Economic Incentives and Perceptions as Critical Factors for Understanding Insider Hacking Behavior

Laura Amo
University at Buffalo
lccasey@buffalo.edu

Joana Gaia
University at Buffalo
joanaalu@buffalo.edu

David Murray
University at Buffalo
djmurray@buffalo.edu

G. Lawrence Sanders
University at Buffalo
mgtsand@buffalo.edu

Sean Sanders
University at Buffalo
spsander@buffalo.edu

Raghvendra Singh
University at Buffalo
rsingh45@buffalo.edu

Shambhu Upadhyaya
University at Buffalo
shambhu@buffalo.edu

Abstract

The objective of this research is to investigate the influence of interest in white hat capabilities, income levels, and perceptions of being apprehended on the willingness to violate privacy regulations as measured by the amount of money required to violate medical privacy. The research model was developed by drawing on the economics of crime literature, prospect theory and the emerging Capability, Opportunity, and Motivation Behavior model. This study involved 523 individuals on the cusp of entering the workforce, which places them all as potential insider hackers according to zero trust models of insider behavior. Despite many subjects believing there is a high probability of being caught, they could still be incentivized to violate HIPAA laws. Approximately 306 (or 58%) of the survey participants indicated a price, ranging from zero dollars to over $10 million, that they deemed acceptable for violating 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

1. Introduction

According to the FBI's Internet Crime Report, the U.S. experienced an unprecedented increase in cyber-attacks and malicious activity in 2022, when losses were more than $10.3 billion (FBI, 2023). Cybercrime is not just a U.S. problem, as security breaches worldwide are growing (Curtis and Oxburgh, 2022). 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 (Weston, 2020). Over three-quarters of organizations involving critical national infrastructure (CNI) have seen a rise in insider-driven cyber threats in the last three years (Hill, 2023). Threats are attributable to negligence, human error, and criminal intent and are exacerbated by reductions in cybersecurity budgets and the financial stress of employees brought on by inflation and the economic downturn (Hijji and Alam, 2021; Pranggono and Arabo, 2021).

Cybercrime requires both technical expertise and extensive training to be carried out effectively (Harkin and Whelan, 2022). The net effect is that an ensemble of cybersecurity specialists is required to implement the ever-popular social engineering and spear phishing approaches. Insiders are particularly problematic when they have technical skills because they understand the inner workings of organizational processes and can disrupt such 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 deal with this issue, but in the interest of specialization and productivity, this is rarely embraced as a mechanism to increase security.

2. Backround and Related Work

2.1. Capabilities, Motives and Opportunities

URI: https://hdl.handle.net/10125/106773
978-0-9981331-7-1

We use several theories to understand why insider attacks occur and lead to hacking behavior. The first theory we draw on to conceptualize insider attacks is the classical Capability, Motive, and Opportunity (CMO) model. In the CMO model, the perpetrator must have the capabilities to attack, the motive for attacking, and the opportunity to violate a security law (Sanders et al., 2019; Schultz, 2002)

Solid technical skills are in abundance in Millenials and Generation Z. Even insiders with weak skills can leverage their organizational knowledge by utilizing the abundance of online information on hacking. They can also turn to the Darknet and Deep Web to purchase hacking expertise (Sanders et al., 2019). And, of course, motives to hack are readily available, and they are usually related to financial difficulties, like credit card debt, student loans, and health insurance premiums. However, there are instances where a disgruntled employee is disappointed with a supervisor who has passed them over for a raise turns to hacking. Finally, opportunities are not in short supply. After an employee has worked in a job for several months, the employee acquires a deep knowledge of their job's inner workings and the flaws of organizational systems.

2.2. Deterrence Theory

Deterrence aims to use threats and sanctions to inhibit criminal behavior (D'Arcy et al., 2009). The idea is that high probabilities of arrest and conviction and adequate punishment levels will deter criminal behavior.

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 (Becker, 1968; Loughran et al., 2016). 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, where the certainty of being apprehended is the most effective treatment (Nagin et al., 2015). An individual will consider committing a cybercrime when the net expected gains from illegal activity are greater than the utility of engaging in legal work (Figure 1) The p term is the perception of the probability of being apprehended 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.

