Distribution Agreement

In presenting this thesis or dissertation as a partial fulfillment of the requirements for an advanced degree from Emory University, I hereby grant to Emory University and its agents the non-exclusive license to archive, make accessible, and display my thesis or dissertation in whole or in part in all forms of media, now or hereafter known, including display on the world wide web. I understand that I may select some access restrictions as part of the online submission of this thesis or dissertation. I retain all ownership rights to the copyright of the thesis or dissertation. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

Signature:

_____ _____

Quang N. Bui Date

Effects of Financial Crimes on Internet Security Behaviors

By

Quang N. Bui
Master of Arts

Political Science and Government

David Davis, Ph.D.
Co-Advisor

Danielle Jung, Ph.D.
Co-Advisor

Accepted:

Kimberly Jacob Arriola, Ph.D.
Dean of the James T. Laney School of Graduate Studies

Date

Effects of Financial Crimes on Internet Security Behaviors

By

Quang N. Bui
B.S., Georgia State University, GA, 2018
M.A., Georgia State University, GA, 2021

Advisors: David Davis, Ph.D, Danielle Jung, Ph.D.

An abstract of
A thesis submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Master of Arts
in Political Science and Government
2024

Abstract

Effects of Financial Crimes on Internet Security Behaviors
By Quang N. Bui

The role of individuals in security has become increasingly important as the magnitude of non-security threats like pandemics have been exacerbated by individual-level non-compliance. Although public safety may depend on the contributions of individuals, personal costs and the expected efficacy of individual effort may cause shirking and delegation to other actors such as firms. I argue that a threat's perceived complexity can deter contributions to public safety. If a threat is considered complex, effort is seen as less effective given the personal costs. Information about simple threats raises the expected success rate of individual effort making individual solutions more attractive if delegation is costly. I examine perceived complexity in the context of cybersecurity, an area considered highly technical, yet reliant on personal security practices to prevent public harm. I outline a survey experiment on American adults to evaluate how information about attacks affects an individual's view of their role in cybersecurity. In the experiment, individuals will record their support for increasing individual effort in cybersecurity and more intrusive firm-level solutions based on a vignette of a hypothetical cyberattack, randomized on complexity. The study aims to contribute to pre-existing studies on public opinion of cybersecurity and research on individual compliance with policy objectives.

Effects of Financial Crimes on Internet Security Behaviors

By

Quang N. Bui
B.S., Georgia State University, GA, 2018
M.A., Georgia State University, GA, 2021

Advisor: David Davis, Ph.D, Danielle Jung, Ph.D.

A thesis submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Master of Arts
in Political Science and Government
2024

Acknowledgments

I would like to thank the faculty, staff, and graduate students of the Emory Political Science Department for their advice and feedback on this project especially my advisors David Davis and Danielle Jung. I would also like to acknowledge the support from my family especially my wife Za Eng Mawi. Lastly, I would like to thank Prudentis Funds for their financial contribution to this study.

Contents

List of Figures

List of Tables

Introduction

How do individuals determine whether to contribute to the security of sensitive data? Through the use of the internet for everyday tasks, individuals generate a significant amount of sensitive data such as passwords, financial records, and browsing histories. Though these data may be unique to an individual user, "private" data is not truly private. By using internet services, individuals share their data with firms which may share and/or sell it to other firms. The interconnected nature of this data poses vulnerabilities for both individuals and firms. Since both parties have access to the same data, a weakness in the security of one can compromise the other's as well. Despite advances in cybersecurity, cyberattacks, or the malicious use of computer systems, can often bypass sophisticated security measures by exploiting less secure connections such as a reused or weak password from an employee or user. For example, the perpetrators of the 2021 Colonial Pipeline attack gained access to the company's secure infrastructure by utilizing an employee's reused password from another site (Endler, 2021).

Proper cybersecurity requires efforts from individuals and firms, but individuals often shirk this responsibility. Many prominent data breaches, such as the 2021 Colonial Pipeline attack or the 2013 Rimasauskas attacks on Google and Facebook were caused by user error despite these organizations' security investments (Endler, 2021; Huddleston, 2019). Despite the rising importance of cyberattacks for voters (NORC, 2021), many individuals routinely utilize poor cybersecurity practices such as reusing multiple passwords or using unsecured internet connections (Smith, 2017). For

individuals, strengthening cybersecurity can be costly. Since the average individual may not be knowledgeable of online threats and computer technology, they may default to experts from their organization or firms that store data and fail to take proper cybersecurity measures.

To determine how information about cyberattacks affects individual willingness to improve their cybersecurity behaviors, I examine how individuals weigh the costs and benefits of improving personal cybersecurity behaviors. Improving internet safety behaviors can be a costly investment for individuals as secure practices can hinder day-to-day operations and its benefits are often unobservable. Actions such as updating software and managing unique passwords can be time-consuming and do not produce immediate benefits. Additionally, cyber threats may be perceived as technically complex to resolve with individual-level actions since the public's understanding of cyberspace is limited. As a result, individuals may perceive that the cost of personal cybersecurity outweighs its benefit and choose to delegate the burden of securing their data to firms.

Delegation of cybersecurity, however, is not costless. Although users may entrust the safety of their data to firms when it is collected and stored by an organization, sharing that data can expose an individual to risk if that organization is targeted in an attack. Strong firm involvement in cybersecurity may also restrict privacy as some cybersecurity operations involve data collection or may regulate how individuals utilize the internet.

In this paper, I argue that public opinion on the role of individuals and firms in cybersecurity is influenced by the information received about cyberattacks. When

determining the duties of each actor, individuals consider the costs of personally improving their cybersecurity behaviors and the risks associated with a cyberattack. Although the cost of cybersecurity incentivizes individuals to free-ride, information about different types of cyberattacks may change how an individual perceives the necessity of each actor's effort. For example, receiving more information about technically unsophisticated attacks that target user error may cause individuals to consider their role in cybersecurity more seriously since these attacks can be prevented by reducing negligence.

To examine how information changes an individual's decision to delegate safety to firms and the government, I utilize a survey experiment that exposes individuals to information about different types of cyberattacks. Specifically, I examine whether individuals' preferences on cybersecurity change depending on the attack's technical complexity. I provide respondents with a vignette of a hypothetical cyberattack on a US financial institution with a randomly assigned exploit. I will then measure support for different cybersecurity actions an actor could take to prevent future cyberattacks.

This paper seeks to contribute to developing the micro-foundations of cybersecurity and the broader literature on voter and consumer preferences for government intervention. Establishing how individuals process information about cyberattacks can explain why voters are increasingly concerned with cybersecurity threats but fail to change their security habits. Understanding how information about attacks changes domestic audiences' preferences on cybersecurity can also inform how states choose to attribute cyberattacks. More generally, the study contributes to areas of political science and policy such as public health or economic intervention where individual

involvement or compliance is an important consideration.

