Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats

Nadiya Kostyuk[*]& Carly Wayne[†][‡]

June 13, 2019

Abstract

Cybersecurity represents a unique national security challenge for states: data breaches with the potential for national, macro-level consequences are most likely to occur at the *micro*-level, originating through the security errors of individual computer users. Thus, aspects of national cybersecurity can often critically depend on the personal attitudes and behavior of average citizens connecting online. However, to date, theories of state cybersecurity have almost exclusively focused on the macro-level, and very little is known about how the mass public reacts to — and protects themselves from — cybersecurity threats. This study addresses this gap, drawing on psychological theories of risk perception to explain why the public simultaneously reports great concern about cybersecurity, yet does little to protect their personal safety online. Using a novel survey experiment, we examine how exposure to different types of data breaches impacts citizens' cyber risk assessments, personal online behavior, and support for various national cybersecurity policies. We find that baseline concerns about cybersecurity and knowledge about safe online practices are very low. However, exposure to a *personally relevant* data breach heightens risk perception and increases willingness to engage in safer online practices. But these effects are circumscribed — *actual* online behavior is more resistant to change. These results have important implications for the design of effective state cybersecurity policy.

Word count: 11,293

[*]Department of Political Science, University of Michigan, Ann Arbor; nadiya@umich.edu;

[†]Department of Political Science, University of Michigan, Ann Arbor; carwayne@umich.edu

[‡]Authors' names are listed alphabetically; this study is pre-registered with EGAP (ID#: 20170131AA)

1 The Paradox of Cyber Threat

Russia's cyber activities undertaken during the 2016 U.S. Presidential election have highlighted the growing role played by cyber operations[1] in state national security. However, the exact type and level of threat posed by cyber operations remains deeply contested, both by security experts and political elites. While political officials often reference the possibility of sensationalist future cyber attacks, akin to a "cyber Pearl Harbor" (Lawson et al., 2016; Valeriano and Maness, 2015), security experts contend that the origin and target of most cyber threats is much more mundane – data breaches of sensitive information triggered by user error (OnlineTrustAlliance, 2018). These data breaches have serious and important consequences, even though the destruction they cause is unlikely to rise to the level invoked by the imagery of Pearl Harbor or other such catastrophic physical violence.

The 2016 hack of the Democratic National Committee (DNC) is a primary example. This operation, an attempt by the Russian government to deliberately subvert the U.S. national election process (McKew, 2018), succeeded because of a single successful phishing email opened by the assistant of Hillary Clinton's campaign chairman, John Podesta.[2] The information attained as a result of this email gave hackers access to sensitive internal Democratic campaign communications, which, when publicized by Wikileaks, may have increased voter antipathy towards the Democratic nominee and impacted the outcome of the 2016 U.S. election. Indeed, according to NBC News, the Trump campaign mentioned Wikileaks at least 145 times in the last month of the Presidential race.[3]

Other recent data breaches have demonstrated that the private sector is also incredibly vulnerable to cyber breaches, affecting millions of citizens and causing significant economic damage: Uber's 2016 data breach revealed private information of over 57 million drivers and rid-

[1] Throughout this paper, we use the term cyber operations to denote "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace capabilities [...] deny or manipulate adversary or potential adversary decision making, through targeting an information medium (such as a wireless access point in the physical dimension), the message itself (an encrypted message in the information dimension), or a cyber-persona (an online identity that facilitates communication, decision-making, and the influencing of audiences in the cognitive dimension)" (*Joint Publication 3 13 Information Operations*, 2014, p. II-9). Note that, importantly, the term "cyber operations" here does not incorporate information about the specific content of the *objective*. Cyber operations can in fact have *multiple* motives — political, social, or economic.

[2] *Phishing* is "the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication" (Stavroulakis and Stamp, 2010).

[3] Source: https://www.nbcnews.com/politics/elections/12-days-stunned-nation-how-hillary-clinton-lost-n794131

ers, the 2017 Equifax hack compromised the financial records of 145.5 million U.S. customers or about 45% of the U.S. population, and the 2017 WannaCry ransomware operation infected more than 300,000 computers across 150 countries, paralyzing healthcare systems throughout Europe for days. This operation, attributed to the North Korean government, had significant national and political consequences and illustrates the confluence of criminal and political motives in some cyber operations: the WannaCry hackers used cyber tools to perpetrate a *crime*, theft, against a private company, in order to support the *political* objectives of the North Korean government, most likely helping to finance their nuclear program (Nakashima, 2017).

These examples demonstrate both the broad variety of cyber operations and the primary reason the perpetrators were successful: user error. In other words, many of the most notable recent cyber operations around the world have been as *serious* as they have been *preventable*. In fact, cybersecurity experts estimate that up to ninety-three percent of data breaches — a particularly prominent type of cyber operation where information is stolen or taken from a system without the knowledge or authorization of the system's owner — can be avoided if "simple steps are taken, such as regularly updating software, blocking fake email messages by using email authentication, and training people to recognize phishing attacks" (OnlineTrustAlliance, 2018). Essentially, if individual computer users engaged in safer online practices, the efficacy of many types of cyber operations, and data breaches in particular, could be vastly diminished, drastically reducing economic and security threats to both individuals and the state from cyber.

However, despite these and other high-profile cyber operations in recent years targeting government, corporate, and individual targets, many computer users still fail to engage in even the most basic cyber-hygiene practices. This is problematic not just from a consumer or industry perspective, but also for national security writ large. Because cyber operations are designed to exploit the weakest link in an online system, the preparedness of individual citizens to defend their computers from breaches can be a crucial component of state cybersecurity. While this is particularly true for users that have access to sensitive networks, in today's digital era, this in fact represents a large share of the population for most developed, connected countries. For example, the U.S. Federal Government alone employs over 2 million civilian workers. But it is not just citizens working for the federal government that may have access to sensitive data. Google, for example, employs over 88,000 people, who, collectively, have access to the private information of more than 1 billion worldwide users of Google products.

This failure to follow digital security best practices is highlighted by a 2017 PEW poll: just

12% of Internet users report using a password management software, 41% report sharing passwords with friends or family, and 54% use public WiFi networks to conduct sensitive online activity, such as banking (Olmstead and Smith, 2017*b*). This is a major reason why up to 30% of data breaches originate not with a software or hardware failure from a corporation but with what is called a "wet-ware" failure by individual users (Levin, 2015).[4] Thus, individual users indeed have a degree of control in protecting their private information online — they simply choose not to engage in many of these basic practices.[5] This lack of care in personal online behavior is striking because cyber is often mentioned by citizens as an important security concern. In 2014, 91% of Americans surveyed by PEW felt that consumers had lost control over how their personal information was collected and used by companies and 81% reported feeling insecure when sharing personal information on social media (Madden, 2014). By 2017, PEW reported that "a sizable share of the public thinks that their personal data have become less secure in recent years, and...lacks confidence in various institutions to keep their personal data safe from misuse...and expects that major cyber-attacks will be a fact of life in the future" (Olmstead and Smith, 2017*a*).[6]

We argue that this disconnect is due to two primary factors. Namely, in order to engage in safer online practices, average citizens need to first understand 1) what exactly the risk from cyber is, and 2) what they can do to reduce it. Relatedly, citizens need to believe that their behavior actually *matters* in terms of protecting their personal information and reducing the risk of an intrusion.[7]

In the present research, we use a pre-registered online survey experiment to investigate how citizens perceive cybersecurity risk, how these perceptions can be altered, and the effect these beliefs may have on personal online behavior and preferences regarding state cybersecurity policies. In this study, we examine one type of cybersecurity threat — the hacking of sensitive

[4] *Wet-ware* is when individuals fail to use basic cyber-hygiene to protect their computers, such as updating their software on time, changing passwords, etc.