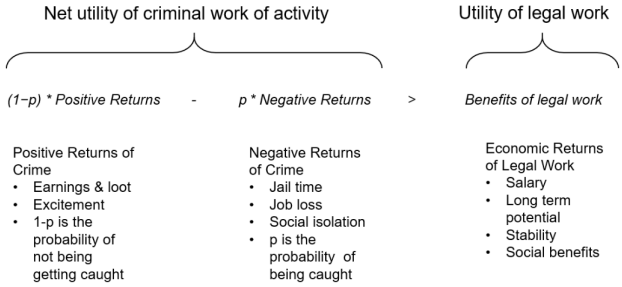

Figure 1. Becker crime utility model (adapted)

Maintaining a high level of deterrence is expensive. The goal of the police and the 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 try and manipulate the perceived likelihood of apprehension and reduce enforcement costs.

2.3. Severity of Punishment

There has always been disagreement on the relationship between the severity of punishment and deterrence. For example: Suppose there is a one in a hundred probability of being convicted for one year or a one in a thousand probability of being convicted for ten years. In both instances, the expected negative returns of engaging in criminal activity lead to the same result (Tullock, 1974). The National Institute of Justice (NIJ), examined research by Nagin, 2013 on the role of lengthy and mandatory prison sentences in deterring (Justice, 2016). The NIJ considers long and mandatory sentences expensive and ineffective in preventing crime and deliberates the perceptions of being caught and punished as the key to deterrence.

This is supported by prospect theory, because people are more risk averse to the possibility of a loss than the prospect of an equivalent gain in order to avoid the negative consequences (Tversky and Kahneman, 1981). Pickett has found experimental evidence that pseudocertainty publicity can increase the perceived arrest risk of arrest and increase deterrent fear, but also that increasing sanctions has a declining impact on deterrence (Pickett, 2018).

2.4. Prospect Theory

Prospect theory is a powerful tool for understanding how individuals make choices and choose paths when there are risky outcomes and was initially developed by Kahneman and Tversky (Kahneman and Tversky,

1979; Tversky and Kahneman, 1992). It was further enhanced by Thaler (Jolls et al., 1998; Thaler, 2008, 2017). Prospect theory posits that risk preferences are a function of risk aversion and loss aversion and that people are more averse to situations with potential losses (Villacis et al., 2021). The decision-maker uses utility-based calculus involving probabilities and a weighting function to examine possible outcomes.

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 stay away from the ocean. On the other hand, even though there is a high probability of record-shattering climate change (Fischer et al., 2021), cognitive biases, mental maps, and the yearning for normality and safety lead many to underestimate the potential impact on society (Marshall, 2014). The key is that perceived differences are a function of individual perceptions, and perceived differences are relative to the personal situation or context.

Prospect theory provides insight and justification for using different income levels to test the influence of personal income on the potential to engage in illegal activity. We will examine the role of increasing monetary incentives on insiders' deviant behavior decisions using a scenario where salaries are $30,000, $55,000, and $100,000. We will investigate if individuals with higher incomes are less inclined to violate privacy laws and demand more money to release health information.

2.5. Integrating Behavioral Economic Theory and the CMO-B framework

The Capability, Opportunity, and Motivation Behavior model (CMO-B) is a comprehensive model for understanding the dynamic process guiding human behavior (Michie et al., 2014, 2011). A capability in the context of cybersecurity involves having the psychological capacity, the technical and social engineering skills, and an interest in hacking activity (van der Klerj et al., 2020). An opportunity involves the occasion to participate in legal or illegal behavior. Motivation involves cognitive processes that direct behavior and an analytical decision-making process that integrates the positive and negative consequences of pursuing a behavior.

The CMO-B model was developed by integrating well-known behavioral theories and U.S. criminal law theory and proves relevant to the economics of crime literature. U.S. criminal law requires that to prove that one is guilty, the person should 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 (Michie et al., 2011). The CMO-B model complements and supports behavioral economics research and amplifies our understanding of illegal security behavior. Figure 2 illustrates how the model integrates with the constructs and items used in this project.

