristics of a task to determine the value of a task (Eccles et al. 1983). The four components of task value are: interest, importance, utility, and opportunity cost.[4] The interest factor is discussed in the section on intrinsic motivation. The importance value refers to how important it is for a person to perform well in a task (Eccles et al. 1983). Importance is also related to the relevance of engaging in an activity to either confirm or disconfirm salient features of actual or ideal self-schema (Wigfield and Eccles 1992). The utility value pertains to a person's perceived usefulness of the task in attaining specific goals (e.g., career prospects or outperforming others) (Pintrich and Schrauben 1992). The opportunity cost of a task refers to the time lost for engaging in other valued alternatives (Eccles et al. 1983).

We theorize that motivation to hack is high when an activity is perceived to be high in interest, importance or utility, or the opportunity cost of engaging in the activity is low. In contrast, motivation to hack is low when the activity is perceived to be low in interest, importance or utility, or the opportunity cost of engaging in the activity is high.

Self-monitoring Theory

Snyder's self-monitoring scale classifies individuals into two groups; namely, high and low self-monitors. Individuals with relatively high scores on the scale are classified as high self-monitors while individuals with relatively low scores are classified as low self-monitors. High self-monitors are concerned about how others perceive their behavior in various social contexts, as such they are adept at adjusting their behavior in accordance with situational appropriateness. High self-monitors may engage in an activity for extrinsic reasons such as recognition of their achievements by and identification with their social groups, financial incentives, or prestige. Low self-monitors are less likely to modify their behaviors to satisfy situational demands. They are more likely to act in accordance with relevant inner sources and are concerned about whether their behaviors in social contexts accurately reflect their underlying values, beliefs, and self-image. Consistent with self-monitoring theory, we predict that high self-monitors may hack for extrinsic reasons (i.e., recognition of their achievements by and identification with their social groups, financial incentives, or prestige) and low self-monitors may hack for intrinsic reasons (i.e., their underlying values, beliefs, and self-image).

Hypotheses

Behaviors are said to be intrinsically motivated when individuals experience interest/enjoyment in the performance of an activity (Deci 1992). Intrinsically motivated individuals receive their rewards in the form of the affective or cognitive experiences that accompany their behavior. We theorize that individuals may engage in hacking for the sake of interest/enjoyment. For example, one hacker indicated that he hacked because of the thrill and enjoyment that he derived from engaging in such an activity (Mulhall 1999). Support for our contention that hacking is an intrinsically motivated behavior can be found in the material of Eric Steven Raymond who defined the hacker attitude as a belief that hacking motivated the individual and facilitated learning (www.catb.org/~esr/faqs). Raymond also identified boredom and drudgery as impediments to the interest/enjoyment that individuals derived from hacking. A person's experience of interest during task performance can be a primary motivator for her continued performance

[4] Although these components can be differentiated, it is not easy to distinguish their relations (Jacobs and Eccles 2000). The correlations among interest, importance, and utility ranged from 0.51 and 0.79 in a sample of adolescents (Eccles and Wigfield 1995).

(Sansone, Wiebe, and Morgan 1999). To our knowledge, empirical research has not been conducted to examine hacking as an intrinsically motivated behavior or to address the question of whether deterrence measures would discourage hacking. Since intrinsically motivated behaviors are performed for the sake of interest/enjoyment, deterrence measures such as the likelihood that the activity is discovered and the rules imposed by regulatory authorities or by the profession may not discourage hacking. This leads to the first set of hypotheses:

H1a: Compared to non-intrinsically motivated individuals, intrinsically motivated individuals are less discouraged by the possibility of being discovered.

H1b: Compared to non-intrinsically motivated individuals, intrinsically motivated individuals are less discouraged by the rules imposed by regulatory authorities.

H1c: Compared to non-intrinsically motivated individuals, intrinsically motivated individuals are less discouraged by the rules imposed by their profession.

Along a similar line of reasoning put forth in the first set of hypotheses, we theorize that individuals with a high motivation to hack would be less discouraged by deterrence measures such as the possibility of being discovered and the rules imposed by regulatory authorities and by their profession than individuals with a low motivation to hack. Thus,

H2a: Compared to individuals with a low motivation to hack, individuals with a high motivation to hack are less discouraged by the possibility of being discovered.

H2b: Compared to individuals with a low motivation to hack, individuals with a high motivation to hack are less discouraged by the rules imposed by regulatory authorities.

H2c: Compared to individuals with a low motivation to hack, individuals with a high motivation to hack are less discouraged by the rules imposed by their profession.

In addition, we examine hacking as a personality trait. We use the self-monitoring scale developed by Snyder (1974, 1979, 1987) to classify individuals into two groups: high or low self-monitors. We propose that high self-monitors may hack because of external cues such as recognition of their achievements by and identification with the hacking community, financial incentives, or prestige.[5] If these external cues are removed, the deterrence measures may discourage high self-monitors from hacking. In contrast, low self-monitors may act in accordance with internal cues such as their underlying values, beliefs, and self-image. They perceive their rewards in terms of expression of attributes associated with their egos. They may not perceive monetary rewards or social recognition to be as valuable as the reward that they receive from their ability in establishing their self-identity and confirmation of the notion of the kind of people they perceive themselves to be (Katz 1960). These individuals believe that hacking establishes or confirms their underlying values, beliefs, and self-image. Thus, low self-monitors are unlikely to be discouraged by deterrence measures. This leads to the third set of hypotheses:

H3a: Compared to high self-monitors, low self-monitors are less discouraged by the possibility of being discovered.