[5] While there are certain elements of cybersecurity that are, of course, outside the average user's control, cybersecurity experts contend that users nonetheless have substantial personal efficacy to enact a host of relatively easy cyber-hygiene practices that would drastically reduce their risk of having their personal information compromised in the event of a corporate breach. For example, even though individual users may not have control over the security of a corporation's servers, they do have control over the frequency with which they change their passwords – which can be critical in protecting online accounts in the aftermath of any corporate data breach.

[6] The results of this most recent PEW study were not published at the time of our study, but the fact that their findings regarding citizens' cybersecurity concerns and practices mirror our own findings is reassuring regarding the generalizability of our sample.

[7] In other words, while individual users do in fact have a high level of personal efficacy in many aspects of their own cybersecurity, many may simply *assume* or perceive that they do not.

personal information (e.g., data breaches). Typically referred to as cyber crime, this type of threat, despite its name, can actually stem from both criminal *and* political motives. In other words, hacking personal information can be used for simple monetary gain (e.g., to blackmail individuals or access banking accounts) or to advance a political agenda, as was the case in the 2016 DNC hack.

We focus on this type of operation for a few key reasons. First, data breaches are currently the most widely used form of cyber operations and, as such, are most likely to impact individual citizens on a daily basis. Identity theft stemming from data breaches is the fastest-growing crime in the United States, costing Americans over $16.8 billion and affecting about 16.7 million people in 2017.[8] It is also the type of cyber operation that most clearly depends on the individual cybersecurity practices of members of the mass public and their (lack of) cyber-hygiene practices. Moreover, while the general impression of these hacks is that they are criminally motivated, many of the most recent famous data breaches have, in fact, been directly tied to foreign governments or dissidents with political aims. Examples include: the 2016 Russian phishing strike on the DNC, the 2017 Equifax hack sponsored by the Chinese, the WannaCry operation that was purportedly used to sponsor North Korea's nuclear program, and the 2014 Sony hack, also perpetrated by the North Koreans.[9] Thus, data breaches are *common*, *preventable*, and, often, *political* — with major downstream economic, diplomatic, and national security consequences.

We hypothesize that, because data breaches do not engage key appraisals central to heightening perceptions of risk, many citizens may simply be unaware of the risk posed by this type of operation. This could explain why average citizens are not motivated to learn about — and actively engage in — preventative steps to protect their personal online security. Specifically, we argue that citizens do not see data breaches as a major threat because these threats are perceived as less common, less catastrophic, and more controllable than spectacular claims of a "cyber Pearl Harbor" or other physical violence concerns frequently mentioned by citizens as major fears (such as terrorism or violent crime) (Slovic, 2016). However, we suspect that exposure to a data breach that *personally impacts* an individual is likely to bring the potential

[8] Source: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[9] Moreover, even when an operation is not explicitly political in nature or directly tied to a foreign government, these types of criminally-motivated hacks — when sufficiently large — can also, nonetheless, have macro-political consequences. For example, as a result of the 2013 Target data breach, private data for seventy million customers was compromised. This data breach had major medium-term economic effects, causing a significant drop of about 40 percent of Target's profit in the fourth quarter of 2013 (Harris, 2014), and a total loss of $290 million USD to data breach relates fees (Manworren, Letwat and Daily, 2016).

costs of these types of cyber intrusions into sharp relief and, as a result, heighten perceptions of future risk from cyber threats. This may also lead citizens to support costlier national cybersecurity policies, particularly those designed to prevent data breaches, and to engage in safer cybersecurity practices themselves.

Our findings our intriguing. First, we find that baseline knowledge about cybersecurity is indeed very low, even though comfort with computers is assessed as quite high. Likewise, despite a relatively high degree of stated concern with privacy online, most respondents did not engage in safe computer use. After exposure to a data breach with a personal dimension, however, subjects report significantly higher levels of perceived personal risk from cyber operations and were marginally more likely to indicate a willingness to improve their use of basic cyber-hygiene practices online. Importantly though, while we find that subjects *expressed* a willingness to improve their cybersecurity practices online after exposure to a personally relevant data breach, we did not observe any difference in *actual* online behavior. Moreover, support for various government cybersecurity policies also remained static.[10] Thus, the effect of exposure to a data breach on future online behavior and macro-level political attitudes is quite circumscribed. These results have important implications for the design of effective cyber policies and the role of the public and public opinion in shaping state cybersecurity.

2 Risk Perception & Attitudes toward Cybersecurity

International political threats, including in the realm of cyber, are inherently *uncertain* and, so, there exist many potential interpretations of the level of risk any particular security concern poses. Thus, risk perceptions can be a crucial variable shaping individuals' understanding of the appropriate behavioral and policy response to a threat. Indeed, "Many public debates, whether on climate change or counterterrorism, center not on whether we should accept risk or not, but rather, on contesting which choices count as risky in the first place" (Kertzer, 2017, p. S118). As a result, taking actors' risk perceptions into account is critical for understanding their foreign policy preferences and behaviors (Kertzer, 2017; Hafner-Burton et al., 2017). For example, perceptions and preferences over risk have been shown to be a critical dimension impacting international conflict (Goldgeier and Tetlock, 2001; Jervis, 1976; Levy, 1983; McDermott, 2001), affecting, for example, the conduct of crisis bargaining (Jervis, 1992), preventative

[10] This is not due to heterogeneous treatment effects pulling in different directions by party ID, suggesting these policies have not yet become significantly politicized. We discuss the implications of this finding at length in the discussion.

wars (Levy, 1992), hostage crises (McDermott, 2001), and deterrence (Stein, 1985).

However, we know surprisingly little about how the public views risk in the so-called "fifth domain," cyberspace (Heal and Bunker, 2014). That is because, to date, most academic work on cybersecurity has focused on the macro-security dynamics of cyber warfare[11] rather than a bottom-up perspective investigating the attitudes of individual citizens. While this macro-approach has shed important light on the overall strategic and technical environments in which cyber operations are used, its does not delve into the attitudes and behavior of individual computer users or the implications this may have for macro-level national security. Thus, we do not have strong empirical evidence regarding how individuals assess the risk from cyber operations and how this impacts their personal online behavior or shapes their support for various cybersecurity policies.

Research that investigates the bottom-up processes associated with cyber-related issues has generally focused on how the attitudes and behavior of the mass public have changed as a result of the proliferation of the Internet, rather than on the implications of these attitudes and behavior for national cybersecurity per se. For example, existing scholarship has explored the effects of the Internet on civic communication and citizens' participation in politics (Coleman, Taylor and van de Donk, 1999; Bimber, 2001; Weber, Loumakis and Bergman, 2003; Kluver, 2004; Polat, 2005; Haynes and Pitts, 2009), on individuals' social activity (Brants et al., 1996; Franzen, 2000; Robinson et al., 2000; Howard, Rainie and Jones, 2001), patterns of collective action (Lupia and Sin, 2003) and the transformation of the citizen-bureaucrat relationship (Scavo and Shi, 2000; Bovens and Zouridis, 2002; Welch and Fulla, 2005; Mossberger, Tolbert and Stansbury, 2003). Though important, this work has not specifically explored citizens' beliefs about cybersecurity risks and how this connects to the safety of their personal online behavior and support for changes to national cybersecurity policies.