3. Research Hypotheses

As noted earlier, subjects use a decision calculus to determine if 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 (Becker, 1968; Loughran et al., 2016). Certainty of punishment also involves a calculus of the perceived probability of apprehension, the likelihood of being charged, the probability of conviction, and the probability of formal sanctions. It has been postulated that the certainty of being apprehended is the most effective treatment for curbing crime (Nagin et al., 2015). Individuals act differently and can be deterred if there is a high likelihood of punishment, and the penalty is severe (Myers, 1983). The market model assumes that offenders are rational economic actors with expectations about the expected returns, the propensity for being caught, and the resulting punishment (Gaia et al., 2022, 2020a; Myers, 1983). The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects sensitive patient health information from being illegally disclosed. As such, we posit that higher-salary individuals will require greater returns, or more money, to violate a HIPAA law.

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.

In the Becker model (Becker, 1968), individuals use a rational calculus, weighing the costs against the benefits of engaging in illicit behavior to maximize their self-interests in the context of their current income (Robinson, 1993). 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 receiving lower wages.

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

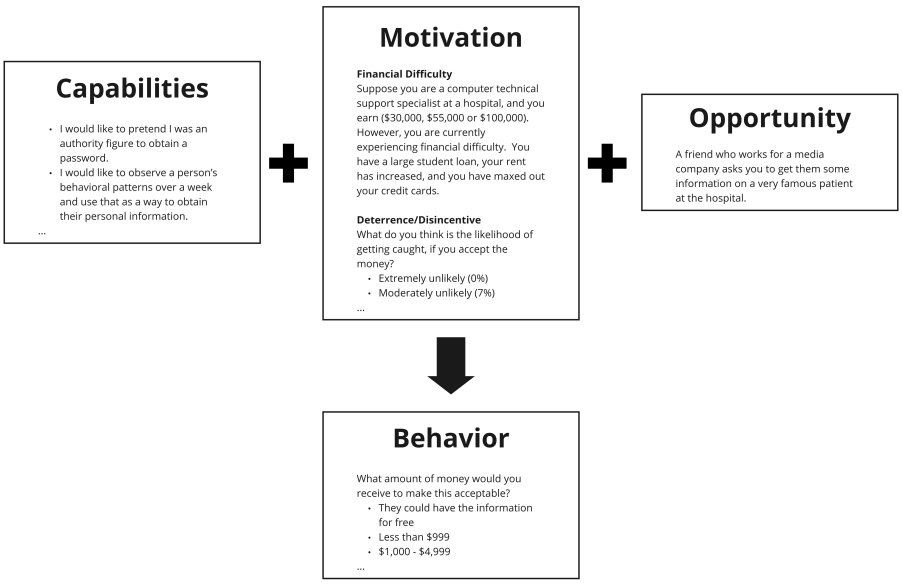

Figure 2. The Capability, Motivation, and Opportunity Behavior Model CMO-B Model

We know from past research that white hat hacking can lead to an interest in any type of hacking (Flood et al., 2012; Gaia, 2021). The goal was to validate earlier work that found a statistically significant relationship between the interest in white and black hat hacking.

White hat hackers are ethical hackers (Palmer, 2001) and assist system owners in detecting and fixing security system vulnerabilities. White hats do not violate laws, even though many use the same tools as black hat hackers. Black hat hackers, or crackers, are typically motivated by personal gains, including financial gains, from illegally breaching computer systems (Krit and Haimoud, 2016). However, they can be social mischief-makers seeking thrills, revenge, and notoriety. The key question is whether white hat hacking can contribute to illegal hacking. A famous example of this drift to the dark side can be found in American Kingpin (Bilton, 2017). One of the government agents investigating Ross Ulbricht became enamored with excitement and monetary attraction and eventually was lured into committing criminal activities. We, therefore, sought to validate previous findings related to whether white hat hackers might drift towards being black hat hacking. This leads to hypotheses H2 and H3.

H2: Higher interest in White hat hacking **capabilities** is positively related to **lower** requirements for monetary incentives in the HIPAA scenario.

The capabilities of the individual are comprised of the expertise and the interest in using those capabilities involving a cybercrime. The opportunity involves access to a situation where the crime can be executed, such as black hat activities. The net effect is that the decision to commit the crime involves a decisional calculus involving three components, the capabilities, the motivation, and the opportunity. This leads to the following hypothesis.

