# The Role of Economic Incentives and Disincentives in Deterring Insider Hacking Behavior

Laura Amor *School of Management*
*State University of New York at Buffalo*
Buffalo, USA
lccasey@buffalo.edu

Joana Gaia *School of Management*
*State University of New York at Buffalo*
Buffalo, USA
joanaalu@buffalo.edu

David Murray *School of Management*
*State University of New York at Buffalo*
Buffalo, USA
djmurray@buffalo.edu

G. Lawrence Sanders *School of Management*
*State University of New York at Buffalo*
Buffalo, USA
mgtgsand@buffalo.edu

Sean Sanders *School of Information Technology*
*Illinois State University*
Normal, USA
spsand1@ilstu.edu

Raghav Singh *School of Management*
*State University of New York at Buffalo*
Buffalo, USA
rsingh46@buffalo.edu

Shambhu Upadhyaya *Computer Science*
*State University of New York at Buffalo*
Buffalo, USA
shambhu@buffalo.edu

***Abstract*—The objective of the research in this paper is to investigate the influence of economic incentives, income levels, interest in White-Hat capabilities, and perceptions of being apprehended on the willingness to violate privacy regulations. The research model was developed by drawing on the economics of crime literature, prospect theory, and the emerging Capability, Opportunity, and Motivation behavioral model. This study involved a sample of 523 people on the brink of entering the workforce as potential insider hackers. Despite many subjects believing there is a high probability of being caught, they could still be incentivized to violate HIPAA laws. Approximately 306 (58%) of the survey participants indicated a price, ranging from zero dollars to more than $10 million, that they considered acceptable for violating the HIPAA laws. Income levels, white-hat hacking capabilities, monetary incentives to commit a crime, and the perceived probability of being apprehended were statistically significant predictors of the amount of money required to violate HIPAA laws.**

***Keywords*—Behavioral economics, economics of crime, cybersecurity, hacking, and insider threats.**

## I. Introduction

The 1996 Health Insurance Portability and Accountability Act created a comprehensive set of restrictions to maintain the privacy of health information for patients [1]. Healthcare privacy breaches have become increasingly prevalent with the increasing use of digital records and interconnected systems. In a recent survey, nearly 60% of the 400 healthcare organizations respondents in all sectors reported a ransomware attack in 2024 [2]. Approximately 42% took up to a month to recover

from the ransomware attack, 29% took from one to three months, and 7% took three to six months.

According to the FBI's Internet Crime Report, the US experienced an unprecedented increase in cyber attacks and malicious activity in 2022, when losses were more than $10.3 billion [3]. Cybercrime is not just a US problem, as security breaches worldwide are growing [4]. The pandemic put additional stress on employees and organizations, with an estimated third of data breaches traced to insiders. Insider incidents have increased by 25% with the move to remote work, the ever-present employee feelings of job insecurity, and the technological ease of moving massive amounts of data to and from the cloud [5].

Insider threats are more pernicious than external threats. A recent study in Virginia found insider attacks cost between $20,000 and $100,000, and the median outsider attack resulted in $5,000 to $10,000 losses. The most common insider attack involved impersonating the organization in emails and social media, and outsider attacks involved viruses, spyware, or malware (59%) [6].

More than three-quarters of organizations involved in maintaining critical national infrastructure have seen an increase in insider-driven cyber threats in the last three years [7]. The cybersecurity landscape for maintaining supply chains in the face of catastrophic events has many challenges due to numerous vulnerabilities and the emergence of sophisticated threats and potential natural disasters [8]. Global supply chains have been exposed to a wide range of catastrophes with increasing frequency. Threats are attributed to negligence, human error, and criminal intent and are exacerbated by reductions in cybersecurity budgets and the financial stress of employees caused by inflation and the economic downturn [9], [10]. System users and employee negligence, coupled with process failures, are the root of many cyberattacks [11].

With the goal of mitigating insider threats, we examine a number of issues related to cybersecurity. Section II reviews the study's research frameworks, including the Capability, Opportunity, and Motive behavioral model (COM-B), deterrence theory, and prospect theory as mechanisms for understanding hacking behavior. Section III discusses the research hypotheses related to salary levels, white-hat hacking interests, and how perceived apprehension influences the decision to violate privacy laws. Section IV details the research methodology related to the survey of the 523 participants, including analyzing their responses under varying scenarios. Section V discusses the model and hypotheses assessment and confirms the significant links between income levels, perceptions of being apprehended, and hacking decisions. Section VI discusses the implications of the findings, including the drift of the white hat to the dark side and the managerial implications of the study. The Conclusion and Future Directions section (VII) emphasizes organizational strategies to deter insider threats and best practices to develop a culture of cybersecurity awareness. It also provides future directions for insider education, research, and training.

## II. Background and Related Work

### A. Capabilities, Motives and Opportunities

To understand the occurrence of insider attacks and their connection to hacking behavior, we apply several theories. The first of these is the classical Capability, Opportunity, and Motive Behavioral model (COM-B), which helps conceptualize insider attacks. In the COM-B model, the perpetrator must have the ability to attack, the motive to attack, and the opportunity to violate a security law [12], [13].

Solid technical skills are relatively abundant among millennials and Generation Z. Both generations are interested in technology and embrace it in their work environment and lifestyle [14]. However, insiders with weak skills can still leverage their organizational knowledge using the abundance of online information on hacking. They can also turn to the Darknet and Deep Web to purchase hacking expertise [13]. Of course, motivations to hack are readily available and usually relate to financial difficulties, such as credit card debt, student loans, and health insurance premiums [15]. There are also numerous instances in which a disgruntled employee is disappointed with a supervisor who has passed them over for a raise and turns to hacking [16]. After several months in a new position, employees gain insight and a comprehensive understanding of organizational systems. If an opportunity arises and an employee is under job or financial stress, there may be a temptation to engage in hacking.

### B. Deterrence Theory

Deterrence aims to use threats and sanctions to inhibit criminal behavior [17]. The idea is that high probabilities of arrest and conviction, along with adequate punishment levels, will deter criminal behavior. The research results for the role of deterrence in criminal behavior are mixed [18]. For example, there is evidence that perceptions of sanctions have a modest impact on behavior. However, the severity of the punishment has a negligible effect on criminal activity. Research has found a substantial indirect effect when formal sanctions trigger informal sanctions. Informal sanctions can take the form of shame, ridicule, social disapproval, and other similar measures.

In the context of cybersecurity, implementing sanctions can be challenging due to the significant burden of monitoring [19]. Passive sanctions have been proposed as a way to counteract the expense and burden of continuous monitoring. For example, rather than constantly checking for strong passwords, the organization will only hold employees accountable when a breach related to a weak password has occurred.

Criminals use a decision calculus to evaluate returns of criminal activity as a function of the probability of getting caught and the severity of the punishment [20], [21]. The certainty of punishment is a function of the perceived probability of apprehension, the likelihood of being charged, the probability of conviction, and the probability of formal sanctions [22]. An individual will consider committing cybercrime when the net expected gains from illegal activity

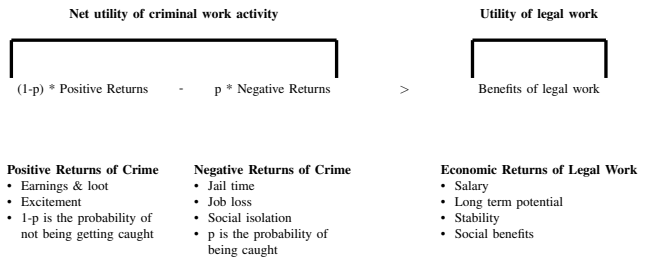


Fig. 1. Becker crime utility model (adapted)

are greater than the utility of engaging in legal work (see Figure 1). The p term in the model is the perception of the probability of being captured or caught multiplied by the sum of the negative returns. The 1-p probability is multiplied by the sum of the positive returns. If criminal work's net utility is greater than legal work's, the budding cybercriminal may be attracted to illegal hacking behavior.

Maintaining a high level of deterrence is expensive. The goal of police and courts is to reduce enforcement costs to a level where the various stakeholders are economically comfortable. The optimal stakeholder enforcement scheme focuses on setting the probability of apprehension as low as possible. The objective is to manipulate the perceived likelihood of apprehension and to reduce enforcement costs.

### C. Severity of Punishment

Severe prison sentences do not always improve deterrence [23]. There has always been disagreement on the relationship between the severity of punishment and deterrence. For example, suppose that there is a 10% probability of being convicted for one year or a 1% probability of being convicted for ten years. In both cases, the expected negative returns of participating in criminal activity lead to the same result [24]. However, people view them differently. The National Institute of Justice (NIJ), examined research by Nagin, 2013 on the role of lengthy and mandatory prison sentences in deterring [25]. The NIJ considers long mandatory sentences expensive and ineffective in preventing crime and that perceptions of being caught and punished is the key to deterrence. Pickett has found experimental evidence that publicity can increase deterrent fear, but also that increasing sanctions has a decreasing impact on deterrence [26].