This is problematic, because research on cybersecurity has broadly emphasized the central role that individual users play in protecting national security. Namely, this work has primarily stressed the threat of system intrusions due to a user or engineer error (Gartzke and Lindsay, 2015; Libicki, 2007), as this is thought to represent the greatest vulnerability of online systems. The 2015 breach of the White House Office of Personnel Management (OPM) is a key example in this regard (Eng, 2015). As a result of this breach, which was the largest government breach

[11] There are many important examples of this type of work, including: Axelrod and Iliev 2014; Borghard and Lonergan 2017; Buchanan 2017; Gartzke 2013; Kreps and Schneider 2018; Libicki 2009; Lindsay 2013; Lindsay and Gartzke 2016; Nye Jr 2017; Rid and Buchanan 2015; Schneider 2017; Valeriano and Maness 2014, 2018.

in U.S. history, the personal data of 22.1 million people, including federal employees, contractors, families and friends from security clearance forms that go back to 1985, were stolen. Security experts have cited "sloppy cyber-hygiene" leading to lax information security at the agency as the primary reason why the perpetrators succeeded in gaining access to this confidential data, which could be used to break into other government systems (Pham, 2016). This example illustrates how individual users can be critical in establishing collective cybersecurity, as well as the potential large potential consequences that the lack of individual cyber-hygiene can have for both macro-level national security and micro-level personal safety.

In addition, in democratic countries, public opinion has been shown to play an important role in shaping the incentives of elected officials when they design state policy. While the extent to which leaders can exert top-down influence on public opinion is a central debate in the American politics field, with some scholars contending that public opinion is primarily a top-down process (Bartels, 2000; Lenz, 2013; Zaller, 1992), others emphasize the conditions under which bottom-up processes predominate (Edwards, 2006; Gelpi, 2010; Kertzer and Zeitzoff, 2017; Levendusky and Horowitz, 2012). For example, in Western democracies, it is likely that there are some limitations to how strongly the government can control public opinion, particularly on issues that are familiar to the public (Canes-Wrone and Shotts, 2004), when elections are close (Canes-Wrone and Shotts, 2004), and when their is a robust opposition and independent media (Baum and Potter, 2015). And, indeed, recent empirical studies of legislator behavior (Saeki, 2013) have found that legislators are, in fact, much more likely to shift their ideology in response to voters than are voters in response to their legislators.

Together, this body of literature suggests that, though public opinion is often shaped and molded by political elites, general attitudes about political issues can be principled (Kertzer et al., 2014) and arise organically in a bottom-up fashion as citizens react cognitively and emotionally to political events (Wayne, 2018). These attitudes thus form the political climate in which politicians then operate. If the public is *already* broadly concerned or in favor or expansive policies in a certain issue area, it becomes easier for politicians to invest effort in that area. On the other hand, if the public is less concerned about a given threat (or even actively opposed to certain measures), it becomes costlier for politicians aiming to change the status quo. Thus, leaders are, on the one hand, constrained by public opinion, but they also have significant power to channel public opinion into a range of different potential policies.

Recent national polls in the United States can shed some light on these public opinion processes and help inform our hypotheses regarding how citizens will likely respond to new cyber threats. First, overall cyber knowledge appears to be relatively low, at least in the American electorate. A 2017 PEW poll found that the median respondent was able to correctly answer only 5 out of 13 cyber knowledge questions, and fewer than 20% were able to correctly answer more than half (Olmstead and Smith, 2017*b*). At the same time, the American public does tend to believe that a major cyber operation against the United States will be coming in the next five years — against national infrastructure (70%) or the banking system (66%) (Olmstead and Smith, 2017*a*). This finding is mirrored globally — in 2016, 51% of respondents across 38 countries named cyber operations as an important threat to their country, just behind ISIS (62%) and climate change (61%) (Poushter and Manevich, 2017). However, at the same time, a full 69% of U.S. adults say they are not at all worried about how secure their *own* online accounts are (Olmstead and Smith, 2017*a*). This disconnect is striking — citizens appear to believe cybersecurity is a major national threat, but not necessarily a threat *to them*.

This mirrors recent work from the field of information studies that has begun to touch on the contradictory attitudes individuals possess with regards to their computer use and the safety of their private information online. For instance, Norberg, Horne and Horne (2007) demonstrate that, even though people complain about the inability to control their personal information, they often freely disclose it. Other research has found that individuals' views on personal privacy trade-offs are relatively malleable and dependent on the specific context (Acquisti, Brandimarte and Loewenstein, 2015). We contend that the contradictory nature of citizens' attitudes and behavior toward cyber, hinted at in this nascent literature and recent public opinion polls, is driven by two factors: lack of basic cybersecurity knowledge, and the ways in which certain types of cyber operations — but not others — engage the dread and uncertainty dimensions central to risk perception (Slovic, 2016).

Indeed, there appears to be important emotional mechanisms underlying citizens' threat perceptions surrounding cyber operations. Exposure to very specific stories about acts of cyberterrorism have been shown to increase anxiety (Jarvis, Macdonald and Whiting, 2017). Some politically motivated cyber operations have even been shown to cause as much emotional distress as typical physical terrorist violence (Canetti, Gross and Waismel-Manor, 2016) and can lead to a hardening of militant political attitudes in conflict contexts. Essentially, when cyber operations *do* elicit fear and dread, they can alter both information processing and political attitudes. However, the direction of this effect is unclear: research on public opinion and voting behavior suggests that fear can promote increased vigilance and information search (Marcus, Neuman and MacKuen, 2000). As such, fear could motivate individuals to engage in safer online practices. On the other hand, this fear and anxiety can represent a significant barrier to individuals' ability to process new information and stay informed about cyber threats (Cheung-Blunden and Ju, 2015), leading individuals to shut down and adopt a fatalistic attitude towards their cybersecurity (Lawson et al., 2016). Thus, in the absence of personal efficacy, information about cyber threat may simply demobilize citizens.

In the present study, we examine the conditions under which cyber operations increase these perceptions of personal risk and the downstream effect this has on citizens' personal behavior and political attitudes. We contend that exposure to information about cyber threats may improve personal online safety, when this information communicates to citizens that a) they may be *personally impacted* by the threat, and, importantly, b) that they have some *influence or control* in reducing their risk. Thus, this research bridges together findings from historically separate research traditions, integrating work on risk perception in international relations with work on cybersecurity, public opinion, and information studies to examine 1) what citizens know about cybersecurity; 2) how they assess cyber risk; 3) how it affects personal online behavior; and 4) support for government cybersecurity policies.

3 Defining Cyber Operations

The world of cyber operations is incredibly broad and varied. Thus, before proceeding to our study, we provide a brief typology of existing definitions of cyber operations and clarify which are the primary focus of the present study.