H3: 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.

The final hypothesis relates to the probability of being apprehended. Previous research has shown that the market model for crime engages in assumes that offenders, victims, and law enforcement engage in optimizing behaviors related to preferences and that offenders have expectations about returns and individual sensitivity for being caught and the resulting punishment (Gaia et al., 2020a; Levitt, 2017). Thus, we include a construct to validate that the probability of being apprehended influences how much money is 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.

4. Methodology

The scales and loadings used in this study can be viewed at GitHub![1] and in the Appendix. The scenario was adapted from a study that identified the role of monetary incentives in violating HIPAA regulations and privacy laws (Gaia et al., 2020a). We created one scenario and randomly assigned each subject to salary levels of $30,000, $55,000, and $100,000. Here is the scenario.

"Suppose you are a computer technical support specialist at a hospital, and you earn $60,000 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."

The validated interest in white hat hacking and the black hat scales were from (Gaia, 2020). The white hat scale measures the attraction to technical and social engineering hacking behaviors. The items are **capabilities** of interest in the context of the CMO-B model. The subjects completing the scale are told they would work for a government agency and would not be prosecuted for participating in white hat activities. The three black hat items involve financial attacks motivated by personal gains for breaching computer systems. These are the monetary incentives to engage in black hat hacking behavior. These activities are typically illegal.

We recruited 593 subjects from sophomore, junior and senior undergraduates enrolled in management information systems and a data analytics class to take 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 removed 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. 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 non-students (Exadaktylos et al., 2013). 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 being studied work environments are reluctant to answer questions truthfully because they do not want to diminish their social prestige (Akbulut et al., 2017; Dodou and de Winter, 2014).

[1]GitHub: https://anonymous.4open.science/r/HICSS_2023-BC49/README.md

5. Model and Hypotheses Assessment

We examined individual loadings and internal consistency to test for item reliability. Loadings for all measurement items were above 0.7. Cronbach's alpha for every construct was greater than 0.7, indicating internal reliability (Werts et al., 1974). Next, we assessed discriminant validity using the Average Variance Extracted (AVE). The square root of the AVE should be higher than the correlations among the constructs. All of the hypotheses were analyzed using SmartPLS 4.1 and the p-values were deemed significant examined at the .05 level. One criterion for evaluating PLS path models is the coefficient of determination (r^2). According to Cohen (Cohen, 1992), 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 3 presents the overall model results for the analysis. The p-values follow the path coefficients on the connecting lines. The r^2 for the money required was 0.240. The r^2 for the black hat hacking was 0.393. All of the hypotheses were supported. The results of the hypotheses tests are presented in Table 1 below.

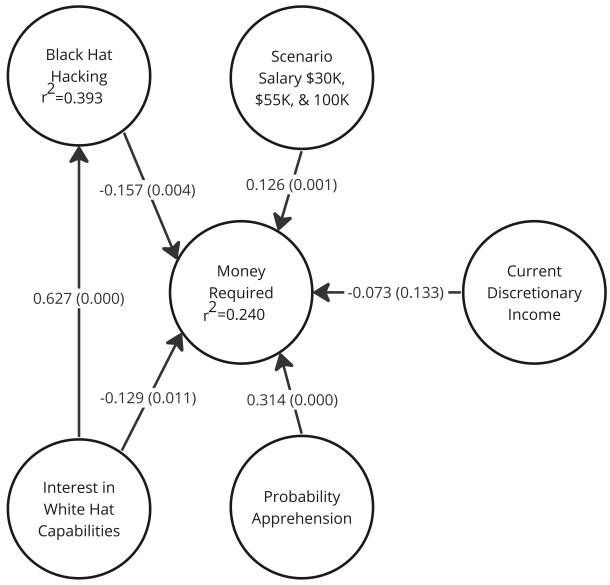

Figure 3. Model Results

Table 1. 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	0.129	0.011	Yes
H3: 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.	0.627	0.000	Yes
H4: Higher perceptions of the probability of apprehension are positively related to higher requirements for monetary incentives to violate HIPAA.	0.314	0.000	Yes