### D. Prospect Theory

Prospect theory is a powerful behavioral economics theory that helps explain how people make choices and select paths when faced with risky outcomes. It was originally developed by Kahneman and Tversky [27], [28]. Nobel Laureate Richard Thaler further enhanced it [29]–[31]. Prospect theory posits that (see Figure 2) risk preferences are a function of risk aversion and loss aversion and that people are more averse to situations with potential losses [32]. The decision maker uses a utility-based calculus that incorporates probabilities and a weighting function to assess possible outcomes.

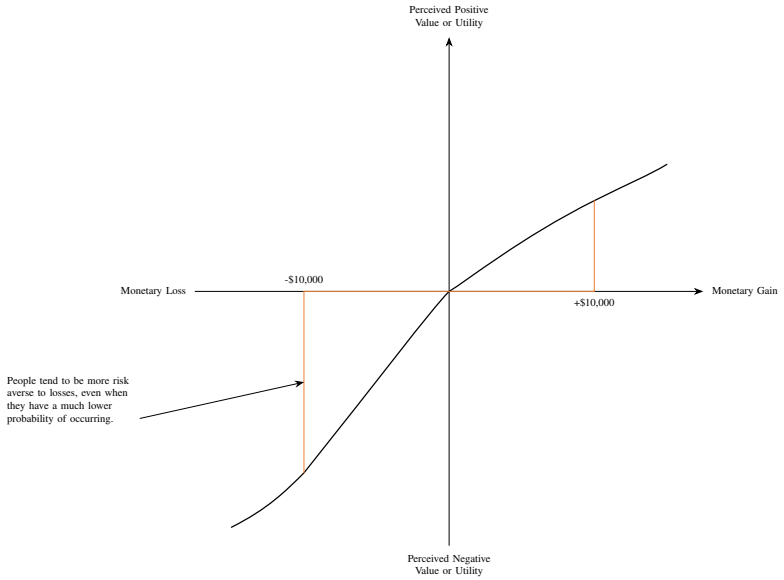


Fig. 2. Prospect Theory and aversion to losses

Prospect theory posits that people overreact to small probability events and underreact to significant probability events. For example, a small probability of being bitten by a shark while swimming may cause people to avoid the ocean. The Jaws movie had a profound influence on perceptions of shark attacks and, indeed, caused widespread panic, although the risk of attack is very low [33]. Even today, many people remain reluctant to swim in the ocean due to the movie. Climate change presents the other side of the coin. Many scientists and climatologists believe that there is a high probability that record-breaking climate change will occur [34], [35]. However, cognitive biases, mental maps, and the longing for normality and safety lead many to underestimate the potential impact on society [36]. The key is that perceived differences are a function of individual perceptions and are related to the personal situation or context.

Prospect theory offers insight and justification for using different income levels to examine the impact of personal income on the potential to engage in illegal activity. We will examine the role of increasing monetary incentives on an insiders' deviant behavior decisions using a scenario where salaries are $30,000, $55,000, and $100,000. We will investigate whether high-income individuals are less likely to violate privacy laws and are more likely to demand higher compensation to release health information.

### E. Integrating Behavioral Economic Theory and the COM-B framework

The Capability, Opportunity, and Motivation leading to Behavior (COM-B) model is a comprehensive model for understanding the dynamic process that guides human behavior [37], [38]. A capability in the context of cybersecurity involves having the psychological capacity, technical skills, social engineering skills, and an interest in pursuing hacking activities [39]. An opportunity involves the opportunity to participate in legal or illegal behavior. Motivation involves

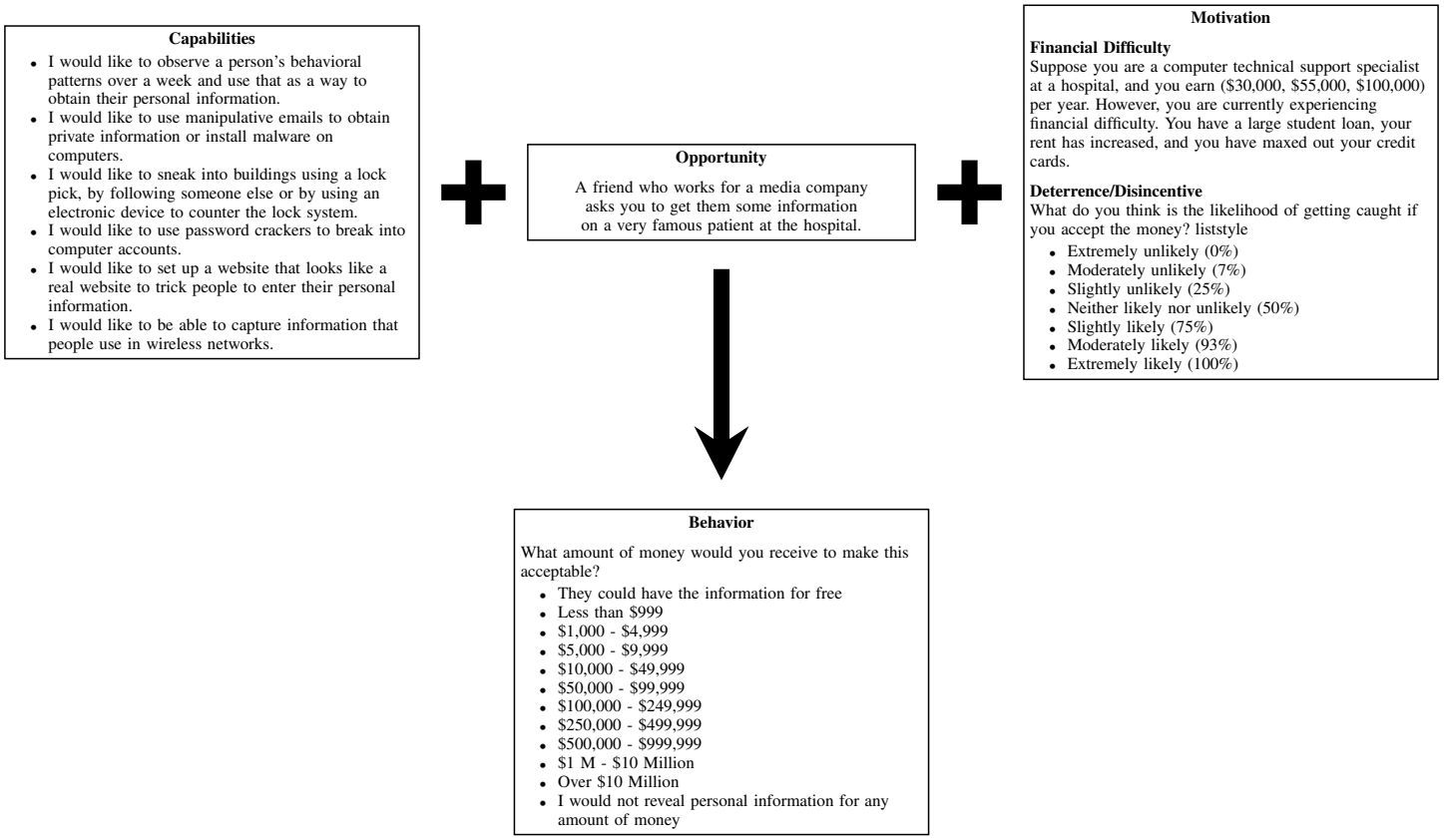


Fig. 3. The Capability, Opportunity, Motivation and Behavior Model

cognitive processes that direct behavior and an analytical decision-making process that integrates the positive and negative consequences of pursuing a behavior.

The COM-B model was developed by integrating well-known behavioral theories and US criminal law theory, and is proving relevant to the economics of crime literature. U.S. criminal law requires that to prove guilt, the person must have the capability to commit the crime, the opportunity, and the motive to commit the crime. Although the model is relatively new, it has been extensively cited [38]. The COM-B model complements and supports behavioral economics research, amplifying our understanding of illicit security behavior. Figure 3 illustrates how the model integrates with the constructs and items used in this project.

## III. Research Hypotheses

As noted above, subjects use a decision calculus to determine whether they will engage in illegal behavior. The decision to engage in criminal activity is a function of the probability of getting caught and the certainty and severity of punishment [20], [21].

In the seminal Becker model [20], individuals use a rational calculus, weighing the costs against the benefits of engaging in illicit behavior to maximize their own interests in the context of their current income. Individuals, for example, with higher salaries, perceive more significant financial and reputational losses. As a result, the monetary incentives to engage in unlawful acts should be higher than those individuals who receive lower wages.

As such, we posit that higher-salary individuals will require greater returns, or more money, to violate HIPAA laws.