Effects of Threat Perception on Policy and Individual Behavior

Research in political science and policy studies often examines how an individual's perception of threat affects personal behavior. Generally, when threats are considered severe, or more likely to cause harm, individuals give greater government discretion to resolve or prevent a threat. Studies on terrorism, for instance, find that individuals are more willing to support counterterrorism efforts when provided information about more deadly attacks, even if informed that such forms of terrorism are rare events (Kantorowicz et al., 2023). When considering how much power to grant governments in handling conventional security threats, individuals consider whether the severity of the threat outweighs the costs associated with expanding the scope of the government. For example, individuals are more willing to accept reductions in privacy for domestic surveillance programs when they are perceived to be more effective in preventing terrorist attacks (Trüdinger & Ziller, 2022). These studies imply that support for government policy to ensure public safety when faced with security threats is determined by the perceived severity of the threat and whether the probability of the policy resolving the threat outweighs its cost to the public.

However, the literature on security studies does not typically examine the relationship of information on an individual's involvement in their security. Because theories and perceptions of conventional security often assume that the primary actor capable

of providing security is the government public opinion studies about foreign policy and national security usually only consider whether individuals choose to support or punish leaders.

On the other hand, work on non-security threats such as those on pandemics examines how the perception of a threat can also lead to more individual contribution to public safety. Studies on the COVID-19 pandemic examine characteristics of government messaging on the public's compliance with health ordinances. When individuals perceive a disease to be more deadly, they are more likely to comply with recommendations from government agencies (Ricci P. H Yue & Ng, 2022; Rosenstrom et al., 2021), but individuals also weigh the risk of the disease relative to their confidence in proposed solutions in determining compliance. Courbage and Peter, 2021 outline a model of an individual's decision to vaccinate against infectious diseases. When individuals consider whether to take a vaccine, they weigh the risk of sickness and its magnitude with the uncertainty of the vaccine's side effects. If individuals feel that the expected benefits of the vaccine outweigh the potential risks of side effects, they opt to vaccinate.

While current literature on security and non-security threats suggests that individuals are more likely to accept personal costs in policy solutions or exert personal effort to maintain public safety, the decision to delegate public safety to the government is under-researched. Though the role of citizens and the government may be clearer in areas like terrorism or public health, other areas, such as cybersecurity are not as obvious. Though individuals may be responsible for securing their data with strong and unique passwords, cybersecurity is often viewed as a technologically complex

field, resulting in over-reliance on the expertise of firms or the government to protect data. By examining preferences over cybersecurity, an area where government and individual responsibilities are not well established, we can better understand what properties of threats to public safety cause deference to the government.

Theory

Individuals' Role in Cybersecurity

Through the use of the internet for everyday tasks, individuals generate a significant amount of sensitive data such as passwords, financial records, and browsing histories. Though these data may be unique to a user, "private" data is not truly private. By using internet services, personal data is given to firms that may share or sell it to others. The interconnected nature of this data poses vulnerabilities for both individuals and firms. Since both parties have access to the same data, a weakness in the security of one can compromise the other's as well. Firms are tasked with technical solutions to cybersecurity. Investments such as storing user data on secure servers or hiring cybersecurity experts are ways that firms may be generally expected to secure the data of their consumers and/or employees. Despite advances in cybersecurity, cyberattacks, or the malicious use of computer systems, can often bypass security measures by exploiting less secure connections such as a reused or weak password from an employee or user. The perpetrators of the 2021 Colonial Pipeline attack, for example, gained access to the company's secure infrastructure by utilizing an employee's reused password from another site and were able to cause a

shortage of gasoline in the Southeastern United States (Endler, 2021).

At an individual level, relatively simple practices can be utilized to prevent less sophisticated attacks that target user error. Individuals can invest time and resources to ensure that their devices and credentials on shared networks are secure. This is typically done through engaging in relatively simple practices such as routinely installing security or operating system updates or managing and creating unique passwords. Though individuals may lack expertise in computer science, investing more effort into improving simple personal security can mitigate potential damages from a data breach. Verizon estimates that 74% of all data breaches in the US originate from some type of user error (Verizon, 2023). While individual cybersecurity practices are often lax, as evidenced by the number of breaches caused by user error, concerns about cybersecurity policy are increasingly important to voters. A poll of American voters conducted by Gallup found that cyberterrorism ranks as the top foreign policy concern for US citizens (Younis, 2023).

In the next section, I outline a theory that explains that the discrepancy between individual cybersecurity behaviors and concerns about cybersecurity threats originates from the perceived costs and benefits of individual cybersecurity behaviors. Due to how cyber threats may be sensationalized in areas like media coverage, individuals view improving personal cybersecurity behaviors as ineffective because the type of information typically received portrays cyberattacks as exclusively complex threats rather than a spectrum of different types of attacks. Because of this perception of complexity, individuals believe that effective cybersecurity is only possible with expertise and prefer to forgo personal autonomy to allow experts from firms to

prevent cyber threats.

Costs Benefit Analysis of Individual Cybersecurity Practices and Delegation

Individuals consider the costs and benefits of different online practices when determining whether to improve their personal cybersecurity. Though cybersecurity practices such as managing and creating unique passwords may not appear to be costly, it is difficult for individuals to see that their benefits outweigh the costs. While creating proper cybersecurity may prevent potential financial losses from a cyberattack, these behaviors do not yield direct, positive benefits. Like insurance, cybersecurity is only a preventative measure as consumption does not directly improve the user's well-being, and can be considered a disutility as it can hinder an individual's internet use. Making unique passwords, while simple and financially costless, is inconvenient and cognitively tiring because it forces a user to create and recall multiple passwords.

Additionally, while users can observe the costs associated with cybersecurity investment, even the benefit of loss prevention may not be easily recognized. Although some security practices such as multi-factor authentication (MFA) may confirm that the measure prevented an attack, this is not true for all security practices (e.g. using a VPN or training against social engineering). Cybersecurity is also not perfect. Even individuals who practice proper internet safety can still be the victim of an attack. When an individual is harmed after investing in cybersecurity, it may deter further investment because of a false perception that cybersecurity was useless. On the other hand, if individuals who do not invest in cybersecurity are never affected by a cyber-

attack, they may perceive that investment is unnecessary, even though investment may benefit them if they were targeted.

Another consideration individuals may make in whether to invest in cybersecurity is the perceived complexity of cyberattacks. On average, individuals have a limited understanding of cyberattacks and the methods necessary to prevent and mitigate more technical attacks. For example, only 16% of Americans understand the idea of a "botnet" and only 13% know that using a virtual private network can minimize the risk of using insecure networks (Smith, 2017). Because of this lack of information, individuals may feel that they cannot secure themselves given the complexity of online threats. Instead, the public may feel that they need to rely on the expertise of firms and the government to secure their data because the cost of doing so on their own is high and ineffective.