6. Discussion

Data is a precious asset that organizations want to protect, but the breach of health and personal information has severe organizational consequences. Our analysis of the survey data unveils an intricate relationship between the 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 required for an individual to violate HIPAA laws. Higher-income levels are positively related to higher requirements for monetary incentives, with a path coefficient of .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 conducted 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 (e.g., Less than $999, $1,000 - $4,999). To get a feel for the magnitude of the differences, we calculated a midpoint for each category and then used the midpoint calculation for the amount required to violate the HIPAA law. We then ran 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 $2,847,510 and for the $100,000 salary 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. The subjects were thus able to project themselves into the scenario. They require more money if there is more income to lose. They are more sensitive to greater losses of income, which supports the economics of crime literature, rational choice theory, and prospect theory.

Table 2 and Figure 4 present some of the descriptive statistics of the study. Here are some of the takeaways from the results.

- Ten percent of the subjects were willing to release their health information for less than $10,000. And over half of this group perceive the risk of being caught to be as low as 25%. This category represents an immediate potential threat to companies.
- The 42 subjects ($\sim$ 8%) in the $10,000 - $99,999 bracket are hesitant as the perceived risk rises.
- On the extreme end of the price spectrum are the 107 subjects ($\sim$ 20%) willing to sell data for amounts exceeding $1,000,000. A substantial portion of this group perceives a high probability of being apprehended. Implying they require significant financial rewards to justify the high risk.

The good news is that 41% of respondents wouldn't sell data under any circumstances. Most of these individuals perceive a high chance (93% plus) of being caught, suggesting they are well aware of the risks associated with such actions and perhaps have ethical mores. Finally, individuals that are interested in white hat hacking, which is legal, are susceptible to drift. White hat hacking interest could lead to black hat hacking activity. As noted, a drift to the dark side can be found in the American Kingpin (Bilton, 2017) story. The government agent investigating the darknet market website Silk Road, developed by Ross Ulbricht, was lured to the criminal side because of the monetary attraction.

7. Conclusion

There is a correlation between the perceived risk of apprehension and the amount of money required to sell data, with a decrease in willingness as the perceived risk increases. Many subjects demanded high sums to counterbalance the high risk involved. Our study underscores the importance of companies investing in robust data security measures and fostering a culture of ethical responsibility among I.T. staff. Effective

Table 2. Relationship between Incentives and Apprehension

IT Worker		Perceived probability of being apprehended					
		Up to 25%	50%	75%	93% plus	Total	Percentage
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%	