H3b: Compared to high self-monitors, low self-monitors are less discouraged by the rules imposed by regulatory authorities.

H3c: Compared to high self-monitors, low self-monitors are less discouraged by the rules imposed by their profession.

We feel that it is necessary to conduct separate tests on the impact of a hacker's underlying values, beliefs, and self-image (i.e., internal cues) on the effectiveness of deterrence measures. The purpose of these tests is to provide additional insight into the findings obtained in hypotheses 3a, 3b, and 3c. Finally,

H4a: Compared to individuals who perceive hacking to be less consistent with their internal cues, individuals who perceive hacking to be more consistent with their internal cues are less discouraged by the possibility of being discovered.

[5] These factors are examples of extrinsic motivation. Since we were not aware of any prior empirical study that examined the behaviors of hackers, we were unable to determine beforehand if our sample would include individuals who hacked because of their extrinsic motivation.

H4b: Compared to individuals who perceive hacking to be less consistent with their internal cues, individuals who perceive hacking to be more consistent with their internal cues are less discouraged by the rules imposed by regulatory authorities.

H4c: Compared to individuals who perceive hacking to be less consistent with their internal cues, individuals who perceive hacking to be more consistent with their internal cues are less discouraged by the rules imposed by their profession.

RESEARCH METHOD

Procedures

One of the authors approached his contacts (most likely hackers) for help in recruiting hackers for our study.[6] These contacts were requested to make our website address and password known to the hacking community. The purpose of the password was to prevent non-target participants (i.e., those who were not hackers) from accessing and completing our online research instrument.[7] The media that the contacts used to make our website address and password known to the hacking community were undisclosed. We speculate that the contacts might have used the Internet Relay Chat to broadcast our study to the hacking underground.[8] Our research instrument was housed at a website rented from an external web hosting company and our data were stored on the university's network of the first author. We felt that it was necessary to store our data on a secured university's network. Codes were written to protect the anonymity of the university's network system and to minimize potential tampering of our data. Our web developer monitored our data for potential hacking activity. He did not find any hacking activity throughout the entire duration of our study. The first author also accessed our website regularly during the entire period that our research instrument was online to ensure that it was working properly and that our data were not hacked or tampered with. Our website was not defaced or hacked throughout the entire period that it was online.

Research Instrument

An overview of our study appeared on the first page of our website. Participants were required to enter a password for accessing our research instrument. They were assured of their confidentiality with respect to their participation in our study. Specifically, participants were informed that their IP addresses would not be tracked and that all log files would be destroyed.[9] We provided our hotmail accounts (without any identifying information that linked us to our university affiliations) so that participants could express their concerns or problems with the way that our study was conducted. Our research instrument[10] consisted of three sections and the estimated completion time was 30 minutes. The first section contained an 18-item self-monitoring scale. A series of questions pertaining to hacking were found in the second section and the final section collected the participants' demographics information. At the end of the experiment, participants were thanked for their participation and asked to provide their mailing addresses if they wished to receive their incentive payment of $10.[11] They were assured that their mailing addresses

[6] The books written by Verton (2002) and Thomas (2002) are based on interviews conducted with some hackers. However, these authors seemed to be associated with the media. It is extremely difficult to obtain hacker subjects because of the unique nature of their activity and the legal implications of hacking. Thus, we believe that it is appropriate to approach one of the authors' contacts to obtain participants for our study.

[7] An individual who hacked to gain access to our website and complete our online instrument would be an appropriate participant for our study.

[8] Unexpectedly, the first author managed to come into contact with a hacker when her identity and affiliation with a university were discovered. We suspected that the hacker might have obtained her personal data from the website where she registered the domain name for our study; i.e., www.academia-research.com. The hacker told the first author that our website would be defaced or hacked if our study were not for research purposes. She engaged in several email communications with the hacker. Eventually, she managed to convince the hacker to help her complete our research instrument and recruit participants for our study.

[9] Since the second author was out of jurisdiction, the web developer downloaded the data from the university's network and sent the data file (without the IP addresses and log files) to the second author. The second author deleted the participants' mailing addresses from the data file after he mailed the incentive payments to the participants. He then sent the data file (without the participants' mailing addresses) to the first author for analysis.

[10] A web developer at a university put the instrument online and wrote the code for collecting the data. He complied with the requirements of the institutional review board in ensuring the anonymity of the university. We pretested our instrument with some graduate students at a university. Valuable comments were also received from faculty members at a university.

[11] Motivation researchers are careful in their administration of incentive payments because of their impact on intrinsic motivation. Since we used an incentive payment that was non task-contingent in nature, it should not have an impact on intrinsic motivation. Our t test results show that incentive payment did not have an impact on our dependent variables.

would be destroyed after payment was sent. Some participants provided their email addresses instead of their mailing addresses. One of the authors checked with them via email if they wished to receive their incentive payment. Two participants declined payment.[12]

Participants

Seventy-six participants completed our online research instrument. Fourteen individuals indicated that they had not hacked previously. As such, their data were excluded from analysis[13], resulting in 62 usable responses: 46 males and 16 females. Participants' ages ranged from 17 to 45 and their mean age is 27. 74% of the participants were employed and 26% were unemployed. 11% had less than a high school education, 40% had a high school diploma, 31% had a bachelor's degree, 11% had a master's degree, and 7% had a doctoral degree. The two major cultural groups are Asians (71%) and Caucasians (21%). Participants' professional certifications include application development (34%), communications (21%), database (27%), hardware (21%), help desk (18%), Internet/Web (31%), networking (29%), operating system (31%), and security (21%).