Because of the perceived complexity of cyber threats, individuals may choose to delegate more authority over cybersecurity to firms or the government. Delegation, however, is not costless. Reliance on firms for cybersecurity may utilize invasive measures to prevent cyberattacks. Many firms, to reduce the risk of a data breach from user error have incorporated "Zero-Trust" security. In Zero Trust models of security, devices that access a network must be continually monitored to verify whether the device has legitimate access or is a malicious actor (Raina, Kapil, 2023). While Zero Trust approaches to cybersecurity are strong safeguards against attacks, the use of surveillance can hinder user experiences and raise concerns about privacy (Lepe, 2023).

Information Effects

While delegated cybersecurity solutions are heavily intrusive, individuals may be willing to utilize such measures when they perceive individual effort in cybersecurity to be ineffective. Why might individuals believe that their cybersecurity practices are inadequate, even though user error is the cause of most data breaches? The type of information that individuals receive about cyberattacks may affect the perceived efficacy of individual security practices.

Media coverage of cyberattacks tends to focus on large-scale data breaches from sophisticated exploits rather than more routine and unsophisticated attacks (Makridis et al., 2024). Cyberattacks, however, are not always technically sophisticated as suggested by media coverage. While most data breaches are caused by user error, the most commonly covered attacks in the media are zero-day exploits which target specific vulnerabilities at a hardware and software level, and require technical updates from firms to prevent intrusions (Makridis et al., 2024; Verizon, 2023). Because media coverage under reports social engineering attacks,the information that individuals utilize to determine their preferences over cybersecurity may be skewed to be more sophisticated than reality. As a result, individuals may falsely believe that all types of cyberattacks require technical expertise to prevent. Receiving more information about unsophisticated attacks, on the other hand, may cause individuals to view personal cybersecurity as more useful since these attacks target user error.

The perceived technical sophistication of online threats may affect what types of solutions may be preferred to improve cybersecurity. By introducing information

about less sophisticated exploits that target user error, individuals may be more likely to view personal action as more important since these attacks target the individual. Additionally, evidence from criminology finds that individuals who divulge sensitive data in an unsophisticated attack may be blamed for their involvement in a data breach. Victims of cybercrime are often blamed for their misfortune due to perceived negligence or misconduct (Cross et al., 2021) and even victims themselves are prone to self-blame for not taking more precautions (Kimpe et al., 2020). Because individuals might find a user responsible for causing a data breach when the attack relies on user error, personal cybersecurity practices may be considered more effective in preventing these attacks.

Complex attacks, on the other hand, may cause demand for increased firm involvement while diminishing demand for individual effort. Individuals may feel less confident in their abilities to prevent and resolve complex attacks, such as viruses that target servers or network devices and prefer to rely on the perceived expertise of firms in cybersecurity. As a result, the estimands of interest are the difference in support for improving individual cybersecurity practices and invasive firm-level methods like Zero-Trust, between respondents that receive complex, programming attacks and those that receive non-complex social engineering attacks. As a result, I test the following two hypotheses in this study:

Hypothesis 1: Complex attacks decrease support for more individual effort in cybersecurity.

Hypothesis 2: Complex attacks increase support for more firm effort in cybersecurity.

Experimental Design

To determine how information changes perceptions about responsibility for cybersecurity, I conducted a survey experiment using the PureSpectrum survey platform. Respondents were given a hypothetical scenario of a cyberattack on an American financial institution that utilized either a technically complex exploit or a simpler social engineering attack. Attacks against financial institutions are common targets of complex and simple methods and are often reported on by major news outlets (Sayegh, 2023). As a result, the scenarios given to respondents are close approximations to cyberattacks that individuals may observe in reality. After reading the vignette, respondents will be asked about their support for different cybersecurity practices to determine their preference for individual effort in cybersecurity or delegate to firms.

Below is a template of the vignette given to respondents as well as an example of one of the possible vignettes in the experiment. Using simple randomization, respondents will be assigned to receive either a vignette about a complex or simple attack with equal probability. The full text of each attack used in the vignette can be found in the Appendix.

Vignette Template

A major American financial institution was recently the target of a cyberattack. Hackers were able to gain access to secure servers by obtaining a user's login credentials [type of exploit].

Sample Vignette

A major American financial institution was recently the target of a cyberattack. Hackers were able to gain access to secure servers by obtaining a user's login credentials **by installing a highly sophisticated virus on an employee's work computer.**

Survey Flow

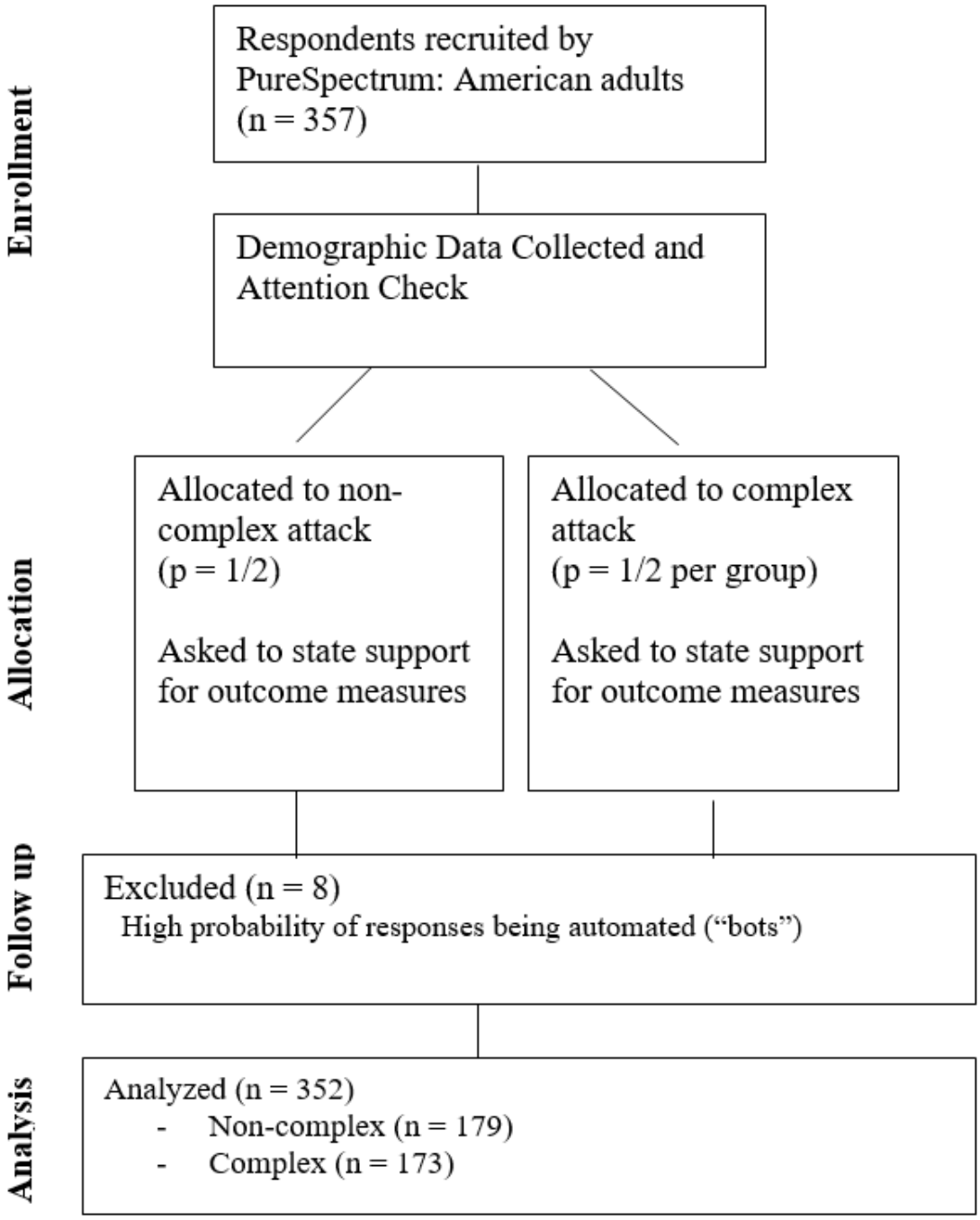
Figure 1 shows the processes respondents navigated the survey as well as were deemed eligible for the analysis via a CONSORT diagram. Once respondents are recruited by PureSpecturum and agree to participate in the survey, they will fill out personal demographic information used in the data analysis. They will then be given an attention check to determine whether information in the survey is comprehended.