*H1*: Higher salary levels in the scenario ($30,000, $55,000, and $100,000) are positively related to higher requirements for monetary incentives to violate HIPAA.

According to COM-B, possessing a set of cybersecurity hacking skills entails having both technical and social engineering skills to participate in hacking activities [35]. Individual capabilities encompass expertise and interest in utilizing those capabilities related to cybercrime. A person who has hacking skills should require less money to participate in a hacking activity. In a study involving 124 countries, researchers found that the economic capital and technological capital of a country are the main factors that influence the frequency of cybercrime originating within the country [40]. This line of research is related to moral drift, which will be examined in greater depth later. Can white-hat hackers migrate to gray-hat or black-hat activities? The net effect is that having strong capabilities to commit a cyber crime, having the opportunity and the motivation to commit the crime. should lead to requiring lower monetary incentives to induce participation in a security breach.

*H2*: Higher interest in White-hat hacking **capabilities**

is positively related to **lower** requirements for monetary incentives in the HIPAA scenario.

White-hat hackers, also known as ethical hackers, are responsible for identifying and addressing security vulnerabilities. They are considered ethical because, despite using tools similar to those of black-and-gray-hat hackers, they operate within the boundaries of the law. Black-hat hackers, often referred to as crackers, typically engage in illegal activities for personal gain. Gray-hat hackers occupy a middle ground between white and black-hats, balancing on the edge of criminal and civil liability. They are often ideologically driven and may target adversarial political positions, company policies, or even nation-states. Sometimes, they are called hacktivists, and they may function as white-Hats during the day, helping companies secure their systems, and as ideological hackers by night, pursuing their own justice through unauthorized actions.

Cybercrime requires technical expertise and extensive training to be carried out effectively [41]. The net effect is that an ensemble of cybersecurity specialists is required to implement social engineering and spear phishing approaches. Insiders are particularly problematic when they have technical skills and decide to engage in social engineering tactics. Insiders with strong technical skills understand the inner workings of organizational processes and can easily disrupt operations. As an employee's tenure increases, so does their insight as they can contemplate security flaws and procedural faults in the systems. Job movement is one way to address this issue, but in the interest of specialization and productivity, it is rarely considered a mechanism to improve security. Computer hacking begins with talent and is enabled by poor controls in schools, organizations, and society [42]. The result is that an interest in white-hat technologies and processes may lead an individual to engage in black-hat and gray-hat activities. This leads to the following hypothesis.

*H3a*: Higher interest in White-hat hacking **capabilities** is positively related to **higher** interest in Black-Hat hacking when they are assured they will not get caught.

*H3b*: Higher interest in White-hat hacking **capabilities** is positively related to **higher** interest in Gray-Hat hacking when they are assured they will not get caught.

The final hypothesis relates to the probability of being apprehended. Previous research has shown that the crime market model assumes that offenders, victims, and law enforcement participate in optimizing behaviors related to preferences and that offenders have expectations about returns and individual sensitivity to being caught and the resulting punishment [15], [43]. Thus, we include a construct to validate that the probability of being apprehended influences the amount of money required for an individual to release HIPAA data for a famous person.

*H4*: Higher perceptions of the probability of apprehension are positively related to **higher** requirements for monetary incentives to violate HIPAA.

## IV. Methodology

The white-hat, black-hat, and gray-hat scales and the scenario used in this study can be viewed in the appendix. The white-hat, black-hat, and gray-hat scales were previously validated [44]. The scenario was adapted from a study that identified the role of monetary incentives in violating HIPAA regulations and privacy laws [15]. The scenario was randomly assigned to each subject at salary levels of $30,000, $55,000, and $100,000.

We were concerned that the subject's discretionary income would influence their responses. So, we also included their discretionary income as a control variable.

We recruited 593 undergraduate, junior, and senior subjects enrolled in management information systems and a data analytics class to complete an online Qualtrics survey. The study was approved by the Institutional Review Board (IRB). The final number of subjects used in the analysis was 523. We excluded subjects from the study who did not answer more than 10% of the questions or who took less than two minutes to complete the survey [45]. We have found that student populations provide a solid foundation for researching and investigating hacking because they will enter the workforce and are the future foundation of the emerging workforce. In addition, there is strong evidence in the context of behavioral research that students are very similar to nonstudents [46]. In addition, subject pools from platforms such as Mechanical Turk pose their own problems because it is difficult to assess their generalizability. Students are generally less concerned with social desirability issues than employed people. The net effect is that employees who are part of the work environment studied are reluctant to answer the questions honestly because they do not want to diminish their social prestige [47], [48].

## V. Model and Hypothesis Assessment

We utilized the most recent version of SmartPLS to conduct a partial least squares analysis, examining the research model and its accompanying hypotheses. SmartPLS is a robust statistical tool that is effective in handling complex multidimensional latent variables and is an excellent tool for prediction [49].

We first examined individual loadings and internal consistency to test the reliability of the latent variables. The loadings for all measurement items were greater than 0.75. Cronbach's alpha for all constructs was greater than 0.9, indicating internal reliability [50]. One criterion for evaluating partial least squares path models is the coefficient of determination ($r^2$). According to Cohen [51], a small $r^2$ effect size is less than approximately 0.14, a medium effect size is between 0.14 and 0.26, and a large effect size is greater than 0.26.

Figure 4 presents the overall results for the research model. The path coefficients are listed first, and the p-values for the paths are in parentheses and highlighted in bold if they are significant at the .05 level. The p-values were generated using

TABLE I
RESULTS FOR HYPOTHESES

| Hypotheses | Path coefficient | p-value | Supported |
|---|---|---|---|
| H1: Higher levels of salary in the scenario ($30,000, $55,000 and $100,000) are positively related to higher requirements for monetary incentives to violate HIPAA. | 0.126 | 0.001 | Yes |
| H2: Higher interest in White hat hacking capabilities are positively related to lower requirements for monetary incentives in the HIPAA scenario | -0.230 | 0.00 | Yes |
| H3a: Higher interest in White hat hacking capabilities are positively related to higher interest in Black Hat hacking when they are assured they will not get caught. | 0.670 | 0.000 | Yes |
| H3b: Higher interest in white hat hacking capabilities are positivley related to higher interest in Gray Hat hacking when they are assures they will not get caught. | 0.759 | 0.000 | Yes |
| H4: Higher perceptions of the probability of apprehension are positively related to higher requirements for monetary incentives to violate HIPAA. | 0.326 | 0.000 | Yes |

1,000 bootstrapped samples. The $r^2$ for the required money was 0.228.

The $r^2$ for the gray hacking was 0.576. The $r^2$ for the black-hat hacking was 0.449. All of the hypotheses were supported. The results of the hypothesis tests are presented in Table I.

The findings suggest that people who have a strong interest in **ethical hacking (White-Hat)** are also more likely to participate in **gray-hat activities**, possibly due to overlapping skill sets or a shared drive for exploratory problem solving. The findings indicate that individuals with a pronounced interest in **ethical hacking (White-Hat)** may also be more inclined to engage in **black-hat activities**, potentially motivated by financial incentives and supported by their existing technical competencies.

Recall that the scenario was presented to the participants as follows:

- Suppose you are a computer technical support specialist at a hospital, and you earn ($30,000, $55,000, $100,000) per year. However, you are currently experiencing financial difficulty. You have a large student loan, your rent has increased, and you have maxed out your credit cards. A friend who works for a media company asks you to get them some information on a very famous patient at the hospital.
- What amount of money would you receive to make this acceptable?
- What do you think is the likelihood of getting caught if you accept the money?

The path from White-Hat to Money Required has a statistically significant negative coefficient. This implies that the level of interest in white-hat hacking will reduce the amount of money required to violate privacy regulations. The statistically significant path (.326) from Probability of Apprehension to money Required) is substantial and positive. This implies that people who believe they will be caught will want more money to violate privacy laws.

Approximately 33% of the subjects were told they made $30k, 33% told they were paid $55k, and 33% were told they were paid $100k. The path coefficient (.126) was positive and statistically significant from Salary to Money Required. This suggests that higher-salaried individuals may require more resources if approached to violate a privacy or HIPAA law.