DATA ANALYSIS AND RESULTS

We operationalized our independent and dependent variables via a series of questions in our research instrument. Exhibit 1 shows how these variables are measured via the participants' responses to the questions.

Independent Variables

Interest/Enjoyment

The interest/enjoyment variable has two levels; that is, the participants either hacked or did not hack for the sake of interest/enjoyment. Participants checked their responses to the following question: Why do you continue to engage in hacking? Those who checked the interest/enjoyment option were assumed to hack for the sake of interest/enjoyment. Participants who did not check this option were not assumed to hack for interest/enjoyment.

Motivation to Hack

The original Perception of Task Value scale has two items in each of the interest, importance, utility, and opportunity cost subscales. We decided to include only one item in our utility subscale because it would be redundant to include two items in this subscale. We found that one measure of interest and one measure of opportunity cost were significantly correlated with each other but not significantly correlated with the remaining items in the subscales. As such, we excluded these two items from the perception of hacking scale. The correlation coefficients for the remaining five items range from 0.43 to 0.85 ($p=0.000$). The reliability coefficient alpha for these five items is 0.90. The motivation to hack construct was obtained by averaging each participant's responses to the five items in the perception of hacking scale. Table 1 presents the reliability analysis of the five items in the perception of hacking scale.

Self-monitoring Scale

Participants were split into two groups based on their scores on the 18-item self-monitoring scale. The more extreme selection criteria of upper and lower quartiles (scores of 13 and above and 7 and below respectively) can be used to increase the purity of the class samples[14] (Synder 1987). Using the more extreme selection criteria as a guideline for classifying the sample, our participants' scores on the self-monitoring scale are as follows: 17 scored 7 or below, 15 scored 13 or above, and 30 scored between 8 and 12. We decided to depart slightly from the more extreme selection criteria by classifying participants with scores of 7 or below as low self-monitors and those with

[12] One of the authors received emails from some participants. These emails were positive in that they addressed the value of our research.
[13] This action was necessary despite the fact that it actually weakened the results of our study.
[14] Scores of 10 or 11 can be used to split the participants into two groups. Those who scored 10 or below on the self-monitoring scale were classified as low self-monitors and those who scored 10 or above on the scale were categorized as high self-monitors (Gangestad and Synder 1985).

scores of 8 or above as high self-monitors. This decision was made so that 30 participants who scored between 8 and 12 can be classified.[15]

Exhibit 1

Independent Variables	
Interest/Enjoyment	
Why do you continue to engage in hacking? (Yes=checked, No= not checked)	
Motivation to Hack (Perception of Hacking Scale)	
1.	In general, I find hacking (very boring…..very interesting)
2.	I feel that being good at hacking is (not at all important…..very important)
3.	How important is it for you to do well at hacking? (not at all important…..very important)
4.	How useful to you is hacking? (not at all useful…..very useful)
5.	How much does the time you spend on hacking keep you from doing other things you would like to do? (takes away no time…..takes away a lot of time)
*Measured on a 7-point scale. The opportunity cost component is reverse scored.	
Internal Cues	
1.	Do you believe that hacking is consistent with your underlying values?
2.	Do you believe that hacking is consistent with your underlying beliefs?
3.	Do you believe that hacking enhances your self-image?
*Measured on a 7-point scale with 1=not at all and 7=to a great extent	
Self-monitoring Scale	
1.	I find it hard to imitate the behavior of other people.
2.	At parties and social gatherings, I do not attempt to do or say things that others will like.
3.	I can only argue for ideas which I already believe.
4.	I can make impromptu speeches even on topics about which I have almost no information.
5.	I guess I put on a show to impress or entertain others.
6.	I would probably make a good actor.
7.	In a group of people I am rarely the center of attention.
8.	In different situations and with different people, I often act like very different persons.
9.	I am not particularly good at making other people like me.
10.	I am not always the person I appear to be.
11.	I would not change my opinions (or the way I do things) in order to please someone or win their favor.
12.	I have considered being an entertainer.
13.	I have never been good at games like charades or improvisational acting.
14.	I have trouble changing my behavior to suit different people and different situations.
15.	At a party I let others keep jokes and stories going.
16.	I feel awkward in company and do not show up quite as well as I should.
17.	I can look anyone in the eye and tell a lie with a straight face (if for a right end).
18.	I may deceive people by being friendly when I dislike them.
*Participants indicated their responses to each question in the self-monitoring scale by selecting either the True or False option. The questions were keyed in the high self-monitoring direction.	
Dependent Variables	
Deterrence Measures	
1.	How likely will the possibility of being discovered discourage you from hacking?
2.	How likely will the rules imposed by your profession discourage you from hacking?
3.	How likely will the rules imposed by regulatory authorities discourage you from hacking?
*Measured on a 7-point scale with 1=not likely and 7=very likely	

[15] Since the self-monitoring theory does not suggest a middle group, we did not create a middle group for comparison purposes.