While several existing classification of cyber operations mainly emphasize goals,[12] we focus on both the motives *and* effects associated with various types of cyber operations. Specifically, we distinguish between *political* and *criminal* goals of cyber operations and, using Valeriano and Maness 2015's classification, we focus on three primary effects – *disruption*, *degradation* and *manipulation*.

Disruption operations prevent the main activities and processes of an online system from operating. Often, these operations attempt to flood systems with requests in order to overload a server and cause it to temporarily shutdown. For example, during the 2015 attacks

[12] For example, Rid 2013 focus on sabotage, espionage, and subversion; and Cavelty 2010; Denning 2001 distinguish activism, hacktivism, cyber terrorism, and cyber warfare.

Table 1: TYPOLOGY OF CYBER OPERATIONS

		Goal/Objective		
		Political	*Criminal*	*Both*
Effect	*Collect/Manipulate*	e.g., Flame and Red October (discovered in 2012), U.S. Office of Personnel Management (OPM) hack (2015), early stages of attacks against power grids in Ukraine (2015, 2016)	e.g., attacks against Target Corporation (2013)	e.g., early stages of WannaCry (2017)
	Disrupt	e.g., attacks against Estonia (2007) and Georgia (2008)	e.g., various ransomware operations (e.g., CryptoLocker)	e.g., WannaCry (2017)
	Degrade/Destroy	e.g., Stuxnet (discovered in 2010), attacks against power grids in Ukraine (2015, 2016)		

against Ukrainian power grids, the perpetrators flooded telephones of customer call centers with phone calls to prevent customers from calling in to report the outage (Zetter, 2016). Politically, these phone- or web-based distributed denial-of-service (DDoS) strikes – the simplest and most commonly used tool in this category – have become a popular tool of government censorship (Deibert and Rohozinski, 2010; King, Pan and Roberts, 2013; MacKinnon, 2013) and contention for protesters (Asal et al., 2016). The international network of activists and hacktivists *Anonymous*, for instance, is well-known for executing DDoS operations on government, religious, and corporate websites to protest policies. But disruption operations can often be *criminally* motivated, with ransomware operations being a primary example. Ports that host online games are often the primary target of these DDoS operations. In these operations, hackers hold the port "hostage" until users pay a ransom to regain access to their accounts. Sometimes such disruption operations have *both* political and criminal goals. For instance, the 2017 WannaCry ransomware operation, attributed to the North Korean government, targeted computers running the Microsoft Windows operating systems by encrypting data and demanding ransom payments to, most likely, sponsor the government's nuclear program (Nakashima, 2017).

Degradation operations use malicious code to inflict physical damage or permanently compromise the use of a given system. Because these operations are costly and complicated, the primary goals of such operations are often political.[13] In this category, the Stuxnet worm launched by Israel is a primary example (Sanger, 2012). First discovered in 2010 by Kaspersky Labs, Stuxnet is often described as the first "cyber weapon," because it caused substantial dam-

[13] Some examples of these political goals include (1) increasing the cost of achieving military objective through destroying or disabling a target's command networks or critical capabilities, (2) eroding an adversary's capability and lowering a probability of its cyber retaliation (Borghard and Lonergan, 2017), and (3) imposing costs through forcing the target to patch vulnerabilities and lowering their reputation (Sharp, 2017).

age to Iran's nuclear program, destroying one-fifth of its nuclear centrifuges (Lindsay, 2013). Stuxnet was the first known cyber attack to actually destroy physical infrastructure, demonstrating how activities in the cyber-sphere can spill over into real world destruction (Kostyuk and Zhukov, 2019). The 2015 and 2016 attacks against the electric power grid in Ukraine that caused power outages throughout the country are another example of degradation operations with political goals. Importantly, these types of degradation operations frequently stem from user error and the security practices of citizens with access to sensitive networks. For example, a careless government or utilities employee who accidentally connects a secure computer to the web to check a personal email or inserts an external USB drive to upload a document may allow hackers a backdoor to enter and destroy vulnerable systems.

The third method of cyber operation involves *data collection and manipulation*. Again, this tool can be used in the pursuit of both political and criminal aims. For example, data breaches are often perpetrated with the goal of espionage or intelligence collection by state agencies. These perpetrators might want to manipulate information to gain offensive and defensive advantage in cyberspace (Gartzke and Lindsay, 2015), influence their targets through propaganda efforts (Lindsay, 2017),[14] or use blackmail to leverage stolen assets for coercive gain (Poznansky and Perkoski, 2018). Data breaches to collect information also often play a central role as part of broader disruption and degradation campaigns. The WannaCry hack and the disruption of Ukrainian power grids, for instance, both would not have been possible without careful digital intelligence collection prior to these campaigns to learn which employees had access to these sensitive systems. On the other hand, other data breaches are designed primarily for monetary gain, enabling hackers to steal identities and, thus, money, from individuals online. The 2013 Target data breach is the example of such operations.

In the present study, we focus on this final category — data collection and manipulation in order to steal online identities. This type of operation can ultimately have criminal or political goals. While criminals would use stolen identities for monetary gain, political adversaries would leverage this data to disrupt political, diplomatic, or national security processes of the state. Politically motivated hackers may even use the information collected from earlier data breaches to launch other disruption and degradation operations. These data breaches, whether

[14] Recent scholarship has intensively studied propaganda campaigns, demonstrating that China (King, Pan and Roberts, 2013, 2017) and Russia (Sanovich et al., 2015) are two leading governments in this regard. For instance, the Russian government has been quite successful in using virtual images of crucified babies and raped women that presumably took place in eastern Ukraine to influence public opinion, both in Ukraine and Russia, during the Ukrainian conflict (Kostyuk and Zhukov, 2019).

criminally or politically motivated, are the most frequently used type of cyber-operation and, as such, constitute a serious threat to the state — harming national economies, undermining confidence in markets, and leading to other security breaches if hacked identities are used as a stepping stone to other more destructive operations.

4 Dimensions of Perceived Cyber Risk

In this research, we develop and test a series of hypotheses regarding the ways in which citizens assess their personal risk from data breaches and how this impacts their policy preferences and personal online behavior. Specifically, we contend that perceptions of personal risk from these cyber operations are relatively *low* in the population, despite growing evidence that data breaches — particularly online identity theft — may present objectively more risk to the average citizen than a host of other concerns citizens frequently reference, such as cyber-attacks on national infrastructure, terrorism and violent crime. We argue that this is due to both low cybersecurity knowledge and because of particular cognitive biases individuals possess when they attempt to calculate probabilities and risk.

Average citizens likely have low knowledge regarding the prevalence of cyber operations, data breaches in particular.[15] This is for multiple reasons. First, because cyber operations are, in general, less covered in the news than other more ′′bloody′′ phenomenon (Gadarian, 2010; Lowry, Nio and Leitner, 2003), citizens may underestimate their frequency. The cyber operations that *are* covered in the news tend to be systematic disruption or degradation attacks against governments or corporations. Individual cases of identity theft simply do not receive as broad of coverage. Thus, citizens may believe that they are not personally likely to be the target of hackers. In other words, citizens may think that they will not personally bear the costs of any data breach, and so be unwilling to sacrifice their own computing efficiency (with complex passwords, etc.) to mitigate their risk. Indeed, in addition to the lack of news coverage, some cyber operations may also be actively covered up by companies or governments who have incentives to hide when a breach has occurred, exacerbating the underreporting of cyber threats. Finally, because most citizens have a low level of political interest and involve-

[15] This lack of cyber knowledge also likely extends to the concrete steps individual citizens can take to prevent their online information from being breached. In other words, unfamiliarity with safe online practices may lead citizens to feel that there is little that they *can* do to obviate their risk, even if they do recognize the risk. In our study, we address this potential explanation by including in our treatment conditions explicit text from cybersecurity experts describing the important role individual users play in protecting their online information, including concrete, easy steps individuals can take in this regard. Thus, differences across treatment conditions is not due to differential knowledge regarding personal efficacy to prevent data breaches.

ment, when these operations *do* make the news, they are less likely to be seen, remembered or attended to (Zaller, 1992).