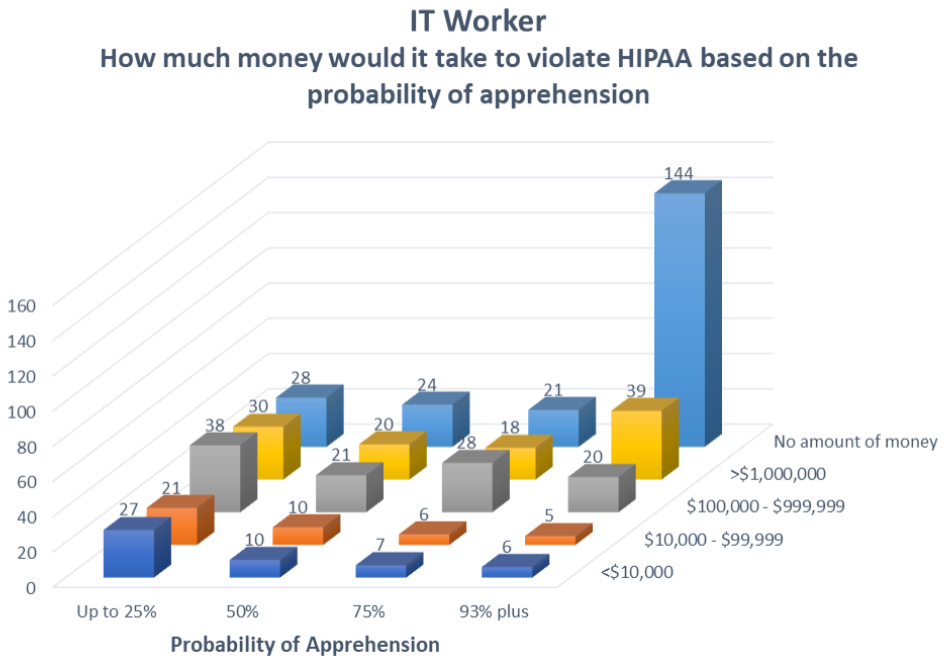

Figure 4. Increasing amount required with increasing probability perceptions

deterrence mechanisms, which increase the perceived risk of being caught, can significantly prevent data breaches.

The findings of this study are that approximately 58.50% (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 even though there was a high probability of being caught, they would still engage in turning over private information. For example, 13.38% (70/523) of the subjects perceived a 93% probability of getting caught, but they would still turn over the health information if the price was right. We did find that individuals receiving higher salaries would be less inclined to violate privacy laws. And those individuals interested in white hat hacking capabilities could be prone to engaging 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 hacking technologies concepts with black hats. Hacking knowledge can be used for mischief and for good (Sanders, Upadhyaya and Wang, 2019)

Organizations can use preventive controls to impede criminal behavior by forcing the perpetrator to deplete resources (Gopal and Sanders, 1998). Preventive controls include sophisticated monitoring technologies and constant attention to authentication protocols to prevent unauthorized access to buildings, software, and databases. Organizations often turn to preventives because they are under the organization's control. Deterrent strategies focus on the apprehension and punishment of wrongdoers, but they also involve education, legal campaigns, and sometimes fear appeals. 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 (Yoo et al., 2018). The goal is to understand the conditions where professionals are tempted to behave unethically and develop suitable data security and staff management strategies to meet the evolving threats.

Cybersecurity threats are not going away. There is a need for in-depth research 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. IBM estimates that data breaches initiated by malicious insiders are the costliest at $4.90 million and 9.5% higher than the $4.45 million cost of the typical data breach (IBM). Research and improved management practices are the key to reducing the impact.

Acknowledgement This material is based upon work supported by the NSF under Grant No. DGE-1754085.

References

Akbulut, Y., Donmez, A., and Dursun, O. O. (2017). Cyberloafing and social desirability bias among students and employees. 72:87–95.

Becker, G. S. (1968). Crime and punishment - economic approach. 76(2):169–217.

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

Cohen, J. (1992). A power primer. 112(1):155–159.

Curtis, J. and Oxburgh, G. (2022). Understanding cybercrime in 'real world'policing and law enforcement. page 0032258X221107584.

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. 20(1):79–98.

Dodou, D. and de Winter, J. C. F. (2014). Social desirability is the same in offline, online, and paper surveys: A meta-analysis. 36:487–495.

Exadaktylos, F., Espín, A. M., and Branas-Garza, P. (2013). Experimental subjects are not different. *Scientific reports*, 3(1):1213.

FBI (2023). Internet crime report 2022. https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics.

Fischer, E. M., Sippel, S., and Knutti, R. (2021). Increasing probability of record-shattering climate extremes. 11(8):689–+.

Flood, J., Denihan, M., Keane, A., and Mtenzi, F. (2012). Black hat training of white hat resources: The future of security is gaming. pages 488–491.

Gaia, Ramamurthy, B. S. G. S. S. U. S. W. X. Y. C. J. (2020). Psychological profiling of hacking potential. volume Proceedings of the 53rd Hawaii International Conference on System Sciences.

Gaia, Sanders, G. L. S. S. P. U. S. W. X. \. Y. C. W. J. (2021). Dark traits and hacking potential. 21(3).

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

Gaia, J., Wang, X. Y., Yoo, C. W., and Sanders, G. L. (2020a). Good news and bad news about incentives to violate the health insurance portability and accountability act (HIPAA): Scenario-based questionnaire study. 8(7).

Gaia, J., Wang, X. Y., Yoo, C. W., and Sanders, G. L. (2020b). 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). 8(9).

Gopal, R. D. and Sanders, G. L. (1998). International software piracy: Analysis of key issues and impacts. 9(4):380–397.