Table 1: Reliability Analysis of Perception of Hacking Scale

Item	Mean	Std Dev
INT2	4.7581	1.8703
IMP1	4.0968	2.1555
IMP2	3.6935	2.1923
USEFUL	3.6452	2.0890
TIME1	4.4194	2.1313

Correlation Matrix

	INT2	IMP1	IMP2	USEFUL	TIME1
INT2	1.0000				
IMP1	0.5427	1.0000			
IMP2	0.4494	0.7592	1.0000		
USEFUL	0.4308	0.7432	0.8457	1.0000	
TIME1	0.7867	0.6369	0.6525	0.6231	1.0000

*The correlation coefficients for all five items are significant at p=0.000. The reliability coefficient alpha for these items is 0.90.

Label	Description of Item
INT2:	In general, I find hacking (very boring…..very interesting)
IMP1:	I feel that being good at hacking is (not at all important…..very important)
IMP2:	How important is it for you to do well at hacking? (not at all important…..very important)
USEFUL:	How useful to you is hacking? (not at all useful…..very useful)
TIME1:	*How much does the time you spend on hacking keep you from doing other things you would like to do? (takes away no time…..takes away a lot of time)

* Reverse scored

Internal Cues

The internal cues construct consists of three measures: values, beliefs, and self-image. The correlation coefficients for these measures range from 0.41 to 0.90 (p=0.000 or 0.001). The reliability coefficient alpha for the items is 0.81. The internal cues construct was derived by averaging each participant's responses to each of the items. Table 2 shows the reliability analysis of the three measures in the internal cues construct.

Table 2: Reliability Analysis of Internal Cues Construct

Item	Mean	Std Dev
VALUES	3.4355	2.0295
BELIEFS	3.3871	2.1831
IMAGE	2.5484	1.5647

Correlation Matrix

	VALUES	BELIEFS	IMAGE
VALUES	1.0000		
BELIEFS	0.9012	1.0000	
IMAGE	0.4243	0.4072	1.0000

*The correlation coefficients for the three items are significant at p=0.000 or p=0.001. The reliability coefficient alpha for these items is 0.81.

Label	Description of Item
VALUES:	Do you believe that hacking is consistent with your underlying values?
BELIEFS:	Do you believe that hacking is consistent with your underlying beliefs?
IMAGE:	Do you believe that hacking enhances your self-image?

Dependent Variables

Deterrence Measures

The deterrence measures were obtained separately via the participants' responses to each of the following three questions (on a 7-point scale with 1=not likely and 7=very likely):

1. How likely will the possibility of being discovered discourage you from hacking?
2. How likely will the rules imposed by your profession discourage you from hacking?
3. How likely will the rules imposed by regulatory authorities discourage you from hacking?

Results

ANOVA was used to test hypotheses 1a, 1b, 1c, 3a, 3b, and 3c. Since the independent variables for hypotheses 2a, 2b, 2c, 4a, 4b, and 4c are continuous in nature, regression was used to test these hypotheses. The results are found in Table 3. Hypothesis 1 proposes that intrinsically motivated individuals are less discouraged by deterrence measures such as the possibility of being discovered and the rules imposed by regulatory authorities and by their profession. We found that intrinsically motivated individuals were less discouraged by the possibility of being discovered (p=0.000) and by the rules imposed by regulatory authorities (p=0.017); however, no significant difference was reported for rules imposed by the profession. Thus, hypotheses 1a and 1b are supported but hypothesis 1c is not supported. The insignificant result obtained in hypothesis 1c could be attributed to our participants' definition of the term "profession". Our participants may consider the hacking community as their profession and think that the hacking community would not impose rules to deter hacking. Hypothesis 2 states that participants with high motivation to hack are less discouraged by the possibility of being discovered and the rules imposed by regulatory authorities and by their profession. This hypothesis is supported at p=0.000 for all three deterrence measures. The results for hypothesis 3 are opposite to what we have expected. Low self-monitors were more discouraged by the likelihood of being discovered (p=0.002), and the rules imposed by regulatory authorities (p=0.021) and by their profession (p=0.000).[16] These findings contradict self-monitoring theory. This can be attributed to the unique nature of our participants and the hacking activity, and the diverse cultural background of our participants.[17] Hypothesis 4 examines whether individuals who feel that hacking is more consistent with their internal cues are less discouraged by the possibility of being discovered and the rules imposed by regulatory authorities and by their profession. We found that participants who felt that hacking was more consistent with their internal cues were less discouraged by the likelihood of being discovered (p=0.004) and by the rules imposed by regulatory authorities (p=0.045); however, no significant difference was reported for rules imposed by the profession. Thus, hypotheses 4a and 4b are supported but hypothesis 4c is not supported. The insignificant result obtained in hypothesis 4c could be explained by a similar reasoning process suggested in hypothesis 1c. Specifically, participants may feel that the hacking community; that is, their profession, would not impose rules to deter hacking.

[16] Use of the extreme selection criteria led to significant results for possibility of being discovered (p=0.00) and rules imposed by the hackers' profession (p=0.03), and marginally significant result (p=0.10) for rules imposed by regulatory authorities.

[17] A colleague offered another potential explanation for the opposite results obtained in hypothesis 3. Low self-monitors may overreact to external cues because they normally would not pay attention to these cues. On the other hand, high self-monitors may be more accustomed to dealing with external cues and as such they may have more realistic expectations with respect to such cues. Future research may consider these differences in terms of perceptions of risk.