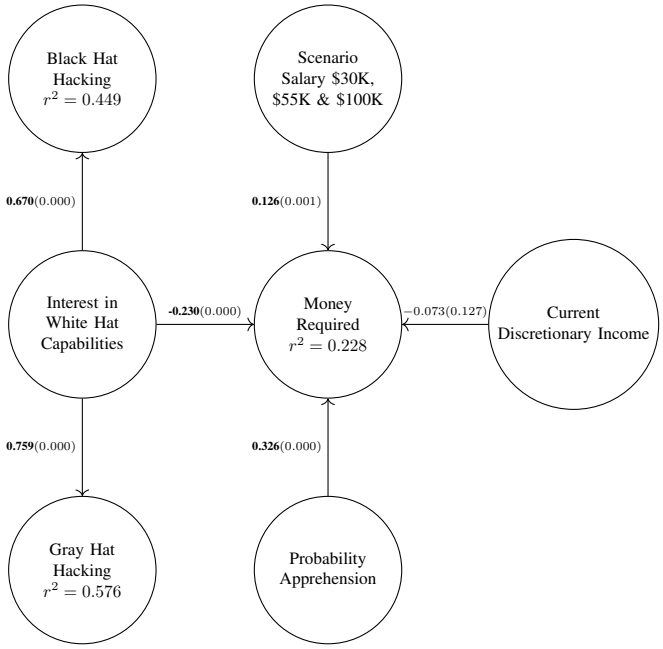


Fig. 4. Model Results

The path from Current Discretionary income to Money Required was not statistically significant. This question was an attempt to determine whether the actual discretionary income would influence their responses. This implies that the survey respondents were able to distance their income from the survey scenario. In essence, the **nonsignificant path** from discretionary income to money required (p = 0.127) suggests that the subject's discretionary income alone does not strongly influence monetary temptation in the context of the research scenario.

## VI. DISCUSSION

Data are a precious asset that organizations want to protect, but the breach of personal and health information has severe organizational consequences. Our analysis of the survey data uncovers an intricate relationship between perceived risk of being caught, white-hat capabilities, salary levels, and financial incentives.

One of the main areas of interest in this paper was the influence of income levels on the amount of money

TABLE II
RELATIONSHIP BETWEEN INCENTIVES AND APPREHENSION

| IT Worker | | Perceived probability of being apprehended | | | | | Percentage |
|---|---|---|---|---|---|---|---|
| | | Up to 25% | 50% | 75% | 93% plus | Total | |
| Amount of money willing to receive | < $10,000 | 27 | 10 | 7 | 6 | 50 | 10% |
| | $10,000 - $99,999 | 21 | 10 | 6 | 5 | 42 | 8% |
| | $100,000 - $999,999 | 38 | 21 | 28 | 20 | 107 | 20% |
| | > $1,000,000 | 30 | 20 | 18 | 39 | 107 | 20% |
| | No amount of money | 28 | 24 | 21 | 144 | 217 | 41% |
| Total | | 144 | 85 | 80 | 214 | 523 | 100% |
| Percentage | | 28% | 16% | 15% | 41% | 100% | |

required for an individual to violate the HIPAA laws. Higher income levels are positively related to higher requirements for monetary incentives, with a path coefficient of -0.126 and a p-value of .001. This is an integral part of the decision calculus used by potential perpetrators of the law crime. We also performed a means test and found statistically significant differences between the three income levels for the amount of money required (F-statistic of 4.244 and p-value of .015). The amount required was a categorical variable (for example, less than $999, $1,000 - $4,999). To gauge the magnitude of the differences, we calculated a midpoint for each category and then used this midpoint calculation to determine the amount required to violate the HIPAA law. We then performed a simple ANOVA comparing the salary levels. The average amount of money required for the $30,000 salary was $2,203,487 for the $55,000 salary it was $2,847,510 and for the $100,000 salary it was $3,306,556 (F statistic of 2.403 and p-value of.09).

It is important to note that the amount of the participants' current discretionary income was not related to the amount of money required. However, the survey subjects were able to project themselves into one of the three income scenarios. They are more sensitive to greater losses of income, which supports the economics of crime literature, rational choice theory, and prospect theory.

Table II and Figure 5 present some of the descriptive statistics of the study. Here are some of the key takeaways from the results.

- Ten percent of the subjects were willing to release their health information for less than $10,000. And more than half of this group perceive that the risk of being caught is as low as 25%. This category represents an immediate potential threat to companies.
- At the extreme end of the price spectrum, 107 subjects ($\sim$ 20%) are willing to sell data for amounts exceeding $1,000,000. A substantial portion of this group perceives a high probability of being apprehended. Hence, they require significant financial rewards to justify the high risk.

The good news is that 41% of respondents would not sell data under any circumstances. Most of these individuals perceive a high probability (93% plus) of being caught, suggesting that they are well aware of the risks associated with such actions and may also have ethical values.

### *A. Drift to the Dark Side: White-Hat Hacking Interest Can Lead to Black-Hat Hacking and Gray-Hat Hacking*

A key concern is whether white-hat hackers might transition to gray-hat or even black-hat activities. Are white-hat hackers susceptible to moral drift? We found support for the drift hypotheses H3a and H3b. A notable example of this shift is documented in American Kingpin [52], which recounts the story of Ross Ulbricht, the creator of the Silk Road darknet marketplace that allowed people to engage in mostly illegal transactions using cryptocurrency. One of the agents investigating Ulbricht eventually succumbed to the criminal temptation, driven by monetary allure.

This research and the papers discussed above highlight the influence of financial incentives on the likelihood that an individual will violate privacy laws. Since people can drift to the dark side, the next question is what personality traits lead to being involved in white-hat hacking.

Freed [53] found that cybersecurity specialists have significantly higher scores of openness, assertiveness, extraversion, and adventurousness and significantly lower scores of acceptableness, empathy, trust, vulnerability, and self-confidence. Many hackers are motivated by what they dislike, rather than what they like [54]. Interest in hacking can be driven by peer recognition, a desire for respect, and the opportunity to participate in team activities. It is not always motivated by intellectual challenges and the pursuit of justice.

The Dark Triad has been used to understand the motivation to participate in hacking. It consists of three personality traits that are considered socially undesirable. Individuals who have high scores for Machiavellianism are manipulative, deceitful, and exploitative. Individuals who have high scores on narcissism are self-centered and seek attention. Individuals who score high on the psychopathy scale lack remorse, are cynical, and insensitive [55]–[57]. Maasberg et al. [58] proposed a research model that integrated the dark triad and the capability, motive, and opportunity (COM-B) framework.

Recently, research has found that Machiavellianism, narcissism, psychopathy, and thrill-seeking are significant predictors of attraction to white-hat hacking. And that there is a very striking correlation with psychopathy and Machiavellianism and an interest in white-hat hacking [59].

### *B. Managerial Implications*

We used the COM-B research model, deterrence theory, and prospect theory to explore how economic incentives

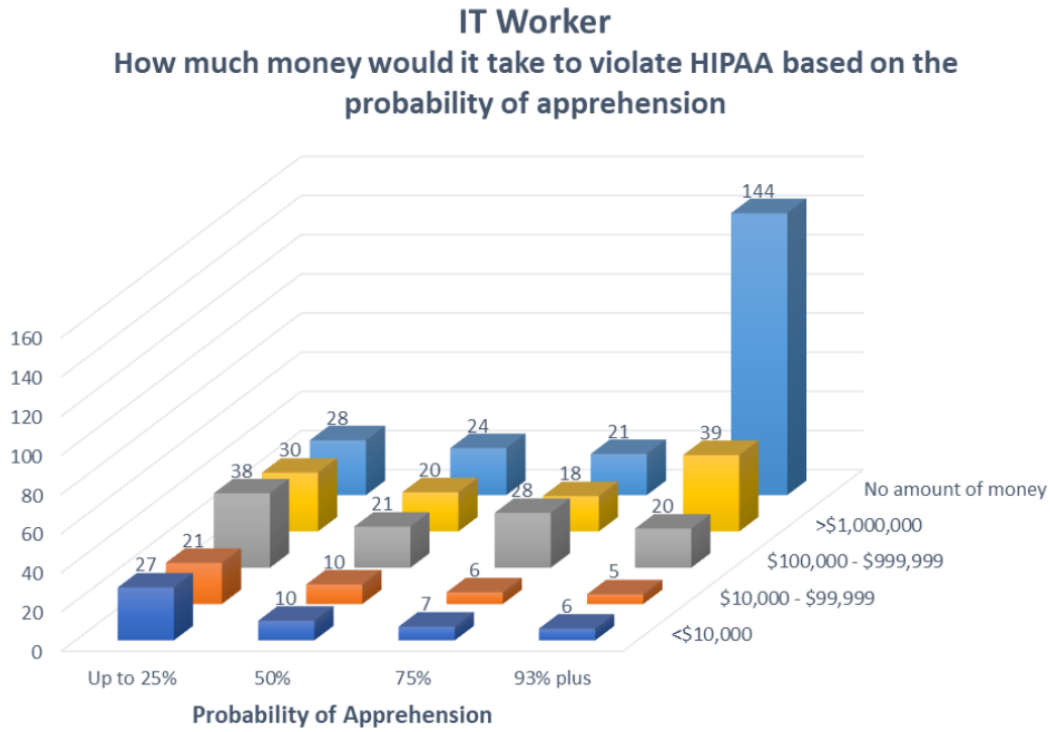


Fig. 5. Increasing amount required with increasing probability perceptions

shape hacker decision-making. Our results demonstrate that individual perceptions of risk and reward and potential gains from illicit cyberactivity influence insider behavior. For example, 58% of the study participants indicated a willingness to violate the policy at sufficiently high monetary levels. The key is to translate our findings into strategies for addressing insider cybersecurity threats. We aligned the results with the theoretical insights and developed a set of guidelines that managers from organizations of various sizes and industries can use to detect, remediate, and prevent insider cybersecurity breaches. They are based on research studies and work conducted with chief security officers. Table III presents the critical strategies that management can use to detect, remediate, and prevent insider threats for organizations of various sizes and industry sectors.