Harkin, D. and Whelan, C. (2022). Perceptions of police training needs in cyber-crime. 24(1):66–76.

Hijji, M. and Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions. 9:7152–7169.

Hill, M. (2023). Insider threats surge across US CNI as attackers exploit human factors. Edition: May 17,2023.

Jolls, C., Sunstein, C. R., and Thaler, R. (1998). A behavioral approach to law and economics. 50(5):1471–1550.

Justice, N. I. o. (2016). Five things about deterrence. Edition: May, 2016.

Kahneman, D. and Tversky, A. (1979). Prospect theory - analysis of decision under risk. 47(2):263–291.

Krit, S. D. and Haimoud, E. (2016). Review on the IT security attack and defense.

Levitt, S. D. (2017). The economics of crime. 125(6):1920–1925.

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

Marshall, G. (2014). *Don't even think about it : why our brains are wired to ignore climate change*. Bloomsbury USA, first u.s. edition. edition.

Michie, S., Johnston, M., West, R., Abraham, C., Hardeman, W., and Wood, C. (2014). Designing behavior change interventions: The behaviour change wheel and behavior change techniques. 47:S157–S157.

Michie, S., van Stralen, M. M., and West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. 6.

Myers, S. L. (1983). Estimating the economic-model of crime - employment versus punishment effects. 98(1):157–166.

Nagin, D. S., Solow, R. M., and Lum, C. (2015). Deterrence, criminal opportunities, and police. 53(1):74–100.

Palmer, C. C. (2001). Ethical hacking. 40(3):769–780.

Pickett, J. T. (2018). Using behavioral economics to advance deterrence research and improve crime policy: Some illustrative experiments. 64(12):1636–1659.

Pranggono, B. and Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. 4(2).

Sanders, G. L., Upadhyaya, S., and Wang, X. (2019). Inside the insider. *IEEE Engineering Management Review*, 47(2):84–91.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & security*, 21(6):526–531.

Thaler, R. H. (2008). Mental accounting and consumer choice. 27(1):15–25.

Thaler, R. H. (2017). Misbehaving: The making of behavioral economics. 6(1):77–81.

Tullock, G. (1974). Does punishment deter crime. (36):103–111.

Tversky, A. and Kahneman, D. (1981). The framing of decisions and the psychology of choice. 211(4481):453–458.

Tversky, A. and Kahneman, D. (1992). Advances in prospect-theory - cumulative representation of uncertainty. 5(4):297–323.

van der Klerj, R., Wijn, R., and Hof, T. (2020). An application and empirical test of the capability opportunity motivation-behaviour model to data leakage prevention in financial organizations. 97.

Villacis, A. H., Alwang, J. R., and Barrera, V. (2021). Linking risk preferences and risk perceptions of climate change: A prospect theory approach. 52(5):863–877.

Werts, C. E., Linn, R. L., and Joreskog, K. G. (1974). Intraclass reliability estimates - testing structural assumptions. 34(1):25–33.

Weston, S. (2020). Insider data breaches set to increase due to remote work shift.

Yoo, C. W., Sanders, G. L., and Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. 108:107–118.

A. Research Variables

Seven item scales ranging from Strongly disagree to Strongly agree

Type of question	White Hat Items and Capabilities 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?	Loadings
Social Engineering	I would like to pretend I was an authority figure to obtain a password.	.871
Social Engineerin	I would like to observe a person's behavioral patterns over a week and use that as a way to obtain their personal information	.846
Social Engineerin	I would like to use manipulative emails to obtain private information or install malware on computers.	.898
Social Engineerin	I would like to sneak into buildings a lock pick, by following someone else or by using an electronic device to counter the lock system.	.886
Technical	I would like to use password crackers to break into computer accounts.	910
Technical	I would like to set up a website that looks like real website to trick people to enter their personal information.	.877
Technical	I would like to be able to capture information that people use in wireless networks.	.900

Type of question	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?	Loadings
Financial	I could see myself engaging in hacking attacks if I needed money to purchase a $400,000 house that for my family.	.931
Financial	I could see myself engaging in hacking attacks if I needed money to purchase a new $60,000 car that I could not afford.	.877
Financial	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.	.924