After collecting demographic data and completing the attention check, respondents will be shown a randomized vignette within Qualtrics. Respondents will be assigned to either an attack with a complex or non-complex exploit using simple randomization within Qualtrics with roughly half of the respondents assigned to each type of attack. Based on the generated vignette, respondents will be asked to report their preference for each actor's involvement in cybersecurity.

Outcome Measurement

I measure a respondent's preference over delegating responsibilities of cybersecurity by recording support for individual and firm-level solutions to cyberattacks given its cost to an individual. Respondents will be given two statements describing an action that each actor can take to prevent future cyberattacks.

Figure 1: CONSORT Diagram



To measure support for individual cybersecurity behavior, I examine support for routinely updating passwords and devices every month. The outcome measure emphasizes to the respondent that the action requires a time investment to improve personal and organizational security, but is a relatively simple task. Support for this action would imply that individuals may be willing to spend some opportunity costs to improve cybersecurity.

Individual Action:

Individuals should be more active in ensuring their safety and the safety of their organization/community by routinely updating their devices and passwords every month

To measure support for delegation to a firm, I examine support for firms utilizing monitoring software to prevent data breaches. Greater support for this action would demonstrate that individuals would be willing to forgo some privacy to leverage more sophisticated firm-level solutions to cyber threats.

Firm Action:

Companies should continually monitor a user's device in their organization to ensure that it is not harmful to others

Estimation Strategy

To estimate the estimands of interest discussed in the hypotheses, I utilize the following regression equations:

$$Y_i = \beta_0 + \beta_1 Complex_i + \mathbf{X}_i'\Gamma + \epsilon_i \tag{1}$$

Where i is an indicator for each respondent in the sample, Y_i refers to the outcome variable of interest, and $Complex_i$ indicates whether the attack described utilized a complex exploit. $\mathbf{X}$ is a vector of respondent characteristics including education, ideology, age, and knowledge of previous cyberattacks, and ϵ_i is the idiosyncratic error term. The baseline comparison, indicated by the intercept β_0 is the average support from respondents who receive information about non-complex attacks.

H1 posits that complex attacks will decrease support for individual-level cybersecurity. As a result, the average treatment effect on support for individual investment when receiving information about a complex virus instead of a social engineering attack will be negative if the hypothesis is true. Thus, H1 is supported when $\beta_1 < 0$ when the outcome variable of interest is support for individual cybersecurity.

H2 argues that complex attacks will generate more support for more obtrusive firm cybersecurity investment than non-complex attacks. H2 is supported when the estimated average treatment effect of virus attacks, in comparison to a non-complex one, is negative for increasing individual and firm cybersecurity effort which would be evidenced by $\beta_1 > 0$ for those outcome variables.

Results

The study was conducted with a sample of 357 American adults on the PureSpectrum platform. After examining responses that consented to data analysis, 5 responses were determined to have a high probability of being automated based on their reCaptcha scores in Qualtrics and were removed from the sample giving a final sample size of 352 respondents. Table 1 shows the demographic breakdown of

the pilot's sample. The sample is skewed towards older white individuals with no college degree. As randomization was conducted independent of the collection of demographic data, and each treatment arm was assigned with equal probability, the treatment arms are balanced on individual demographics. Additionally, while the majority of respondents in the sample utilize online banking, a significant portion of respondents (roughly 25%) reported not using online banking, which may have influenced how attacks on financial institutions may be perceived.

Table 1: Summary Statistics

	Non-Complex		Complex	
Variable	N = 179	Mean	N = 173	Mean
Female	105	59%	108	62%
Income				
... $0-$30,000	56	31%	56	32%
... $31,000-$60,000	50	28%	51	29%
... $61,000-$90,000	33	18%	36	21%
... $91,000+	40	22%	30	17%
Race				
... White	118	66%	103	60%
... Black	30	17%	28	16%
... Native American	3	1.7%	6	3.5%
... Asian/Pacific Islander	7	3.9%	9	5.2%
... Hispanic/Latino	12	6.7%	18	10%
Age				
... 18-24	15	8.4%	11	6.4%
... 25-34	34	19%	32	18%
... 35-44	33	18%	35	20%
... 45-54	31	17%	34	20%
... 55-64	30	17%	26	15%
... 65+	36	20%	35	20%
Ideology				
... Moderate	53	30%	50	29%
... Liberal	45	25%	43	25%
... Conservative	81	45%	80	46%
Education				
... No college degree	95	53%	83	48%
... Non-graduate degree	63	35%	74	43%
... Graduate Degree	20	11%	16	9.2%
Occupation				
... Finance	7	4%	6	3%
... Tech	4	2%	5	3%
Online Banking	119	66%	129	75%

The results of the survey indicate that individuals make small distinction between technically complex and non-complex attacks when considering whether to demand more effort in cybersecurity from individuals or firms. Table 2 shows the estimated difference in support for individual and firm investment in cybersecurity from the collected sample. The full results including values of the covariates can be found in the Appendix. In both attack variations, respondents overwhelmingly supported greater contributions from both individuals and firms in cybersecurity. The study finds a statistically insignificant decrease in support for firm and individual cybersecurity when an attack is complex, supporting H1 but not H2.