Table 3: Results of Hypotheses

Panel A: Hypothesis 1 (ANOVA)				
Independent Variable	**Option**	**Mean**	**Dependent Variable**	**p-value**
Interest/enjoyment	Yes	2.63	Possibility of being discovered	0.000
	No	4.51		
	Yes	2.96	Rules imposed by regulatory authorities	0.017
	No	4.23		
	Yes	2.93	Rules imposed by profession	0.334
	No	3.43		
*Interest/enjoyment had two levels: checked=1 (Yes); unchecked=0 (No) as indicated in the Option column.				
Panel B: Hypothesis 2 (Regression)				
Independent Variable	**Dependent Variable**	**Mean**	**t**	**p-value**
Motivation to hack	Possibility of being discovered	3.69	5.047	0.000
	Rules imposed by regulatory authorities	3.68	5.376	0.000
	Rules imposed by profession	3.21	4.202	0.000
Panel C: Hypothesis 3 (ANOVA)				
Independent Variable	**Level**	**Mean**	**Dependent Variable**	**p-value**
Self-monitor	High	3.16	Possibility of being discovered	0.002
	Low	5.12		
	High	3.29	Rules imposed by regulatory authorities	0.021
	Low	4.71		
	High	2.58	Rules imposed by profession	0.000
	Low	4.88		
Panel D: Hypothesis 4 (Regression)				
Independent Variable	**Dependent Variable**	**Mean**	**t**	**p-value**
Internal cues	Possibility of being discovered	3.69	3.022	0.004
	Rules imposed by regulatory authorities	3.68	2.048	0.045
	Rules imposed by profession	3.21	0.914	0.364
*The dependent variables were based on a 7-point Likert scale with 1=not at all and 7=to a great extent.				

Additional Analyzes

We conducted additional tests to provide additional insight into our findings. Exhibit 2 shows the questions (taken from our research instrument) for additional analysis. We examined the impact of the participants' reasons for hacking on the effectiveness of various deterrence measures. The results are presented in Table 4. Participants who continued to hack for interest were found to be less discouraged by the possibility of being discovered (p=0.000) and by the rules imposed by regulatory authorities (p=0.017), and more discouraged by a ban on future access to systems (p=0.029). Individuals who continued to hack for challenge were less discouraged by the rules imposed by regulatory authorities (p=0.021). Those who continued to hack for curiosity were more discouraged by imprisonment (p=0.043) and a ban on future access to systems (p=0.021). Participants who continued to hack for fun were more discouraged by imprisonment (p=0.009). A ban on future access to systems precludes convicted computer criminals from future engagement in hacking. Since individuals may perceive hacking to be interesting or challenging, they might be more devastated by a ban on future access to systems than by the consequences of discovery of the act or non-compliance with the rules imposed by regulatory authorities. Individuals who hacked for recognition by the hacking community were less discouraged by publicity of their hacking activity (p=0.002) and their identity (p=0.000). Those who hacked for financial incentives were less discouraged by the rules imposed by regulatory authorities (p=0.021) and the possibility of losing their job (p=0.000). Individuals who hacked for prestige were less discouraged by publicity of their hacking activity (p=0.002). Those who hacked to identify with the hacking community were less discouraged by a fine (p=0.000), censure by their profession (p=0.000), publicity of their hacking activity (p=0.002), and publicity of their identity (p=0.000).

Table 4: Impact of Reasons for Hacking on Effectiveness of Various Deterrence Measures

Reasons for Hacking*	Option	Mean	Various Deterrence Measures	p-value
Interest/enjoyment	Yes	2.63	Possibility of being discovered	0.000
	No	4.51		
	Yes	2.96	Rules imposed by regulatory authorities	0.017
	No	4.23		
	Yes	0.59	Ban on future access to systems	0.029
	No	0.31		
Challenge	Yes	3.00	Rules imposed by regulatory authorities	0.021
	No	4.24		
Curiosity	Yes	0.65	Imprisonment	0.043
	No	0.39		
	Yes	0.58	Ban on future access to systems	0.021
	No	0.29		
Fun	Yes	0.70	Imprisonment	0.009
	No	0.37		
Recognition by hacking community	Yes	0.00	Publicity of hacking activity	0.002
	No	0.16		
	Yes	0.00	Publicity of identity	0.000
	No	0.31		
Financial incentives	Yes	2.75	Rules imposed by regulatory authorities	0.021
	No	3.74		
	Yes	0.00	Loss of job	0.000
	No	0.38		
Prestige	Yes	0.00	Publicity of hacking activity	0.002
	No	0.16		
Identify with hacking community	Yes	0.00	Fine	0.000
	No	0.34		
	Yes	0.00	Censure by profession	0.000
	No	0.29		
	Yes	0.00	Publicity of hacking activity	0.002
	No	0.16		
	Yes	0.00	Publicity of identity	0.000
	No	0.31		

*Participants indicated their responses by checking all the applicable options for the following question: Why do you continue to engage in hacking? We coded the checked option as 1 (Yes) and the unchecked option as 0 (No).