Just as importantly, the most ubiquitous form of cyber operations also do not engage central dimensions of risk perception that would lead them to be recalled and assessed as dangerous (Slovic, 2016). Thus, research has shown that individuals will over-estimate the risk of threats that elicit a high degree of dread and are perceived as uncontrollable (Slovic, 2016). However, while events such as terror attacks, mass shootings, and other violent crimes possess many of the components that maximize risk perception on both dimensions (Breckenridge and Zimbardo, 2007; Horgan et al., 2004), cyber threats do not. Namely, we argue that, citizens will generally possess a low level of dread and a relatively high belief in their ability to control their exposure, leading individuals to potentially under-estimate cyber risk. This is because much of the suffering that cyber operations seem to bring lacks the pain and persistence of many physical injuries (Canetti, Gross and Waismel-Manor, 2016). For example, terrorist attacks are often catastrophic and fatal; whereas cyber operations, at least to date, have not caused significant physical harm (they are more likely to cause monetary harm). As a result, the damage that cyber operations cause does not trigger "light bulb memory" whereby "emotionally potent events are better remembered than low emotional ones" (Siddiqui and Unsworth, 2011). Essentially, the "dread" factor of cyber operations is lower than those for physical violence. Even though cyber operations can indeed be catastrophic for the individuals involved — destroying their socio-economic well-being or exposing sensitive private information to the world — they are simply not *perceived* as such. Likewise, while terrorist attacks and violent crime are often highly uncertain and uncontrollable, cyber threats appear less so.

Computer usage also provides a veneer of controllability — individuals feel like they are in control of their computers and online accounts in a way that they do not feel in charge of their physical safety in public. This is because individuals use computers from the relative safety and security of their own home and make conscious choices about how they use these devices – setting their own passwords, choosing which websites they visit, and downloading the programs that they find most useful. This feeling of control is central to perceptions of risk (Slovic, 2016). For example, it helps explain why people tend to be so much more scared of planes than automobiles, despite the fact that automobiles are exponentially more dangerous. People feel in control of automobiles – they are in the driver's seat – whereas being a passenger in a plane requires a surrender of control to those they do not necessarily know or trust. Computers possess that same characteristic feeling of control, particularly for those who use computers often in their daily life.[16]

As a result, the way that civilians think about cyber threats versus physical threats may suffer from a form of probability neglect (Sunstein, 2003) whereby individuals "imagine the numerator" (Kahneman, 2011) and forget to think about the denominator — the actual probability that the event will come to pass. This is related to the well-known availability bias (Tversky and Kahneman, 1973), where sensational events are easier to access in memory and, as a result, assessed as more frequent than mundane events that occur with similar or greater frequency. With threats like terrorism, the denominator is very low; with cyber threats, it is actually much higher; it is simply not recalled. In short, low knowledge of cyber threats may lead citizens to underestimate the personal costs, and biases in risk assessment may lead citizens to also underestimate the probability of a data breach that personally threatens them occurring at all. These constitute the core elements of any utility calculation: the costs or benefits of an occurrence multiplied by the probability that the event will occur.

The public's lack of concern or care in cybersecurity has important public policy implications. First, because cyber operations are designed to exploit the weakest link in a system, the individual vulnerability of hundreds of millions of users can aggregate to a major national security risk for the state. For example, the public will frequently make large, ill-advised changes to their personal behavior in the name of avoiding low risks like terrorism — such as driving rather than flying after 9/11, which is estimated to have contributed to 1,600 more traffic fatalities (Gaissmaier and Gigerenzer, 2012) — but few behavioral changes to protect their cybersecurity, such as using more complicated passwords and changing them frequently. Moreover, in democratic states,[17] where public support can be critical for passing budget priorities, the public's lack of attention to even the most common cybersecurity threats could hamper the passage of important cybersecurity legislation. Indeed, public concern about terrorism and

[16] In our study, we measure subjects' relative comfort with computers and find that, on average, comfort is very high. It is conceivable that other populations, for example the elderly, may feel less comfort and, therefore, see computer usage as more risky and uncertain.

[17] In this paper, we restrict our focus to democracies; however, studying this phenomenon in an autocratic context would be very interesting. For one, to the extent that citizens of autocratic states have access to the internet, many of the same challenges of "securing the weakest link in a system" apply for autocratic leaders as for democratic ones. However, individual attitudes would likely be less important in affecting policy formation in these contexts (though see Weeks (2012) for conditions under which autocrats also face domestic audience costs). A third intervening variable in autocratic contexts would be the restrictions those governments often place on their citizenry's ability to use and access online systems, which might mitigate some security concerns for these states, while raising others.

support for costly counter-terror policies, for example, vastly outstrips public concern about cyber and demand for costly cybersecurity policies (Poushter and Manevich, 2017). This potentially creates incentives for elected officials to allocate public budgets away from some of the costlier cybersecurity policies recommended by cybersecurity experts.

However, we contend that exposure to a cyber operation that *personally threatens* the individual may alter these underlying perceptions of personal cost and likelihood, increasing dread and reducing perceptions of controllability, such that citizens become more aware of cyber risks and, with it, become more motivated to address them. Essentially, we hypothesize that individuals may feel more personally vulnerable after experiencing a data breach first-hand. They may learn from the exposure that this sense of security they had in using their computer was, in fact, misplaced. The personal data that they thought they had a high degree of control over is now shown to be very uncontrollable and vulnerable to breach. Moreover, the potential consequences of this breach — economic or reputational loss — are drawn into sharper relief. When they are simultaneously provided with information about how to increase their cybersecurity, they may be more apt to both improve their personal online practices to better protect themselves and support government policies designed to do so as well.

5 Research Design

Getting at these specific mechanisms undergirding citizens' responses to cyber threats requires experimental work to directly test five core hypotheses regarding civilian responses to cyber operations.

5.1 Study Hypotheses

We posit that exposure to a data breach —- particularly one that is personally relevant to the individual — should increase risk perceptions and, when accompanied with information about potential protective actions, change behavior and attitudes. Thus, we expect exposure to a news story about a data breach that compromised an individual's personal information to engender changes in perceptions about personal risk from cyber operations, attitudes toward government cybersecurity policies, and willingness to change personal online behaviors. In contrast, exposure to that same type of cyber operation against a government target is unlikely to move risk perceptions to the same degree because it does not directly engage these two core mechanisms of risk perception. In other words, a hack on the government fits the existing perception that citizens should not personally expect to be victimized, so, does not increase a sense of dread or feeling of uncontrollability.