Table 2: Preferences for Individual and Firm Preference Based on Complexity

	Dependent variable:	
	Individual	Firm
	(1)	(2)
Complex	−0.173	−0.129
	(0.125)	(0.127)
Constant	5.819***	5.633***
	(0.175)	(0.178)
Observations	352	352
R^2	0.056	0.061
Adjusted R^2	0.028	0.033
Residual Std. Error (df = 341)	1.162	1.184
F Statistic (df = 10; 341)	2.011**	2.207**
Note:	*p<0.1; **p<0.05; ***p<0.01	
1 = Strongly Disagree - 7 = Strongly Agree		

In addition to testing the main hypotheses, the study provides exploratory insights into how different individuals may process information about cyberattacks. Table 3

shows the differences in support for individual and firm cybersecurity contributions among different demographics. Respondents differ in their support for cybersecurity based on previous experience with cybersecurity or financial crime. Age is known to be correlated with reduced confidence in technology (Fatokun et al., 2019), and in the sample, respondents over 55 were less likely to agree with increasing their personal contribution to cybersecurity but more likely to agree with allowing invasive security procedures from firms.

The survey also indicates that tailoring information about attacks specific to an individual's background or internet usage may affect internet security behaviors or support for more intrusive policies. Providing information about attacks on an individual's specific industry may also be more effective in improving personal cybersecurity behaviors. Individuals in technology or finance, who may be more affected by similar attacks outlined in the scenario, were more willing to support individual and firm cybersecurity than the average respondents in other occupations. A surprising finding is that while past knowledge of the Equifax leak is correlated with greater support for both firm and personal cybersecurity, personal or familial victimization from fraud does not affect support.

The effects of individual characteristics on cybersecurity preferences potentially indicate that the internal mechanism of the theory is consistent with how respondents view cybersecurity despite the limited effects of the treatment. Respondents that possess characteristics associated with lower confidence in technology such as age behave consistent with the theoretical prediction in the theory as individuals over 55 are more willing to accept the costs of delegation and less willing to support

additional individual effort due to lower confidence in its efficacy. Greater confidence in personal cybersecurity effort, on the other hand may not tradeoff with firm-level practices as predicted. Respondents with employment in tech-related fields reported higher support for both personal and firm-level effort than the average respondent.

Table 3: Preferences for Individual and Firm Preference Based on Demographics

	Dependent variable:	
	Individual	Firm
	(1)	(2)
Over 55	−0.038	0.337**
	(0.131)	(0.133)
Female	−0.109	0.007
	(0.129)	(0.131)
Tech Employment	0.707*	0.687*
	(0.397)	(0.406)
Finance Employment	0.583*	0.322
	(0.332)	(0.340)
Equifax Knowledge	0.238*	0.324**
	(0.125)	(0.127)
Online Banking	0.200	0.405***
	(0.138)	(0.139)
Fraud Victimization	0.097	0.052
	(0.128)	(0.131)
Observations	352	352
R^2	0.056	0.061
Adjusted R^2	0.028	0.033
Residual Std. Error (df = 341)	1.162	1.184
F Statistic (df = 10; 341)	2.011**	2.207**
Note:	*p<0.1; **p<0.05; ***p<0.01	
1 = Strongly Disagree - 7 = Strongly Agree		

Discussion

Although the study's results do not provide sufficient evidence that the perceived complexity of cyberthreats affects the acceptance of personal or firm-level cybersecurity, the findings improve current understanding of public opinion on cybersecurity. First, complexity seems to affect willingness to advance personal efforts and more invasive firm measures in cybersecurity in similar ways. While the theoretical prediction of the paper argued that complex attacks would decrease support for individual cybersecurity effort but increase support for firm-level contribution, the results of the study finds that the complexity of an attack decreases support for both individual and firm cybersecurity. Though the findings are not statistically significant or sufficiently powered, they suggest that attacks that utilize more advanced programming methods diminish the perceived efficacy of personal cybersecurity also make more invasive methods of security at the firm level less attractive since the costs may be perceived to outweigh the security benefits.

In addition to outlining and testing a theory of complexity in cybersecurity the project also examined how attacks are perceived by different individuals. As a result, the study may have implications for how organizations should structure training or information on cybersecurity. Consistent with pre-existing work, I find that older respondents are less willing to demand cybersecurity effort from individuals, perhaps due to lack of confidence in technology skills, but are more willing than other age groups to accept more invasive firm measures. Tailoring cybersecurity information more specifically to populations of interest may also be more effective than emphasiz-

ing damages or complexity. Since the scenario was specific to a financial institution, respondents directly employed in the finance industry exhibited higher support for individual and firm-level cybersecurity practices.

While the study reinforces pre-existing research in cybersecurity preferences and demonstrates that complexity of a policy issue may have consequences for the adoption of certain practices and policies, additional work in this field is needed to understand individual-level compliance. One such issue is that although more complex attacks seem to lower support for more intrusive measures from firms, the higher support for cybersecurity practices among respondents from the finance sector makes the interpretation of this finding less clear. In the measurement of the outcome, it is unclear whether respondents believe that the cost of surveillance will be imposed onto them as consumers or on employees of the institution. Support from those in the finance industry suggests that individuals are willing to impose costs on themselves to reduce the risk of an attack, but additional work is needed to determine whether the invasive nature of cybersecurity is permissible for both consumers and employees.

Additionally, a pilot study of 231 respondents was conducted prior to the study in the paper. In addition to analyzing the effects of attack complexity on the preferences for individual and firm contributions to cybersecurity, the pilot study also varied the attacker's identity between a Chinese military group, a Chinese criminal group, and an American criminal group, and also examined preferences for government contributions to cybersecurity. In the pilot study, respondents who received an attack from a Chinese group were more likely to support individual contributions to cybersecurity than those who received an American-based attack. A full breakdown of the pilot

study instrument and results can be found in the Appendix.

Though the sample size of the pilot was limited, the results of the pilot in conjunction with the main study suggest that non-complex, foreign-based cyber threats are most likely to cause demands for improvements in individual cybersecurity behaviors. Because of these factors, reducing the complexity of cyberspace by tailoring information about cybersecurity and threats to focus on user error and its effects in an individual's specific industry or setting may be useful to enhance security at both a firm and policy level.

Potential Contributions

The study seeks to contribute not only to the cybersecurity literature but also other areas of political behavior and security studies. In cybersecurity, this project builds upon pre-existing research on public opinion on cyber policy and personal behaviors on cybersecurity. Pre-existing research in political science examines the effects of attribution claims on support for cybersecurity policy and its saliency (M. Leal & Musgrave, 2022; M. M. Leal & Musgrave, 2023; Shandler et al., 2023), or how individuals determine personal cybersecurity behaviors (Kostyuk & Wayne, 2020). This paper seeks to bridge research between these two approaches by determining how individuals view their role in cybersecurity given the implications of policy intervention. Additionally, while previous research has focused on the effects of severity of cyberattacks on support for policy, this study highlights an important component of cybersecurity that is mostly unexplored in the literature: the perceived complexity of technology and cyber threats.