We analyzed the demographic data to gain understanding on our participants' reasons for hacking and the effectiveness of various deterrence measures. The results are shown in Table 5. Compared to females, males hacked more for the sake of interest (p=0.012). Hacking enhanced the self-image of males more than that of females (p=0.011). Females were more discouraged by the possibility of being discovered (p=0.002), the rules imposed by their profession (p=0.055), and censure by the IT community (p=0.053). Compared to those aged 25[18] or below, participants aged above 25 hacked more for the sake of challenge (p=0.032) and were less discouraged by publicity of their hacking activity (p=0.015). A comparison of the two major cultural groups revealed that Caucasians hacked more for the sake of interest than Asians (p=0.015) and that they hacked more for desire to identify with the hacking community (p=0.021). Caucasians also perceived hacking to be more consistent with their values (p=0.000) and beliefs (p=0.000). Asians were more discouraged by the possibility of being discovered (p=0.000), and by the rules imposed by their profession (p=0.051) and regulatory authorities (p=0.000).

[18] The median was used to split the participants into two age groups.

Exhibit 2

Reasons for Hacking
Why do you continue to engage in hacking? (Please check all applicable boxes)
____ interest/enjoyment
____ recognition of achievement by the hacking community
____ challenge
____ financial incentives
____ prestige/status
____ identification/association with the hacking community
____ curiosity
____ political motives
____ fun
____ others (please specify)

Other Deterrence Measures
What kinds of consequences would discourage you from hacking? (Please check all applicable boxes)
____ imprisonment
____ fine
____ censure by your profession
____ censure by the IT community
____ ban on future access to systems
____ loss of job
____ publicity of your hacking activity
____ publicity of your identity
____ others (please specify)

*We coded the checked option as 1 and the unchecked option as 0.

Table 5: Analysis of Demographics

Demographics	**Group**	**Mean**	**Reasons for Hacking/ Various Deterrence Measures**	**p-value**
Gender (46 males; 16 females)	Male	0.52	Interest	0.012
	Female	0.19		
	Male	2.78	Image	0.011
	Female	1.88		
	Male	3.17	Possibility of being discovered	0.002
	Female	5.19		
	Male	2.91	Rules imposed by profession	0.055
	Female	4.06		
	Male	0.15	Censure by IT community	0.053
	Female	0.44		
Age (median=25; range=17 to 45)	<= 25	0.31	Challenge	0.032
	> 25	0.59		
	<= 25	0.25	Publicity of hacking activity	0.015
	> 25	0.03		
Ethnicity (2 major groups: 44 Asians; 13 Caucasians)	Asians	0.32	Interest	0.015
	Caucasians	0.69		
	Asians	1.89	Identify with hacking community	0.021
	Caucasians	3.54		
	Asians	2.86	Values	0.000
	Caucasians	5.31		
	Asians	2.70	Beliefs	0.000
	Caucasians	5.38		
	Asians	4.18	Possibility of being discovered	0.000
	Caucasians	2.08		
	Asians	3.50	Rules imposed by profession	0.051
	Caucasians	2.31		
	Asians	4.25	Rules imposed by regulatory authorities	0.000
	Caucasians	1.92		

CONCLUDING REMARKS

Implications

Systems security is an important issue that has received considerable attention as a result of the increasing number of attacks on information systems. Despite the importance of this issue, very little empirical research is available for promoting understanding on the hacking behavior and the effectiveness of deterrence measures in discouraging hacking. The source of the problem (i.e., the underlying behaviors of hackers) should be understood before effective measures can be implemented to mitigate this problem. In this respect, our study makes a significant contribution to the systems security literature in that we use addiction, intrinsic motivation, and self-monitoring theories to provide valuable insight into the behaviors of hackers. Using addiction theory as a framework, we examine hacking both as a state and trait. Our findings suggest that it is difficult to discourage an intrinsically motivated behavior such as hacking. Indeed, one hacker stated that only death would stop him from hacking. We found that individuals who hacked for the sake of interest/enjoyment were less discouraged by the possibility of being discovered and the rules imposed by regulatory authorities; however, we did not find any significant result for rules imposed by the profession. Interestingly, we found that those with a high motivation to hack were less discouraged by all three deterrence measures. Since the perception of hacking scale consists of four components (i.e., interest, importance, utility, and opportunity cost), the motivation to hack construct may be a more comprehensive measure for assessing the effectiveness of the deterrence measures in discouraging hacking. Contrary to the predictions of self-monitoring theory, we found that relative to the high self-monitors, low self-monitors were more discouraged by all three deterrence measures. We use the internal cues construct to provide additional insight into this finding. Our results suggested that individuals who perceived hacking to be more consistent with their underlying values, beliefs, and self-image were less discouraged by the possibility of being discovered and the rules imposed by regulatory authorities; no significant result was reported for rules imposed by the profession. Further, we found that the self-monitoring scale was weakly correlated with the internal cues construct (i.e., values, beliefs, and self-image).

The results of our study may help clear some of the misconceptions that a layperson might have about hackers and hacking. The negative connotation that the general public attaches to hackers may have an impact on the severity of punishment imposed by the judicial system. The hacking community may also challenge any uniform punishment meted out to hackers. Since intrinsically motivated individuals hack for the sake of interest/enjoyment, they may not harbor malicious intentions to harm any individual, system, or organization. Indeed, firms can consider assimilating these individuals into their systems security control teams to help combat security breaches. However, perpetrators who hack for malicious intentions should be punished and the severity of such punishment should be a function of the hackers' malicious intentions and the extent of damage or harm caused to the target.