## VII. Conclusion and Future Directions

The research reported in this paper integrates the Capability, Opportunity, Motivation, and Behavior model with deterrence theory, prospect theory, and behavioral economics to understand insider threats. It also uses a unique scenario approach to capture motivations and behaviors related to white-hat, black-hat, and gray-hat hacking. Ultimately, there is always a price, and many can be tempted to cross over to the dark side. A key finding of this study is that approximately 58% (306/523) of the subjects would succumb to monetary incentives and violate privacy laws if the price is right. That price can be high, exceeding 10 million dollars. The right price is a function of their perceptions of the probability of being apprehended. Some of the study participants indicated that, despite the high probability of being caught, they would still engage in private information disclosure. For example, 13% (70/523) of the subjects perceived a 93% probability of getting caught, but would still turn over health information if the price was right.

The skill set that attracts people to white-hat hacking, such as sneaking into buildings, using password trackers, and developing fake websites, will also attract gray-hat and black-hat hackers, provided the proper context is given. They will be attracted to black-hat hacking, such as receiving monetary compensation to pay off debt or buy a new car. In the case of gray-hat hacking, they may be attracted to hacking individuals with different political views, or to punish cyberbullying.

But there are ways to curb black-hat and gray-hat hacking. In the research scenario where an individual is experiencing financial difficulty, they are asked how much money they would require to release health information about a famous patient; people with higher salaries would need more funds to violate HIPAA. For example, individuals receiving $100,000 a year will be less inclined to participate in the violation of HIPAA, and if they do, they would require significantly more money than those paid $30,000. And perceptions of being caught and prosecuted also reduce the tendency to violate privacy laws. The link between white-hat capabilities and black-hat and gray-hat hacking raises concerns about the drift from ethical to unethical hacking. Although technical prowess is central to white-hat roles, it can inadvertently empower morally ambiguous behavior when disinhibition sets in, particularly under low perceived risk. Approximately 58% of the survey participants reported that they could be tempted to violate HIPAA regulations if offered the right monetary

incentive.

Organizations must evaluate their hiring, training, and security practices by applying behavioral economics, such as prospect theory, and the COM-B framework, to enlighten their security practices. In-depth ethics education, fostering and cultivating a culture of psychological ownership, understanding economic pressures on employees, and shifting the organizational climate to prioritize the protection of customer and employee assets should be the key objectives. Without such tectonic shifts, capable insiders can become high-risk actors in the cybersecurity landscape.

We found that individuals receiving higher salaries would be less inclined to violate privacy laws. Individuals interested in white-hat hacking capabilities may be more likely to engage in black-hat hacking. It should be noted that White-Hats are not necessarily more likely to go 'bad', but that they share an interest in understanding concepts of hacking technologies with black-hats. Hacking knowledge can be used for mischief and for good [13].

### A. Education, Training, and Research

Developing security education, training, and awareness is always a challenge. Successful security training approaches use flow theory and facilitate psychological ownership by immersing employees in security training [60]. The goal is to understand the conditions under which professionals are tempted to act unethically and to develop appropriate data security and staff management strategies to meet evolving threats.

The Carnegie Mellon University Software Engineering Institute provided a comprehensive overview of the procedures for addressing insider cybersecurity threats. Table IV presents the best practices. Promoting awareness and education can also discourage people from engaging in cybercrime by highlighting the negative consequences and risks associated with it. Initiatives that promote economic opportunity, social inclusion, cybersecurity literacy, and a more secure digital environment are part of the solution.

Information is, in fact, power. Privacy is not the absence of sharing, but rather the ability to control what is shared and with whom. Being able to selectively share some personal information while safeguarding other data is the gold standard for privacy. However, the risks of exposing personal information and the risks of unintended disclosure of information are not always apparent. Businesses can use such information for price discrimination and to target their products and services. However, bad actors can use personal information for identity theft, for blackmail, and this often leads to financial fraud. Openness is a two-edged sword. This highlights the importance of finding a balance between transparency and the protection of privacy.

Tim Cook has noted the power struggle between the good and the bad actors:

"*Our own information is being weaponized against us with military efficiency. Every day, billions of dollars change hands and countless decisions are made on the basis of our likes and dislikes, our friends and families, our relationships and conversations, our wishes and fears, our hopes and dreams. These scraps of data, each one harmless enough on its own, are carefully assembled, synthesized, traded and sold.* [61]"

Cybersecurity threats are not going away. The number and variety of cyber threats have increased significantly in recent times. This poses a significant challenge for organizational supply chains, regardless of industry or company size. The threats are real and substantial, which require new capabilities, such as knowledge redundancy and simplification of the digital supply chain, to accelerate recovery [62]. In-depth research is needed on the behavioral economics and personality traits of individuals who deliberately and accidentally violate a system. Longitudinal and lab studies must involve new employees, legacy employees, contractors, and business partners. More research is needed on the role of psychological and economic factors that drive insider behavior, including examining the role of financial stress in insider breaches.

AI will continue to be a tool for both white-hat and black-hat hackers. In remote and hybrid work environments, advances in AI and behavioral analytics could improve the real-time detection and prediction of insider risks. Large and small organizations can use powerful analytical tools to design effective cybersecurity systems that mitigate insider threats. Security Information and Event Management (SIEM) systems facilitate detection, analysis, and response to security threats by collecting, correlating, and integrating security event data from several sources [63]. SIEM uses log-in patterns, network traffic, and pattern monitoring to identify suspicious and anomalous behavior in real time. SIEMs are expensive, but they are crucial for addressing insider and outsider threats. Data collection on insider threats is challenging because breaches are often unreported [64]. Cybercriminals are often difficult to convict due to the relative anonymity of cryptocurrency transactions and the significant expenses associated with investigating and prosecuting cybercrimes.

Counteracting insider threats requires robust detection and prevention strategies for small and large organizations [65].

- Detection of new attacks, followed by remediation and prevention of similar breaches in the future, is the standard course of action.
- Prevention of a threat from ever occurring is the ideal path to deal with cybersecurity attacks.

The high-level guidelines for small and large organizations to combat insider threats are very similar. The devil is in the details, in terms of intensity, comprehensiveness, and the technology used to implement the procedures. Security procedures should be documented and frequently reviewed. Training should still be cross-functional and immersive, involving simulations. Cross-functional teams should evaluate the technology to grant access privileges and password development. Existing and potential employees must be assessed for signs of disgruntlement, burnout, and financial stress.

Prevention is the ultimate goal, but it is challenging to achieve. The dynamic interplay between hackers and

organizations is a cat-and-mouse game of evolution. It is characterized by hackers identifying cracks and system deficiencies, and the organization countering with new detection and remediation approaches. Both sides are attempting to learn about the organizational processes and technologies used to protect data and identify any deficiencies. The good guys aim to plug those holes. The bad guys are looking to exploit the holes.

However, there are big ideas for combating cybercrime. The decentralized architecture of the Internet, coupled with cultural resistance to regulation, has undermined traditional deterrence strategies. However, Holt and Steinmentz argue for a large-scale computer crime new deal that will reshape infrastructure while still protecting civil liberties and reducing criminal opportunities online [66].

Research will always be a step behind combating insider threats. We need ongoing comparative studies across industries and cultures to identify unique vulnerabilities and develop mitigation strategies to counter emerging threats.