In security studies, this paper hopes to illustrate the importance of expanding the scope of research from state-level analysis to explore how other actors such as individuals or firms may affect a nation's security or other foreign policy objectives. Though the role of the public in security has been explored through mechanisms such as audience costs (Fearon, 1994; Kertzer & Brutger, 2016), the threats posed to national security from data breaches caused by human error, such as Colonial Pipeline, illustrate how individuals can have a direct effect on security.

In other fields of political behavior and policy studies, the survey will contribute to our understanding of how individuals decide whether to comply or support policy aimed at resolving a threat to the public. Though pre-existing research in areas like public health focuses on compliance given the perceived severity of a threat (Ricci P. H Yue & Ng, 2022; Rosenstrom et al., 2021), examining how the complexity of a threat affects the perceived efficacy of individual compliance can explain why individuals choose not to comply with policy mandates even when a threat is perceived to be severe.

Appendix A

Additional Tables

Table A.1: Regression Model without Covariates - Individual

	Dependent variable:
	Support for Individual Cybersecurity
Complex	−0.160
	(0.126)
Constant	6.056***
	(0.088)
Observations	352
R^2	0.005
Adjusted R^2	0.002
Residual Std. Error	1.178 (df = 350)
F Statistic	1.622 (df = 1; 350)
Note:	*p<0.1; **p<0.05; ***p<0.01

Table A.2: Regression Model without Covariates - Individual

	Dependent variable:
	Support for Individual Cybersecurity
Complex	−0.119
	(0.128)
Constant	6.056***
	(0.090)
Observations	352
R^2	0.002
Adjusted R^2	−0.0004
Residual Std. Error	1.204 (df = 350)
F Statistic	0.865 (df = 1; 350)
Note:	*p<0.1; **p<0.05; ***p<0.01

Appendix B

Survey Instrument

Vignette Attributes

Type of Exploit

Individual/unsophisticated level exploit

after the user accidentally input the information when responding to a suspicious e-mail

Organizational/sophisticated exploit

by installing a highly sophisticated virus on the organization's network

Attacker Identity

Demographic Questions

Choose one or more races that you consider yourself to be:

- Black or African American
- American Indian/Native American or Alaska Native

- Asian
- Native Hawaiian or Other Pacific Islander
- Hispanic and/or Latino
- Other

What is the highest level of education you have completed?

- Some high school or less
- High school diploma or GED
- Some college, but no degree
- Associates or technical degree
- Bachelor's degree
- Graduate or professional degree (MA, MS, PhD, JD, MD, DDS etc.)
- Prefer not to say

What was your total household income before taxes during the past 12 months?

- $\$0 - \$30,000$
- $\$31,000 - \$60,000$
- $\$61,000 - \$90,000$
- $\$91,000+$

What best describes your political ideology?

- Extremely Conservative
- Conservative
- Slightly Conservative
- Moderate
- Slightly Liberal
- Liberal
- Extremely Liberal

How old are you?

- 18-24 years old
- 25-34 years old
- 35-44 years old
- 45-54 years old
- 55-64 years old
- 65+ years old

How do you describe yourself?

- Male

- Female
- Non-binary, other, or prefer not to say

Which of the following industries most closely matches the one in which you are employed?

- Forestry, fishing, hunting or agriculture support
- Real estate or rental and leasing
- Utilities
- Management of companies or enterprises
- Legal services
- Manufacturing or Constructing
- Educational services
- Health care or social assistance
- Technology or Data Processing
- Arts, entertainment or recreation
- Transportation or warehousing
- Food services
- Finance or insurance
- None of the above

Behavioral Questions

Please select the following online activities that you engage in regularly

- Online banking
- Social media
- Downloading and installing software
- Streaming video and/or music
- Access work files from home and/or Remote work

If you utilize online banking, what device do you most regularly use to access your services?

- Personal computer (Laptop, Desktop, Mac)
- Mobile device (Phone, Tablet)

Have you or a family member been a victim of identity theft or credit card fraud?

- Yes
- No

What news sources do you utilize from the following?

- Fox News
- NBC News

- CNN
- Wired/CNET/Medium
- New York Times
- CBS News
- Social Media
- Other news source
- None

Select your agreement with this statement. "Individuals have a responsibility to take measures to ensure the safety of their community."

- Strongly disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree

Select your agreement with this statement. "The government should be able to access an individual's private messages to investigate an ongoing crime?"

- Strongly disagree
- Disagree

- Neither agree nor disagree
- Agree
- Strongly agree

Select your agreement with this statement. "It is okay for companies to collect information on an individual's activity on their websites to improve the individual's user experience, so long as the individual's identity remains private."

- Strongly disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree

Were you previously aware that in 2017 the credit bureau Equifax was the subject of a data breach?

- Yes
- No

Attention Check

You will be now asked a few questions about your understanding of cybersecurity concepts. Your answers in the next section will not affect your compensation for participating in the survey. Select "yellow" below to continue the survey.