Limitations

Our sample may comprise primarily hackers who perceived hacking as an intrinsically motivating activity. Although we believe that hacking is an intrinsically motivated behavior, our sample may not be representative of the entire hacking population. However, we did not have control over the participants self-selecting themselves into our study. Only four participants indicated that they hacked for prestige or financial incentives[19], or to identify with or to have their achievements recognized by the hacking community. One individual indicated that he hacked for political motives. Since these reasons are extrinsic in nature, there is evidence that some individuals may hack because of their extrinsic motivation[20]. A sample of four is too small for any meaningful examination of the behavior of extrinsically motivated individuals; however, this opens up an avenue for future research.

[19] For example, a group of hackers stole one million credit card numbers over the Internet, revealed the break-in, posted the credit card numbers on the Internet, and offered to provide "security" services for a fee (Wallace 2001). In another instance, a Russian hacker stole more than 55,000 credit cards from creditcards.com (a website that processes transactions for online merchants) and posted about 25,000 credit card numbers online when his demand for $100,000 was ignored (Hopper 2001).

[20] Extrinsic motivation is defined as a person's "orientation toward money, recognition, competition, and the dictates of others" (Amabile et al. 1994, p. 951).

Future Research

Our predictions about the behavior of hackers based on self-monitoring theory are opposite to what we have expected. One potential explanation could be the unique nature of our sample. Future work can provide insight into this contradictory finding. In addition, the general public's misconceptions about hackers and hacking can be attributed to failure in recognizing the behavioral differences among different groups of hackers. One hacker categorized hackers into five groups: "young and stupid", "coders", "anarchist", "security professionals", and "elite". This person felt that the "young and stupid" group caused the most problem because they did not understand the implications and costs associated with their activity. He indicated that "coders" write codes to prove to a non-technical person that anything is possible and that "anarchists" believe that all information should be free. He stated that "security professionals" create a self-sustaining need for themselves by releasing vulnerabilities to the hacking community. The "elite" group reflects the lifestyle of the hacking underground.

Additional research is needed to help firms determine whether they should hire former hackers or individuals who claim that they are reformed. Firms might consider hiring a white hat or reformed hacker. Finally, future research can help identify individuals who hack because of extrinsic motivation, and provide insight into whether deterrence measures such as the possibility of being discovered and the rules imposed by regulatory authorities or by the profession, or other penalties would discourage extrinsically motivated individuals from hacking.

References

1. Advisory/Axent security expert available to discuss hiring hackers; modern day pirates or robin hoods? *Business Wire*, August 14, 2000, pp. 2190.
2. Anders, G. eBay's CEO reacts to hacker attack, seeks joint action on Web security. *Wall Street Journal*, February 10, 2000.
3. Amabile, T. M., Hill, K. G., Hennessey, B. A., and Tighe, E. M. The Work Preference Inventory: Assessing intrinsic and extrinsic motivational orientations. *Journal of Personality and Social Psychology* (66), 1994, pp. 950-967.
4. AMR Research: Sarbanes-Oxley compliance spending will exceed $5 billion in 2004. *DM Review*, January, 2004.
5. Bennett, M. Can you trust an ethical hacker? *IT Week*, http://www.vnunet.com, April 12, 2002.
6. Benson, C., Jablon, A. V., Kaplan, P. J., and Rosenthal, M. E. Computer crimes. *American Criminal Law Review* (34-2), 1997, pp. 409-443.
7. Callaway, E. Breach of security. *PC Week*, December 23, 1996.
8. Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security* (forthcoming).
9. Chan, S. H., and Yao, L. J. An exploratory study on systems security and hacker hiring. *Review of Business Information Systems* (8), 2004, pp. 17-28.
10. Cushing, K. Would you turn to the dark side? *Computer Weekly*, 2001.
11. Deci. E. L. The relation of interest to the motivation of behavior: A self-determination theory perspective. In *The Role of Interest in Learning and Development*, A. K. Renninger and S. Hidi (eds.), Hillsdale, NJ: Erlbaum, 1992, pp. 43-70.
12. Deci, E. L. The relation of interest to motivation and human needs – The self-determination theory viewpoint. In *Interest and Learning: Proceedings of the Seeon Conference on Interest and Gender*, L. Hoffmann, A. Krapp, K. Renninger, and J. Baumert, (eds.), Kiel, Germany: IPN, 1998, pp. 146-163.
13. Eccles (Parsons), J. S., Adler, T. F., Futterman, R., Goff, S. B., Kaczala, C. M., Meece, J. L., and Midgley, C. Expectancies, values, and academic behaviors. In *Achievement and Achievement Motives*, J. T. Spence (ed.), New York: W. H. Freeman and Company, 1983, pp. 75-146.
14. Eccles, J. S., and Wigfield, A. In the mind of the achiever: The structure of adolescents' academic achievement related beliefs and self-perceptions. *Personality and Social Psychology Bulletin* (21), 1995, pp. 215-225.
15. Farber, D. Cybersecurity report card: Serious improvements needed. *Tech Update*, May 30, 2003.