As such, we have five pre-registered hypotheses.[18] After exposure to a data breach, but particularly after exposure to one that is *personally relevant*, citizens will be more likely to:

- **H1:** *Express a heightened risk to their personal safety and perceived threat from cyber operations*
- **H2:** *Support larger, costlier government policies to defend against cyber operations*
- **H3:** *Report a willingness to engage in cyber-protective behaviors*
- **H4:** *Actually engage in more cyber-protective behaviors*
- **H5:** *Become more wary of (and avoid) future cyber threats*

Moreover, if the causal mechanisms of knowledge, dread, and uncontrollability indeed drive assessments of cyber risk and personal behavior, we would expect the effects of exposure to a cyber operation to be *strongest* among those individuals who were previously low on these dimensions. For example, respondents who knew little about the technology of cyber operations (e.g. had low knowledge), were unconcerned about online privacy (e.g. had low dread) and felt very comfortable with computers or had not previously been the victim of a cyber operation (e.g. felt low uncontrollability) should be the ones whose views were *most* altered by exposure to a cyber operation. Moreover, due to ceiling effects, we would expect those respondents who did not previously engage in safe computer practices to be most likely to improve their personal online hygiene in the wake of exposure to a new cyber threat, rather than those who already engage safe computer practices. We explore these potential interactions at length in Section 6.3.

5.2 Participants

To test these hypotheses, we recruited five hundred and eight students from the University of Michigan (211 males and 268 females), ages ranging from eighteen to fifty-eight ($M = 21.9957$, $SD = 5.95$), to participate in an online study in February, 2017.[19] Respondents were entered into a raffle to win $50 USD for their participation.

[18] EGAP ID: *anonymized*

[19] See details on the study's power analysis and descriptive statistics of the sample in the Supplementary Information. Our final sample consisted of four hundred forty-four participants (199 males and 237 females). Fifty-eight students were omitted from our analyses because they did not finish the study (there is no significant difference in attrition patterns across conditions). Additionally, seven more participants were excluded from our analyses because they fail two of our data checks: 1) they did not answer our attention question correctly; 2) they spent

For this study, using a student sample was important, as it enabled us to tailor a manipulation that we knew would be personally relevant to all participants — a data breach on the university they were attending. Theoretically, understanding how this particular sample of young, college students approaches cybersecurity is also an important question for study, given the high level of Internet usage among this population relative to its size. This is particularly true because this cohort represents the next generation of public- and private-sector professionals who will routinely access systems containing sensitive information throughout their working lives. Poor cyber hygiene within this cohort is thus a disproportionately serious security concern.

Though the student population in this study represents a limitation to generalizability, student samples have often produced similar trends to those found in the general population (Altemeyer, 1996; Druckman and Kam, 2009; Mullinix et al., 2015). Indeed, two recent PEW studies (Olmstead and Smith, 2017*a*,*b*) conducted on representative samples of U.S. adults support our main observational findings, suggesting that our experimental study likely apply beyond a student population. Nonetheless, conducting this type of sample among a representative sample is an important step for future research, and we see our study as an important first test of how cyber risk is evaluated and weighed in the general population.[20]

5.3 Procedure

All participants received a survey in which they were asked to answer several batteries of questions regarding political attitudes potentially associated with cybersecurity risk percep-

less than five seconds reading the article. We omit these respondents in order to conduct a conservative test of any null results we find. The Supplementary Information demonstrates that our results generally hold, even if we include those seven participants in our sample. However, the effect size for planned changes to personal online behavior does become smaller.

[20] If student responses indeed vary from that of a more representative sample, this sample represents a *conservative* test of our theory, since cyber knowledge among this population is arguably much higher than the rest of the population. This is because students from our sample grew up with the Internet always present and are more computer savvy than the older generations (Herring, 2008). Indeed, a 2017 PEW poll (Olmstead and Smith, 2017*a*,*b*) found that age and education were the two most important predictors of cyber knowledge: younger and more educated respondents knew the most about cybersecurity. On each question in their survey, there is at least an 11 percentage point difference in correct answers between the highest- and lowest-educated groups. Likewise, 18- to 29-year-olds correctly answered a mean of 6.0 out of 13 questions, compared with a mean of 5.0 among those 65 and older (Olmstead and Smith, 2017*b*). This means that, to the extent that lower risk perceptions and poor online hygiene are driven by lack of knowledge, our use of a college student sample should bias us toward a null finding — respondents should *already* possess a high level of cyber knowledge, understanding of cyber risk, and practice safer online behavior. Thus, if we see an impact of exposure on risk perceptions, personal behavior and political attitudes in this sample, it is likely that, among other less privileged populations or older respondents who are less familiar with online tools, these effects may be larger.

tions, policy attitudes, and behaviors. Specifically, we assessed subjects' partisanship and ideology, concern about online privacy, comfort with using computers, current computer safety practices, general knowledge of cyber terminology and high-profile cyber operations, and any prior experiences of being a victim of hacking.

Participants were then randomly assigned either to a control, national, or personal condition. In the national scenario, participants were asked to read a fictional article (that they thought was genuine) about a cyber-hack of the U.S. Navy that compromised the private information of thousands of servicemen and took place a few days prior to the day of the survey. In the personal scenario, participants were asked to read a fictional article (that they thought was genuine) about a cyber operation against the university that they were attending (University of Michigan).[21] As a result of this breach, students' record and ID numbers were stolen.[22] After reading the article, the students were asked a battery of questions about the threat from cyber operations, their evaluation of government's cybersecurity policies and their online behavior.[23]

To ensure that participants understand not just the *threat*, but also potential solutions to reduce the risk of data breaches, we include quotes from a cybersecurity expert, listing specific strategies consumers can use to protect themselves online, including using different passwords for different accounts, updating passwords every 30 days, and enabling two-factor authentication, which will tip a user off anytime someone is trying to log on to their account from a new device. The cybersecurity expert also highlights national cybersecurity policies that would be effective in reducing the probability of breaches, such as the need to re-recruit cyber-security experts who have been recruited away from government work by the comparatively higher salaries offered in the private sector, the importance of partnerships both between governments internationally and between the public and private sector, a centralized cyber-response force and more investment in cyber-security education.[24]

[21] Importantly, the experimental treatment is designed to appear like a real news story. Subjects thus believe this is an event that has actually occurred (and are subsequently debriefed). This simulation of a real news story is a crucial aspect of the experimental design and significant time was spent designing the articles so that the "look and feel" matched that of real online news stories subjects would routinely read.

[22] Thus, subjects are led to believe they may pay personal costs due to this breach, in the form of potential identity theft. To the extent that this "personal cost" is smaller than that experienced in the real world (e.g., respondents may feel that the likelihood that their user information will be chosen by the hackers is still very low), this means that our treatment is a *conservative* estimate of the role of personal threat in shaping changes in cybersecurity behavior. In the "real" world, where individuals actually experience the downstream consequences of, for example, having their identity stolen, any effect on risk perception or behavior is likely to be further amplified.

[23] The full survey instrument is located in the Supplementary Information.

[24] Thus, subjects in *both* treatment arms received this information about the steps they and their government could take to improve online safety. This suggests that any differences in stated willingness to change behavior or

In the control condition, respondents did not read any news story about a new data breach and proceeded directly to the dependent variables. These dependent variables included perceptions of the national and personal risk from cyber operations, willingness to engage in safer online practices, and support for a variety of state cybersecurity policies.