**Acknowledgment** This research is supported in part by the National Science Foundation under Grant No. DGE-2234945. Usual disclaimers apply.

| Organization Scale | Strategic Imperative | Managerial Guidance |
|---|---|---|
| Multinational/ Global firms | Institutionalize deterrence through formal governance and cross-unit coordination.<br><br>Leverage organizational slack to invest in advanced controls. | Employ a centralized incentive-design framework tied to both financial and non-financial metrics.<br><br>Establish a global insider-threat thought-leadership group to harmonize policy enforcement and share anomaly detection insights across business units.<br><br>Allocate R&D budgets for AI-driven behavioral analytics. |
| Large domestic enterprises | Balance bureaucratic rigor with localized responsiveness.<br><br>Embed economic deterrents in divisional performance systems. | Integrate insider-threat key performance indicators (KPI) into divisional scorecards and executive dashboards.<br><br>Mandate scenario-based simulation exercises semi-annually, incorporating both quantitative and qualitative learning objectives.<br><br>Deploy enterprise Security Information and Event Management (SIEM) platforms augmented with regular managerial review cycles. |
| Midsize firm | Align structured policy with resource constraints.<br><br>Foster a security-aware culture through visible leadership commitment. | Create a dual-reporting "Ethics Officer" role to bridge IT governance and human resources.<br><br>Design tiered economic incentives calibrated to incident severity.<br><br>Adopt modular, cloud-based monitoring solutions and incorporate monthly "learning huddles" to review near-miss events. |
| Small enterprises | Prioritize culture-driven controls over heavy processes.<br><br>Exploit managerial proximity to reinforce norms. | Exploit managerial proximity to reinforce norms.<br><br>Convene regular all-hands forums to discuss ethical scenarios and reinforce contribution to organizational reputation.<br><br>Implement lightweight reward/penalty mechanisms.<br><br>Use low-cost audit tools (e.g., periodic log reviews) embedded into existing operational workflows. |
| Startups & high-growth ventures | Integrate security into innovation pipelines.<br><br>Align incentive structures with rapid iteration and product-market fit goals. | Institute "bug–bounty for employees" schemes, offering equity-linked or milestone-based rewards for vulnerability disclosures.<br><br>Embed brief security-awareness modules within sprint retrospectives to reinforce best practices alongside feature planning.<br><br>Leverage open-source monitoring stacks and integrate security metrics into OKRs and board-level reporting. |

TABLE III
ORGANIZATION STRATEGIES AND MANAGEMENT APPROACHES

**Identifying critical organizational assets.** Focus on safeguarding the most valuable resources. Including customer data, financial data, intellectual property, proprietary and legacy software, employee personal information, and strategic business information such as business plans and critical operational data.

**Formalize procedures to detect and address risks.** What are the potential external threats from hackers, malware, and natural disasters? What are the internal threats: from malicious insiders and the unintentional threats from human errors? What are the third-party risks and vulnerabilities of partners and vendors?

**Identify Vulnerabilities.** Where are the weaknesses in the legacy and new systems and processes that could be exploited?

**Identify the risk levels and likelihood of an attack.** What is the probability of each threat exploiting a vulnerability in terms of high and low probability? Look at historical breach patterns and estimate risks for new systems.

**Prioritize risk moderation, mitigation, and resolution.** Use the information on the impact and likelihood of an attack in terms of high, medium, or low to prioritize resolution.

**Implement technologies and processes to mitigate attacks.** Implement technical solutions and controls like firewalls, encryption, monitoring tools, physical security systems for facilities, and hardware. Install administrative control policies, establish access restriction policies, and develop training programs.

**Continuously monitor and review the threat program.** Evaluate the risk mitigation strategies to determine their effectiveness. Evaluate the threat assessment to determine their effectiveness in protecting the organization.

TABLE IV
BEST PRACTICES FOR COUNTERING INSIDER THREATS

# REFERENCES


[1] K. Theodos and S. Sittig, "Health information privacy laws in the digital age: Hipaa doesn't apply," *Perspectives in health information management*, vol. 18, p. 1l, 2020.

[2] E. Olsen, "Two-thirds of healthcare organizations hit by ransomware in past year: survey." [Online]. Available: https://www.healthcaredive.com/news/healthcare-organizations-ransomware-attack-increase-sophos-survey/728327/

[3] FBI, "Internet Crime Report 2022," 2023. [Online]. Available: https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

[4] J. Curtis and G. Oxburgh, "Understanding cybercrime in 'real world'policing and law enforcement," *The Police Journal*, p. 0032258X221107584, 2022.

[5] S. Weston, "Insider data breaches set to increase due to remote work shift," 10 2020. [Online]. Available: https://www.itpro.co.uk/security/data-breaches/357545/insider-data-breaches-third-2021

[6] T. Dearden, K. Parti, J. Hawdon, and R. Gainey, "Differentiating INSIDER AND OUTSIDER CYBERATTACKS," vol. 48, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s12103-023-09727-7

[7] M. Hill, "Insider threats surge across US CNI as attackers exploit human factors," 2023. [Online]. Available: https://www.csoonline.com/article/3696318/insider-threats-surge-across-us-cni-as-attackers-exploit-human-factors.html

[8] N. C. Suresh, G. L. Sanders, and M. J. Braunscheidel, "Business continuity management for supply chains facing catastrophic events," *IEEE Engineering Management Review*, vol. 48, no. 3, pp. 129–138, 2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9139326/

[9] M. Hijji and G. Alam, "A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions," *Ieee Access*, vol. 9, pp. 7152–7169, 2021. [Online]. Available: ://WOS:000608200600001

[10] B. Pranggono and A. Arabo, "Covid-19 pandemic cybersecurity issues," *Internet Technology Letters*, vol. 4, no. 2, 3 2021. [Online]. Available: ://WOS:000581657700001

[11] G. Culot, F. Fattori, M. Podrecca, and M. Sartor, "Addressing industry 4.0 cybersecurity challenges," *IEEE Engineering Management Review*, vol. 47, no. 3, pp. 79–86, 2019.

[12] E. E. Schultz, "A framework for understanding and predicting insider attacks," *Computers security*, vol. 21, no. 6, pp. 526–531, 2002, publisher: Elsevier.

[13] G. L. Sanders, S. Upadhyaya, and X. Wang, "Inside the insider," *IEEE Engineering Management Review*, vol. 47, no. 2, pp. 84–91, 2019, publisher: IEEE.

[14] M. B. Elayan, "The New World Of Work And Digital Learning: Millennials And Generation Z." *Webology*, vol. 19, no. 2, 2022.

[15] J. Gaia, X. Y. Wang, C. W. Yoo, and G. L. Sanders, "Good News and Bad News About Incentives to Violate the Health Insurance Portability and Accountability Act (HIPAA): Scenario-Based Questionnaire Study," *Jmir Medical Informatics*, vol. 8, no. 7, 7 2020. [Online]. Available: ://WOS:000557459300033

[16] M. Maasberg, X. Zhang, M. Ko, S. R. Miller, and N. L. Beebe, "An Analysis of Motive and Observable Behavioral Indicators Associated With Insider Cyber-Sabotage and Other Attacks," *IEEE Engineering Management Review*, vol. 48, no. 2, pp. 151–165, 2020.

[17] J. D'Arcy, A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research*, vol. 20, no. 1, pp. 79–98, 3 2009. [Online]. Available: ://WOS:000264258200006

[18] R. Paternoster, "Perceptual deterrence theory," in *Deterrence, Choice, and Crime, Volume 23*. Routledge, 2018, pp. 81–106.

[19] M. Siponen, "Toward a theory of passive sanctions in cybersecurity," 2025.

[20] G. S. Becker, "Crime and Punishment - Economic Approach," *Journal of Political Economy*, vol. 76, no. 2, pp. 169–217, 1968. [Online]. Available: ://WOS:A1968ZA37600001

[21] T. A. Loughran, R. Paternoster, A. Chalfin, and T. Wilson, "Can Rational Choice Be Considered a General Theory of Crime? Evidence from Individual-Level Panel Data," *Criminology*, vol. 54, no. 1, pp. 86–112, 2 2016. [Online]. Available: ://WOS:000370446200004

[22] D. S. Nagin, R. M. Solow, and C. Lum, "Deterrence, Criminal Opportunities, and Police," *Criminology*, vol. 53, no. 1, pp. 74–100, 2 2015. [Online]. Available: ://WOS:000349969200004

[23] A. Acquisti, C. Taylor, and L. Wagman, "The Economics of Privacy," *Journal of Economic Literature*, vol. 54, no. 2, pp. 442–492, jun 1 2016. [Online]. Available: http://dx.doi.org/10.1257/jel.54.2.442

[24] G. Tullock, "Does Punishment Deter Crime," *Public Interest*, no. 36, pp. 103–111, 1974. [Online]. Available: ://WOS:A1974T473800005

[25] N. I. o. Justice, "Five Things About Deterrence," 2016. [Online]. Available: https://www.ojp.gov/pdffiles1/nij/247350.pdf

[26] J. T. Pickett, "Using Behavioral Economics to Advance Deterrence Research and Improve Crime Policy: Some Illustrative Experiments," *Crime Delinquency*, vol. 64, no. 12, pp. 1636–1659, 11 2018. [Online]. Available: ://WOS:000446529800006

[27] D. Kahneman and A. Tversky, "Prospect Theory - Analysis of Decision under Risk," *Econometrica*, vol. 47, no. 2, pp. 263–291, 1979. [Online]. Available: ://WOS:A1979GR75700001

[28] A. Tversky and D. Kahneman, "Advances in Prospect-Theory - Cumulative Representation of Uncertainty," *Journal of Risk and Uncertainty*, vol. 5, no. 4, pp. 297–323, 10 1992. [Online]. Available: ://WOS:A1992JV04500001

[29] C. Jolls, C. R. Sunstein, and R. Thaler, "A behavioral approach to law and economics," *Stanford Law Review*, vol. 50, no. 5, pp. 1471–1550, 5 1998. [Online]. Available: ://WOS:000074456000001

[30] R. H. Thaler, "Mental accounting and consumer choice," *Marketing Science*, vol. 27, no. 1, pp. 15–25, 1 2008. [Online]. Available: ://WOS:000253952700006

[31] ——, "Misbehaving: The Making of Behavioral Economics," *International Journal of Applied Behavioral Economics*, vol. 6, no. 1, pp. 77–81, 1 2017. [Online]. Available: ://WOS:000396638000005

[32] A. H. Villacis, J. R. Alwang, and V. Barrera, "Linking risk preferences and risk perceptions of climate change: A prospect theory approach," *Agricultural Economics*, vol. 52, no. 5, pp. 863–877, 9 2021. [Online]. Available: ://WOS:000669594000001

[33] D. B. Reid, *Running the Risk: From Shark Attacks to Nuclear Disaster-understanding life's biggest risks and how we build a safer future*. Legend Press Ltd, 2025.