- Red
- Blue
- Yellow [Correct]
- Green

Appendix C

Pilot Survey Results and Figures

Balance Table

Table C.1: Balance Table

Treatment Assignment	Control		China Gov Simple		China Crime Simple		US Crime Simple		China Gov Complex		China Crime Complex		US Crime Complex	
Variable	N = 26	%	N = 33	%	N = 27	%	N = 30	%	N = 42	%	N = 38	%	N = 38	%
Age														
- 18-24	6	23%	2	6%	4	15%	6	20%	6	14%	1	3%	3	8%
- 25-34	3	12%	7	21%	5	19%	0	0%	3	7%	5	13%	6	16%
- 35-44	3	12%	5	15%	4	15%	7	23%	9	21%	9	24%	4	11%
- 45-54	6	23%	6	18%	6	22%	5	17%	6	14%	5	13%	5	13%
- 55-64	1	4%	4	12%	3	11%	5	17%	10	24%	6	16%	8	21%
- 65+	7	27%	9	27%	5	19%	7	23%	8	19%	12	32%	12	32%
Degree														
- <HS	1	4%	0	0%	2	7%	1	3%	4	10%	4	11%	3	8%
- HS	7	27%	10	30%	11	41%	8	27%	12	29%	10	26%	8	21%
- Some College	6	23%	6	18%	5	19%	4	13%	8	19%	8	21%	6	16%
- Associates	5	19%	5	15%	3	11%	4	13%	5	12%	1	3%	2	5%
- BA	4	15%	11	33%	5	19%	10	33%	9	21%	8	21%	15	39%
- Grad	3	12%	1	3%	1	4%	3	10%	4	10%	7	18%	4	11%
Female	13	50%	17	52%	11	41%	18	60%	22	52%	21	55%	19	50%
Ideology														
- Conservative	7	27%	11	33%	10	37%	11	37%	13	31%	12	32%	18	47%
- Liberal	8	31%	12	36%	6	22%	11	37%	10	24%	10	26%	9	24%
- Moderate	11	42%	10	30%	11	41%	8	27%	19	45%	16	42%	11	29%
Income														
- $0-$30,000	9	35%	10	30%	10	37%	10	33%	14	33%	14	37%	9	24%
- $31,000-$60,000	5	19%	11	33%	5	19%	7	23%	15	36%	10	26%	9	24%
- $61,000-$90,000	8	31%	7	21%	6	22%	8	27%	3	7%	5	13%	8	21%
- $91,000+	4	15%	5	15%	6	22%	5	17%	10	24%	9	24%	12	32%
Race														
- White	22	85%	24	73%	20	74%	23	77%	30	71%	29	76%	28	74%
- Black	3	12%	5	15%	6	22%	5	17%	7	17%	4	11%	4	11%
- Native American	0	0%	1	3%	1	3.7%	0	0%	2	4.8%	2	5.3%	2	5.3%
- Asian/Pacific Islander	0	0%	2	6.1%	1	3.7%	1	3.3%	2	4.8%	2	5.3%	0	0%
- Hispanic and/or Latino	3	12%	4	12%	1	3.7%	3	10%	5	12%	4	11%	6	16%

Results

Figure C.1: Average Support for Actor Investment by Treatment Assignment

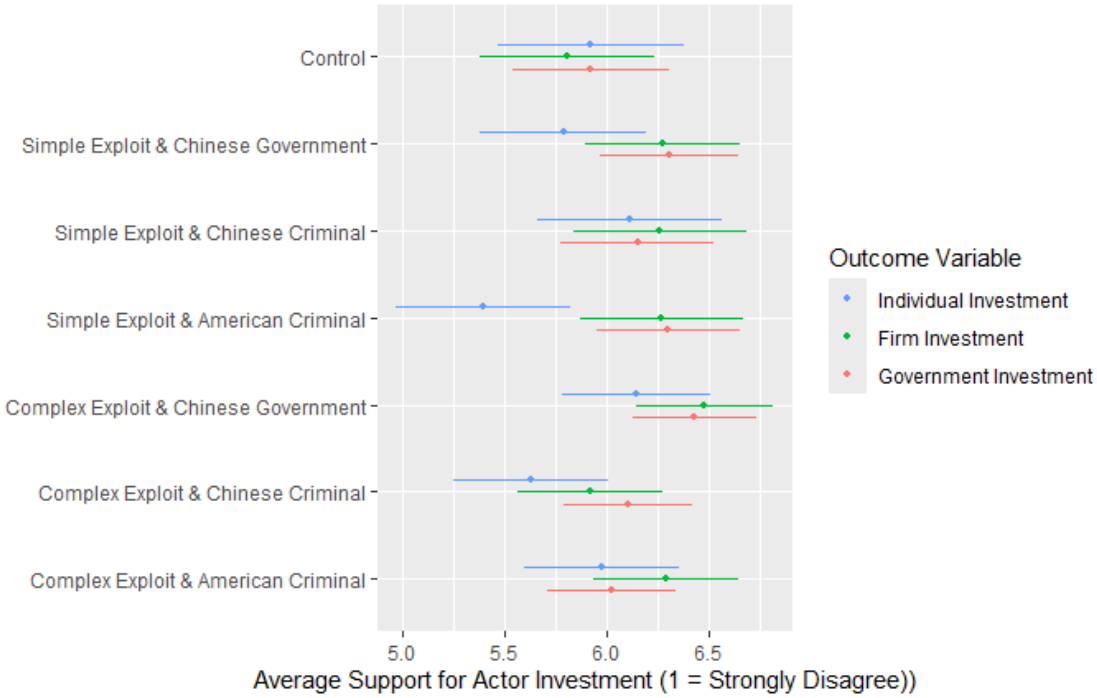


Figure C.2: Average Support for Actor Punishment by Treatment Assignment

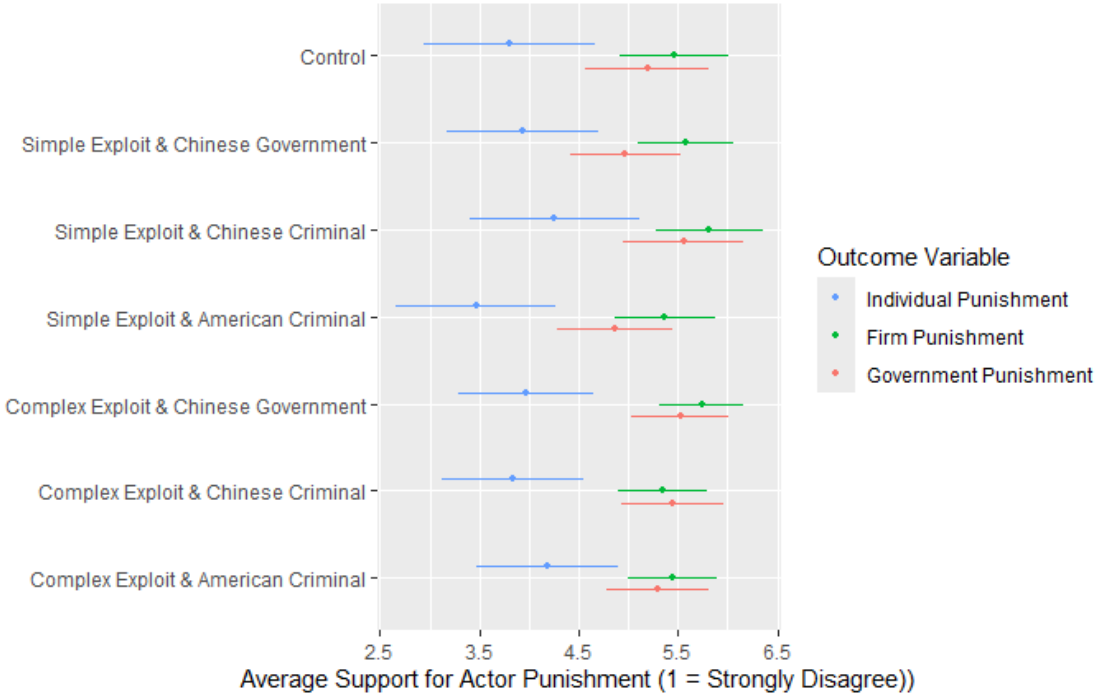
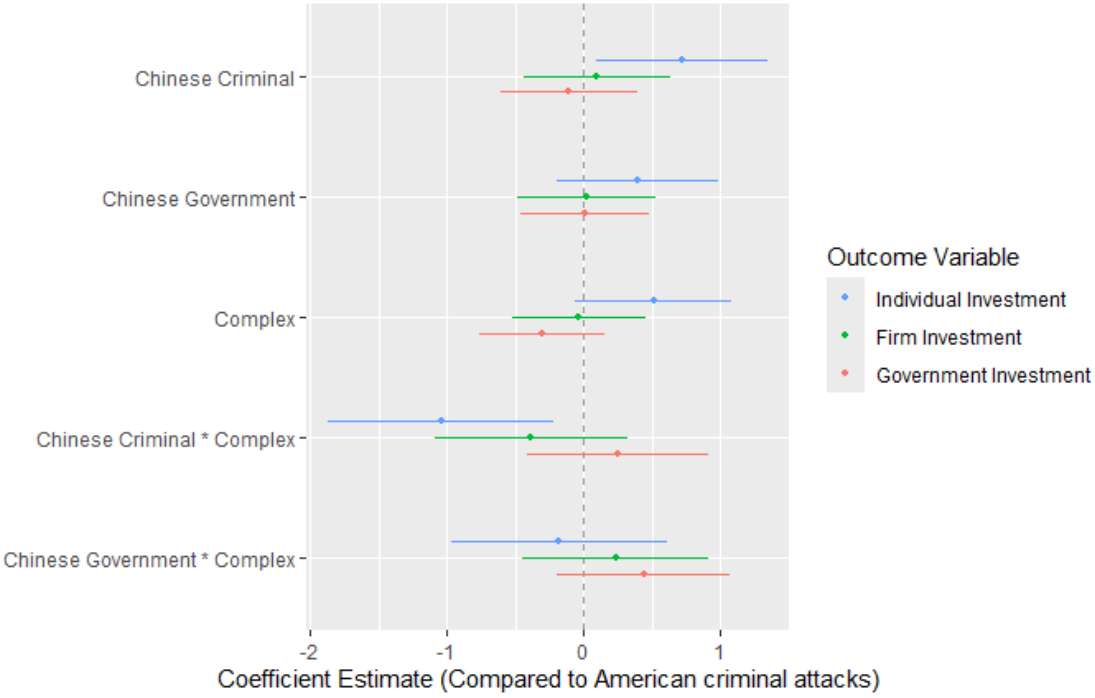