After respondents completed their survey forms, they saw a debrief message on screen that informed them the study was complete, but did not yet tell them that the news story they read was false. Later that evening, we sent a follow-up email to all participants, thanking them for their participation in our study and providing them with several resources written for individuals to learn more about how to protect themselves online. The email contained a title and four short blurbs with five links they could access to read additional information. Then, we matched up respondents' email addresses with their original survey form (for which they input their email in order to enter into a prize raffle) to monitor who opened this email and how many links the individual clicked on within this email. Thus, we were able to ascertain the impact of the manipulation on respondents' actual willingness to read more about tools for protecting their online security a real-world behavioral outcome.

The next morning, we emailed all participants, using a different email address (specifically created for this purpose) that contained a spam message informing them that they were about to receive an inheritance, once they provided their personal information.[25] We were also able to monitor who opened this email and who responded to the provided email address. Then, we matched up respondents' email addresses with their original survey form in order to see if the manipulation affected respondents' susceptibility to this type of online scam. Several hours later, all subjects received an actual debrief message — indicating that the news article they read the previous day was fictional and that both email messages had been a part of the study.[26]

5.4 Measures

As we describe above, we expect that predispositions may interact with our treatment to affect how exposure to cyber operations changes attitudes and behavior. Namely, subjects' political predispositions and their familiarity and knowledge of cyber issues is likely to have

support for government cybersecurity policies between the two treated conditions are not driven by knowledge gaps persay, but, rather, the exposure to a personally relevant cyber-operation or not.

[25] The text of these emails are in the Supplementary Information.

[26] At this point, all identifying information from participants was removed from our dataset.

a strong effect on how powerful exposure to a new cyber threat is on changing their political views and personal behavior. To this end, we included several covariates in our study, using both previously validated and newly constructed scales to assess each attribute. For each variable, full measurement details are available in the Supplementary Information.

First, we expect that support for various cybersecurity policies may affect respondents differently based on their ideology and partisanship. *Ideology* was assessed using a 7-point scale from the American National Election Study, ranging from extremely liberal (1) to extremely conservative (7). *Party Identification* was assessed using a two-part question used in the American National Election Study to assess party identification on a 7-point scale from strong Democrat to strong Republican.

Next, subjects who already espouse a strong concern for online privacy may already experience significantly higher *dread* of a future cyber threat than those who are less concerned about this issue. Thus, we expect that those with few privacy concerns at baseline are most likely to express heightened risk perceptions after exposure to a new cyber threat. To measure these *Privacy Concerns*, we used a six-question agree-disagree scale that measures respondents' concerns about government surveillance (Dinev, Hart and Mullen, 2008) ($\alpha = 0.85$). A high score on this scale represents individuals' higher level of concerns about government violating their privacy, while a low score represents an individual's support of government surveillance. This variable is also important to measure because it is conceivable that a significant segment of the population is more worried about *government* hacking than *criminal* or *non-state actor* hacking, in which case they may engage in very safe personal online behavior, but still be unwilling to support cybersecurity policies that potentially give the government more power.

Likewise, respondents that already engage in high levels of computer safety are expected to express a higher baseline perceived risk from cyber and, as a result, be less moved by exposure to an additional threat. To measure *Computer Safety*, we use an eight-question scale (Egelman and Peer, 2015) ($\alpha = 0.62$). A high score on this scale represents individuals' more secure/careful online behavior. This *ex ante* level of computer safety may cause heterogeneity in the effect of exposure to a new cyber threat: namely, those who already engage in safe computer practices may be less likely to shift their beliefs or practices in response to a new threat.

Third, we expected that subjects who express a high level of comfort with computers feel a higher degree of *controllability* over their online safety. As a result, subjects with a high degree of comfort should be most likely to have their beliefs changed, and express heightened risk perceptions, once they are exposed to a cyber operation. *Comfort with Computers* measures these attitudes towards computers using an eight-item bi-polar scale developed by Shaft, Sharfman and Wu 2004 ($\alpha = 0.75$). A high score on this scale represents individuals' high level of comfort using computers.

Fourth, subjects with a low baseline knowledge of how cyber operations are launched are likely to *know the least* regarding future possible cyber operations, prior to treatment. Thus, we expect that those with the lowest baseline knowledge of cyber-terminology will be most likely to express heightened risk perceptions after exposure to a threat. To test this idea, we use a newly developed battery of questions in which we ask respondents two types of questions to assess *Cyber Knowledge*: 1) knowledge of recent real-world cyber operations (e.g. Stuxnet virus, Sony Pictures Hack, WikiLeaks); and 2) familiarity with different types of cyber operations and what they do (for example, what a DDoS is, what phishing means, how to define a Trojan Horse). A high score on this scale represents individuals' better familiarity with cyber operations and cyber terminology ($\alpha = 0.70$).[27]

We also measure *Previous Exposure to Cyber Operations*, asking respondents if (to their knowledge) they had ever had their online accounts hacked, had their computer infected with a virus, or had their personal information stolen. Respondents with prior experience of cyber operations may already be hyper-aware of the threat as compared to respondents with no past history of being victimized online.

Moving to our dependent variables, we have three concepts of interest: 1) threat or risk perceptions, 2) personal security behaviors; and 3) policy preferences. We operationalize each as follows:

First, we measure individuals' *Threat Perception*, using four questions. Subjects were asked to estimate the likelihood of 1) cyber-attacks against the U.S. government or infrastructure happening in the next year; 2) cyber-attacks against average American citizens happening in the next year; 3) they or someone they know being a victim of cyber-attacks in the next year; and 4) ”the risk posed to their or their family's well-being” from a host of potential public health threats: gun violence, terrorism, heart disease, cancer, natural disasters, traffic accidents, cyber-attacks, or military conflict with nuclear powers. To the extent that exposure to

[27] We also create two sub-scales, since knowledge about types of cyber operations versus real-world examples are potentially theoretically distinct constructs, but these scales have lower reliability (current events $\alpha = 0.48$, terminology $\alpha = 0.57$).

a personally relevant attacks heightens knowledge, dread, and the perceived uncontrollability of cyber-attacks, these threat perceptions should increase after exposure.[28]

Next, our *Policy Scale* measures an individual's preferences for various potential cybersecurity policies that have been suggested by national security professionals. We asked a series of six newly developed questions regarding potential policy responses that the government could engage in with regards to cyber threats, all of which are costlier than the status quo (on some dimension) and all of which have been recommended by cybersecurity experts. We also asked a separate question regarding cybersecurity spending, whether (and by how much) it should be increased or decreased. We expect support for these policies to increase after exposure due to increased risk perceptions.[29]

Third, our *Online Behaviors* scale measures whether exposure to cyber threats increased citizens' willingness to engage in costly or time-consuming cyber-protective behaviors. To assess this question, we asked seven questions, developed based on recommendations from cybersecurity professionals. A high score on this scale represents individuals' higher willingness to engage in safe online behavior ($\alpha = 0.65$). Here too, we expect willingness to engage in these behaviors to increase after exposure due to increased risk perceptions.