[34] F. Dablander, M. S. Sachisthal, V. Cologna, N. Strahm, A. Bosshard, N.-M. Grüning, A. J. Green, C. Brick, A. R. Aron, and J. M. Haslbeck, "Climate change engagement of scientists," *Nature Climate Change*, vol. 14, no. 10, pp. 1033–1039, 2024.

[35] E. M. Fischer, S. Sippel, and R. Knutti, "Increasing probability of record-shattering climate extremes," *Nature Climate Change*, vol. 11, no. 8, pp. 689–+, 8 2021. [Online]. Available: ://WOS:000677708500001

[36] G. Marshall, *Don't even think about it : why our brains are wired to ignore climate change*, first u.s. edition. ed. Bloomsbury USA, 2014. [Online]. Available: Table%20of%20contents%20http://bvbr.bib-bvb.de:8991/F?func=service&doc_library=BVB01&local_base=BVB01&doc_number=027596197&line_number=0001&func_code=DB_RECORDS&service_type=MEDIA%20Full%20list%20of%20references%20and%20sources,%20updated%20http://climateconviction.org/refs.html%20http://bvbr.bib-bvb.de:8991/F?func=service&doc_library=BVB01&local_base=BVB01&doc_number=027596197&line_number=0002&func_code=DB_RECORDS&service_type=MEDIA%20Klappentext

[37] S. Michie, M. Johnston, R. West, C. Abraham, W. Hardeman, and C. Wood, "Designing Behavior Change Interventions: The Behaviour Change Wheel and Behavior Change Techniques," *Annals of Behavioral Medicine*, vol. 47, pp. S157–S157, 4 2014. [Online]. Available: ://WOS:000334408300601

[38] S. Michie, M. M. van Stralen, and R. West, "The behaviour change wheel: A new method for characterising and designing behaviour change interventions," *Implementation Science*, vol. 6, 4 2011. [Online]. Available: ://WOS:000290665400001

[39] R. van der Klerj, R. Wijn, and T. Hof, "An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations," *Computers Security*, vol. 97, 10 2020. [Online]. Available: ://WOS:000567774600001

[40] S. K. Srivastava, S. Das, G. J. Udo, and K. Bagchi, "Determinants of cybercrime originating within a nation: a cross-country study," *Journal of Global Information Technology Management*, vol. 23, no. 2, pp. 112–137, 2020.

[41] D. Harkin and C. Whelan, "Perceptions of police training needs in cyber-crime," *International Journal of Police Science Management*, vol. 24, no. 1, pp. 66–76, 2022. [Online]. Available: https://journals.sagepub.com/doi/abs/10.1177/14613557211036565

[42] Z. Xu, Q. Hu, and C. Zhang, "Why computer talents become computer hackers," *Communications of the ACM*, vol. 56, no. 4, pp. 64–74, 2013. [Online]. Available: http://dx.doi.org/10.1145/2436256.2436272

[43] S. D. Levitt, "The Economics of Crime," *Journal of Political Economy*, vol. 125, no. 6, pp. 1920–1925, 12 2017. [Online]. Available: ://WOS:000417579700028

[44] J. Gaia, B. Ramamurthy, L. Sanders, S. Sanders, S. Upadhyaya, X. Wang, and C. Yoo, "Psychological profiling of hacking potential," in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020.

[45] F. Brühlmann, S. Petralito, L. F. Aeschbach, and K. Opwis, "The quality of data collected online: An investigation of careless responding in a crowdsourced sample," *Methods in Psychology*, vol. 2, p. 100022, 2020. [Online]. Available: http://dx.doi.org/10.1016/j.metip.2020.100022

[46] F. Exadaktylos, A. M. Espín, and P. Branas-Garza, "Experimental subjects are not different," *Scientific reports*, vol. 3, no. 1, p. 1213, 2013, publisher: Nature Publishing Group UK London.

[47] Y. Akbulut, A. Donmez, and O. O. Dursun, "Cyberloafing and social desirability bias among students and employees," *Computers in Human Behavior*, vol. 72, pp. 87–95, 7 2017. [Online]. Available: ://WOS:000401395200009

[48] D. Dodou and J. C. F. de Winter, "Social desirability is the same in offline, online, and paper surveys: A meta-analysis," *Computers in Human Behavior*, vol. 36, pp. 487–495, 7 2014. [Online]. Available: ://WOS:000338387300054

[49] J.-H. Cheah, F. Magno, and F. Cassia, "Reviewing the smartpls 4 software: the latest features and enhancements," 2024.

[50] C. E. Werts, R. L. Linn, and K. G. Joreskog, "Intraclass Reliability Estimates - Testing Structural Assumptions," *Educational and Psychological Measurement*, vol. 34, no. 1, pp. 25–33, 1974. [Online]. Available: ://WOS:A1974S613600004

[51] J. Cohen, "A Power Primer," *Psychological Bulletin*, vol. 112, no. 1, pp. 155–159, 7 1992. [Online]. Available: ://WOS:A1992JB40500008

[52] N. Bilton, *American kingpin : the epic hunt for the criminal mastermind behind the Silk Road*. Portfolio/Penguin, 2017.

[53] S. E. Freed, "Examination of personality characteristics among cybersecurity and information technology professionals," 2014.

[54] R. Madarie, "Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers." *International Journal of Cyber Criminology*, vol. 11, no. 1, 2017. [Online]. Available: https://zenodo.org/record/495773

[55] P. K. Jonason and G. D. Webster, "The dirty dozen: a concise measure of the dark triad." *Psychological assessment*, vol. 22, no. 2, p. 420, 2010. [Online]. Available: http://dx.doi.org/10.1037/a0019265

[56] D. N. Jones and D. L. Paulhus, "Duplicity among the dark triad: Three faces of deceit." *Journal of personality and social psychology*, vol. 113, no. 2, p. 329, 2017.

[57] D. L. Paulhus and K. M. Williams, "The dark triad of personality: Narcissism, Machiavellianism, and psychopathy," *Journal of research in personality*, vol. 36, no. 6, pp. 556–563, 2002.

[58] M. Maasberg, J. Warren, and N. L. Beebe, "The Dark Side of the Insider: Detecting the Insider Threat through Examination of Dark Triad Personality Traits," in *2015 48th Hawaii International Conference on System Sciences*. IEEE, 1 2015, pp. 3518–3526. [Online]. Available: http://dx.doi.org/10.1109/HICSS.2015.423

[59] J. Gaia, D. Murray, G. Sanders, S. Sanders, S. Upadhyaya, X. Wang, and C. Yoo, "The interaction of dark traits with the perceptions of apprehension," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2022.

[60] C. W. Yoo, G. L. Sanders, and R. P. Cerveny, "Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance," *Decision Support Systems*, vol. 108, pp. 107–118, 4 2018, [Online; accessed 2023-06-15]. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167923618300381

[61] T. Cook, "Keynote address from Tim Cook, CEO, Apple Inc," https://www.youtube.com/watch?v=kVhOLkIs20A, YouTube. [Online]. Available: https://www.youtube.com/watch?v=kVhOLkIs20A

[62] R. Pergande, J. Hamann-Lohmer, and R. Lasch, "From attack to adaptation: A case study of capabilities driving digital supply chain recovery," *IEEE Engineering Management Review*, 2025.

[63] J. M. López Velásquez, S. M. Martínez Monterrubio, L. E. Sánchez Crespo, and D. Garcia Rosado, "Systematic review of siem technology: Siem-sc birth," *International Journal of Information Security*, vol. 22, no. 3, pp. 691–711, 2023.