Figure C.3: Effect of Attack Characteristics on Support for Actor Investment



Appendix D

Pilot Survey Instrument

Vignette Attributes

Type of Exploit

Individual/unsophisticated level exploit

discovering a reused password from an employee

Organizational/sophisticated exploit

installing a virus on an employee's work computer

Attacker Identity

Chinese military:

The attackers were determined to be affiliated with the Chinese government

Chinese criminal group:

The attackers were determined to be affiliated with a prominent Chinese criminal group

American criminal group:

The attackers were determined to be affiliated with a prominent American criminal group

Demographic Questions

Choose one or more races that you consider yourself to be:

- Black or African American
- American Indian/Native American or Alaska Native
- Asian
- Native Hawaiian or Other Pacific Islander
- Hispanic and/or Latino
- Other

What is the highest level of education you have completed?

- Some high school or less
- High school diploma or GED
- Some college, but no degree
- Associates or technical degree
- Bachelor's degree
- Graduate or professional degree (MA, MS, PhD, JD, MD, DDS etc.)
- Prefer not to say

What was your total household income before taxes during the past 12 months?

- $\$0 - \$30,000$
- $\$31,000 - \$60,000$
- $\$61,000 - \$90,000$
- $\$91,000+$

What best describes your political ideology?

- Extremely Conservative
- Conservative
- Slightly Conservative
- Moderate
- Slightly Liberal
- Liberal
- Extremely Liberal

How old are you?

- 18-24 years old
- 25-34 years old
- 35-44 years old

- 45-54 years old
- 55-64 years old
- 65+ years old

How do you describe yourself?

- Male
- Female
- Non-binary, other, or prefer not to say

Behavioral Questions

Please select the following online activities that you engage in regularly

- Online banking
- Social media
- Downloading and installing software
- Streaming video and/or music
- Access work files from home and/or Remote work

If you utilize online banking, what device do you most regularly use to access your services?

- Personal computer (Laptop, Desktop, Mac)
- Mobile device (Phone, Tablet)

Have you or a family member been a victim of identity theft or credit card fraud?

- Yes
- No

What news sources do you utilize from the following?

- Fox News
- NBC News
- CNN
- Wired/CNET/Medium
- New York Times
- CBS News
- Social Media
- Other news source
- None

Select your agreement with this statement. "Individuals have a responsibility to take measures to ensure the safety of their community."

- Strongly disagree
- Disagree
- Neither agree nor disagree

- Agree
- Strongly agree

Select your agreement with this statement. "The government should be able to access an individual's private messages to investigate an ongoing crime?"

- Strongly disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree

Select your agreement with this statement. "It is okay for companies to collect information on an individual's activity on their websites to improve the individual's user experience, so long as the individual's identity remains private."

- Strongly disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree

Attention Check

You will be now asked a few questions about your understanding of cybersecurity concepts. Your answers in the next section will not affect your compensation for participating in the survey. Select "yellow" below to continue the survey.

- Red
- Blue
- Yellow [Correct]
- Green

Comprehension Check

Cyberattacks refer to many different scenarios, but they attempt to cause harm by gaining access a computer system or device. Hackers can steal sensitive communications or financial information by retrieving a user's passwords or using programming tools such as viruses.

There are many ways to prevent cyberattacks. For individuals, utilizing strong and unique passwords as well as anti-virus can help secure personal data. For organizations, storing consumer data on modern devices with encryption, as well as collaborating with government cybersecurity experts can prevent data theft.

To continue the survey please answer the following based on the previous information you read about cyberattacks. Which of the following is true about cyberattacks?

- There is only one way to prevent cyberattacks

- Cyberattacks can steal sensitive communications [Correct]
- The phrase cyberattack refers to one specific scenario
- Utilizing strong passwords increases vulnerability to a cyberattack

Cybersecurity Knowledge Questions

Basic Question: *Which of the following is an example of software?*

- Central Processing Unit (CPU)
- Operating System (OS) [Correct]
- Random Access Memory (RAM)
- All of the above

Intermediate Question: Which of the following is true about a distributed denial of service (DDoS) attack?

- It occurs when attackers are able to physically destroy computer equipment
- It occurs when attackers flood a network with false requests [Correct]
- It installs malware on the targeted device
- It requires the attacker to obtain a password to a secure server

Cyberattack Specific Question: In 2017, the credit bureau Equifax was victim to which of the following:

- distributed denial of service (DDoS) attack

- data breach [Correct]
- ransomware attack
- kinetic attack