16. Gangestad, S., and Snyder, M. To carve nature at its joints: On the existence of discrete classes in personality. *Psychological Review* (92), 1985, pp. 317-349.
17. Gates, R. Sarbanes-Oxley: Ten things you must do in 90 days or else! http://www.bettermanagement.com, September 13, 2003.
18. Gordon, L. A., and Loeb, M. P. The economics of information security investments. *ACM Transactions on Information and System Security* (5-4), 2002, pp. 438-457.
19. Gordon, L. A., and Loeb, M. P. Return on information security investments: Myths vs. realities. *Strategic Finance*, 2002, pp. 26-31.
20. Gordon, L. A., Loeb, M. P., and Lucyshyn, W. Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal* (forthcoming).
21. Hirschman, E. C. The consciousness of addiction: Toward a general theory of compulsive consumption. *Journal of Consumer Research* (19), September 1992, pp. 155-179.
22. Hopper, D. I. Credit card hacker warning issued. *Associated Press*, March 9, 2001.
23. Imhoff, C. Intelligent solutions: The year of compliance, Part 1. *DM Review*, January 2004.
24. Jacobs, J. E., and Eccles, J. S. Parents, task values, and real-life achievement-related choices. In *Intrinsic and Extrinsic Motivation: The Search for Optimal Motivation and Performance*, C. Sansone and J. M. Harackiewicz (eds.), San Diego: Academic Press, 2000, pp. 405-439.
25. Katz, D. The functional approach to the study of attitudes. *Public Opinion Quarterly* (24), 1960, pp. 163-204.
26. Lepper, M. R. and J. Henderlong. The role of interest in learning and self-regulation: "Extrinsic versus "intrinsic" motivation reconsidered. In *Intrinsic and Extrinsic Motivation: The Search for Optimal Motivation and Performance*, C. Sansone and J. M. Harackiewicz (eds.), San Diego: Academic Press, 2000, pp. 257-307.
27. Mulhall, T. Where have all the hackers gone? Part 3: Motivation and deterrence. *Computers & Security* (16), 1999, pp. 291-297.
28. Piaget, J. Intelligence and affectivity: Their relationship during child development. *Annual Reviews*, Palo Alto, 1981. (Original work published in 1954).
29. Pintrich, P. R., and De Groot, E. V. Motivational and self-regulated learning components of classroom academic performance. *Journal of Educational Psychology* (82-1), 1990, pp. 33-40.
30. Pintrich, P. R., and Schrauben, B. Students' motivational beliefs and their cognitive engagement in classroom academic tasks. In *Student Perceptions in the Classroom*, D. H. Schunk and J. L. Meece (eds.), Hillsdale, NJ: Erlbaum, 1992, pp. 149-183.
31. Raymond, E. S. www.catb.org/~esr/faqs, March 14, 2004.
32. Ryan, R. M. and E. L. Deci. When rewards compete with nature: The undermining of intrinsic motivation and self-regulation. In *Intrinsic and Extrinsic Motivation: The Search for Optimal Motivation and Performance*, C. Sansone and J. M. Harackiewicz (eds.), San Diego: Academic Press, 2000, pp. 13-54.
33. Sansone, C., Wiebe, D. J., and Morgan, C. Self-regulating interest: The moderating role of hardiness and conscientiousness. *Journal of Personality* (67-4), 1999, pp. 701-733.
34. Sansone, C. and J. M. Harackiewicz. Controversies and new directions – Is it déjà vu all over again? In *Intrinsic and Extrinsic Motivation: The Search for Optimal Motivation and Performance*, C. Sansone and J. M. Harackiewicz (eds.), San Diego: Academic Press, 2000, pp. 443-453.
35. Sansone, C. and J. L. Smith. Interest and self-regulation: The relation between having to and wanting To. In *Intrinsic and Extrinsic Motivation: The Search for Optimal Motivation and Performance*, C. Sansone and J. M. Harackiewicz (eds.), San Diego: Academic Press, 2000, pp. 341-372.
36. Smith, G. Love bug victims don't want a cure. *Wall Street Journal*, May 8, 2000.
37. Snyder, M. The self monitoring of expressive behavior. *Journal of Personality and Social Psychology* (30), 1974, pp. 526-537.
38. Snyder, M. Self-monitoring processes. In *Advances in Experimental Social Psychology*, L. Berkowitz (ed.), New York Academic Press, 1979.
39. Snyder, M. *Public appearances private realities: The psychology of self-monitoring*. New York W. H. Freeman and Company, 1987.
40. Thomas, D. *Hacker Culture*. University of Minnesota Press, 2002.

41. Tomer, J. F. Good habits and bad habits: A new age socio-economic model of preference formation. *Journal of Socio-Economics* (25-6), 1996, pp. 619-638.
42. Varghese, S. Blaster worm took heavy toll: Survey. http://www.theage.com.au, September 23, 2003.
43. Verton, D. *The hacker diaries: Confessions of teenage hackers*. McGraw Hill, 2002.
44. Wallace, B. European hackers plunder U.S. firms, FBI says 40 victims in 20 states were hit. *San Francisco Chronicle*, March 9, 2001.
45. Weinstein, B. Should you hire an ex-hacker? http://www.builder.com, June 11, 2002.
46. Wigfield, A., and Eccles, J. S. The development of achievement task values: A theoretical analysis. *Developmental Review* (12), 1992, pp. 265-310.
47. Zajonc, R. B. Feeling and thinking: Preferences need no inferences. *American Psychologist* (35-2), 1980, pp. 151-175.

NOTES