[64] X. Li and A. B. Whinston, "The economics of cyber crime," *Available at SSRN 3603694*, 2020. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3603694

[65] R. A. Alsowail and T. Al-Shehari, "Techniques and countermeasures for preventing insider threats," *PeerJ Computer Science*, vol. 8, p. e938, 2022.

[66] T. J. Holt and K. F. Steinmetz, "Rethinking cybercrime prevention in the age of the internet," *Crime, Law and Social Change*, vol. 83, no. 1, pp. 1–17, 2025.

[67] J. Flood, M. Denihan, A. Keane, and F. Mtenzi, "Black Hat Training of White Hat Resources: The Future of Security is Gaming," *2012 International Conference for Internet Technology and Secured Transactions*, pp. 488–491, 2012. [Online]. Available: ://WOS:000317120000077

[68] Gaia, "Dark Traits and Hacking Potential," *Journal of Organizational Psychology*, vol. 21(3), 2021.

[69] J. Gaia, X. Y. Wang, C. W. Yoo, and G. L. Sanders, "Good News and Bad News About Incentives to Violate the Health Insurance Portability and Accountability Act (HIPAA): Scenario-Based Questionnaire Study (vol 8, e15880, 2020)," *Jmir Medical Informatics*, vol. 8, no. 9, 9 2020. [Online]. Available: ://WOS:000577388800018

[70] R. D. Gopal and G. L. Sanders, "International software piracy: Analysis of key issues and impacts," *Information Systems Research*, vol. 9, no. 4, pp. 380–397, 12 1998. [Online]. Available: ://WOS:000078525800007

[71] S. D. Krit and E. Haimoud, "Review On The IT Security Attack And Defense," *2016 International Conference on Engineering Mis (Icemis)*, 2016. [Online]. Available: ://WOS:000391535300095

[72] S. L. Myers, "Estimating the Economic-Model of Crime - Employment Versus Punishment Effects," *Quarterly Journal of Economics*, vol. 98, no. 1, pp. 157–166, 1983. [Online]. Available: ://WOS:A1983QD21300009

[73] C. C. Palmer, "Ethical hacking," *Ibm Systems Journal*, vol. 40, no. 3, pp. 769–780, 2001. [Online]. Available: ://WOS:000170634500010

[74] A. Tversky and D. Kahneman, "The Framing of Decisions and the Psychology of Choice," *Science*, vol. 211, no. 4481, pp. 453–458, 1981. [Online]. Available: ://WOS:A1981KZ36500009


## APPENDIX

**Seven item scales ranging from Strongly disagree to Strongly agree**

## WHITE HAT, BLACK HAT, AND GRAY HAT QUESTIONER ITEMS

### White Hat Items

For the following questions, assume that you would be working for a government agency and that you would not be prosecuted for participating in these activities. Also, assume that you have the necessary technical skills to engage in these activities. Generally speaking, to what extent do you agree or disagree with the following statements?

**Cronbach's Alpha = 0.971**

- I would like to observe a person's behavioral patterns over a week and use that as a way to obtain their personal information.
- I would like to use manipulative emails to obtain private information or install malware on computers.
- I would like to sneak into buildings using a lock pick, by following someone else or by using an electronic device to counter the lock system.
- I would like to use password crackers to break into computer accounts.
- I would like to set up a website that looks like a real website to trick people to enter their personal information.
- I would like to be able to capture information that people use in wireless networks.

### Black Hat Items

For the following questions, assume that you would not get caught for participating in the following activities and that you have the necessary technical skills to engage in these activities. Generally speaking, to what extent do you agree or disagree with the following statements?

**Cronbach's Alpha = 0.917**

- I could see myself engaging in hacking attacks if I needed money to purchase a $400,000 house that for my family.
- I could see myself engaging in hacking attacks if I needed money to purchase a new $60,000 car that I could not afford.
- I could see myself engaging in hacking attacks if I needed money to pay off a credit card debt that had reached $100,000 and I was just fired from my job.

**Gray Hat Items**

For the following questions, assume that you would not get caught for participating in the following activities and that you have the necessary technical skills to engage in these activities. Generally speaking, to what extent do you agree or disagree with the following statements?

**Cronbach's Alpha = 0.941**

- I could see myself engaging in hacking attacks against a company that was supporting a political candidate that I did not like.
- I could see myself engaging in hacking attacks against a twitter account of a person that had extreme views that I did not believe in.
- I could see myself engaging in hacking attacks against a government agency that was engaging in an activity that I felt was wrong.
- I could see myself engaging in hacking attacks against an individual that was bullying me during an online game.

## SCENARIO

**Used to capture amount of money need to violate HIPAA and probability of being apprehended**

Suppose you are a computer technical support specialist at a hospital, and you earn ($30,000, $55,000, $100,000) per year. However, you are currently experiencing financial difficulty. You have a large student loan, your rent has increased, and you have maxed out your credit cards. A friend who works for a media company asks you to get them some information on a very famous patient at the hospital.

What amount of money would you receive to make this acceptable?

- They could have the information for free
- Less than $999
- $1,000 - $4,999
- $5,000 - $9,999
- $10,000 - $49,999
- $50,000 - $99,999
- $100,000 - $249,999
- $250,000 - $499,999
- $500,000 - $999,999
- $1 M - $10 Million
- Over $10 Million
- I would not reveal personal information for any amount of money

What do you think is the likelihood of getting caught, if you accept the money?

- Extremely unlikely (0%)
- Moderately unlikely (7%)
- Slightly unlikely (25%)
- Neither likely nor unlikely (50%)
- Slightly likely (75%)
- Moderately likely (93%)
- Extremely likely (100%)

## BIOGRAPHY

**Laura Amo** is an associate professor at the State University at Buffalo. Her research interests include deviant technology behavior, cybersecurity education, AI trust and signaling, educational information systems, and online information search on community-based platforms. Dr. Amo has published in outlets such as MIS Quarterly, European Journal of Information Systems, Educational Psychology Review, Journal of Medical Internet Research, and IEEE Transactions on Education. She has received over $1 million in funding from the National Science Foundation, the National Security Agency, and the Spencer Foundation.

**Joana Gaia** has investigated the psychology of hackers, as well as how privacy concerns can impact an individual's smartphone use or willingness to share personal health information. Additionally, she has expertise in multi-agency collaboration during emergency management situations. She is also the Co-founder of Girl Tech Day, where students discuss the importance of introducing kids to coding and other STEM concepts at a young age.

**David Murray** is a Clinical Professor of Management Science and Systems and serves as the Associate Dean for Undergraduate Programs in the School of Management at the State University of New York at Buffalo. Throughout his career, he has taught a wide range of technology and business courses to thousands of undergraduate and graduate students. Since 2004, he has conducted dozens of cybersecurity outreach workshops for local middle school and high school students, adult learners, business owners, and the general public. The National Science Foundation and the National Security Agency have supported his prior research and projects.

**G. Lawrence Sanders** research interests include profiling hacking behavior, the ethics and economics of digital piracy, privacy and security, game design and addiction, gamification, database design, systems success measurement, and virtual worlds. He is a co-Principal Investigator on $5.79 million in grants from the National Science Foundation to train future cybersecurity experts. He has been actively involved in developing academic programs at the undergraduate, master's, and doctoral levels.

**Sean Sanders** is an Assistant cybersecurity professor at Illinois State University in the School of Information Technology. His primary research interests include the implications and applications of blockchain in cybersecurity, compiler frameworks for malware detection, and the psychological profiling of hackers. His work also explores mobile malvertising detection and the role of dark traits and economic incentives in hacking behavior. He has authored and coauthored several publications in refereed journals and conferences.

**Raghvendra Singh** is a Ph.D. candidate in Management Science & Systems at the University at Buffalo (SUNY), with an M.S. in MIS from the same university. His research focuses on information security leadership, security & privacy, healthcare IT, and AI. He has published in top IS journals, co-edited books on security and auditing, and presents at major IS conferences. He teaches cybersecurity, privacy and ethics, and statistical decision-making. His service includes reviewing for IS outlets, leadership with AIS Doctoral Student College and MISQ Insider, and collaboration with STEP at University of Memphis. He previously worked 4+ years in industry as a Product Manager and Consultant, and served in the Indian Army. He holds certifications in information security, machine learning, and AI.

**Shambhu Upadhyaya** is a Professor of Computer Science and Engineering at the State University of New York at Buffalo, where he also directs the Center of Excellence in Information Systems Assurance Research and Education (CEISARE), designated by the National Security Agency. Prior to July 1998, he was a faculty member at the Electrical and Computer Engineering department. His research interests span broad areas, including information assurance, computer security, behavioral biometrics authentication, and fault-tolerant computing. He has authored or coauthored more than 300 articles in refereed journals and conferences in these areas. His research has been supported by the National Science Foundation, U.S. Air Force Research Laboratory, the U.S. Air Force Office of Scientific Research, DARPA, and National Security Agency. He is a Fellow of the IEEE.