Our final dependent variable is actual *Cyber-Protective Behavior.* Thus far, the experiment is designed as a lab experiment with attitudinal measures — subjects realize they are participating in a study and are answering attitudinal and hypothetical behavioral questions accordingly. However, we are also interested in seeing exposure to a news story about a type of cyber operation can impact real future behavior, outside of the context of the lab experiment. Our behavioral outcome thus tracks 1) whether subjects opened our email about security tips online and how many links they clicked to find out more information; and 2) whether subjects opened or responded to our ''spam" email sent from a fake email address. These measures thus track actual behavioral outcomes outside of the lab setting.

[28] In the phrasing of the survey, we employ the term cyber attack rather than cyber operation, as this lay terminology is more accessible to an average survey respondent. In the context of the survey, we thus believe respondents interpret the phrase "cyber-attack" broadly, to include data breaches.

[29] In our analyses, we assess each of these policies both separately and as part of a scale ($\alpha = 0.66$). We do this because it is possible that support for policies designed specifically to address the threat of data breaches may be particularly moved by our experimental treatment. However, we do not find substantial differences across different policies. See the Supplementary Information.

6 Results

Analysis for this study proceeds in three stages: 1) basic descriptive statistics of the sample to establish baseline attitudes and knowledge surrounding cyber issues; 2) regression analysis of the main effects of the manipulation; and 3) an exploration of heterogeneous treatment effects of exposure based on preexisting cyber attitudes and behaviors. Below, we go into detail regarding each of these stages.

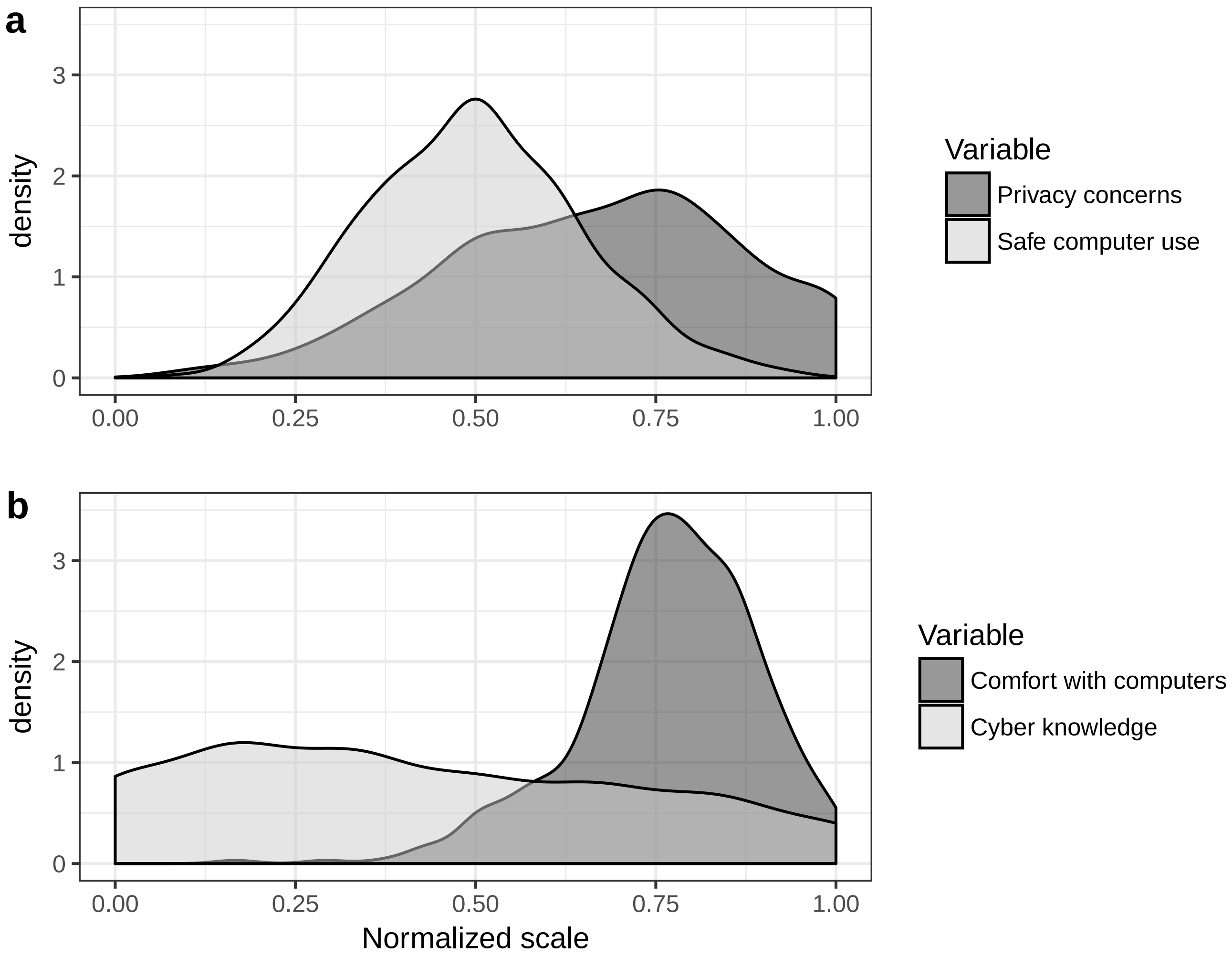
6.1 Descriptive Statistics and Correlations between Variables

To begin, we present basic descriptive statistics of the levels of cyber knowledge and sophistication of our sample. This is valuable in and of itself because little is known about how literate the mass public is on issues of cybersecurity and computer safety.[30]

Respondents were, in general, relatively concerned about privacy online and surveillance, perhaps stemming from, among other things, the 2013 Snowden revelations about the U.S. government spying on its citizens. However, on the other hand, respondents were only moderately likely to engage in common computer safety strategies recommended by experts (Figure 1). Thus, there is a striking disconnect between stated concern and actual action to address those concerns. Likewise, despite being comfortable and actually enjoying using computers, 54.2% of the sample had very limited knowledge of cyber terminology and of current events related to cybersecurity (Figure 1). This suggests that respondents *think* they are more sophisticated computers users than they actually *are*.

[30] Though see the recent PEW studies published after our study was conducted (Olmstead and Smith, 2017*a*,*b*).

Figure 1: Attitudes & Knowledge toward Cyber Issues



These descriptive statistics highlight the paradox of cybersecurity highlighted above: subjects report high levels of concern about their online privacy, but feel very comfortable in their computer usage — despite knowing little about cyber operations and taking little action to protect themselves online. Indeed, 42% of our sample indicated they had an online account hacked in the past and 64% they had previous had a computer virus and 21% reported that they had had their personal information stolen.[31]

6.2 Main Effects

While this general information about computer literacy and online safety habits in our sample is important, the core contribution of this paper focuses on the impact of exposure to a *new*

[31] We also examine the correlations between our various moderators and dependent variables in the Supplementary Information.

cyber threat on subsequent perceptions of risk, behavior and political attitudes. This section summarizes these main effects in detail. The main effect analysis uses the following model:

$$Y_i = \alpha + \beta_1(T_i) + \epsilon_i, \tag{1}$$

Y_i denotes the outcome variable of interest *risk perceptions, policy preferences, and personal cybersecurity behaviors*. $\beta_1(T_i)$ denotes the estimate of the average treatment effect; α is the effect of the omitted condition; and ϵ_i is the error term.

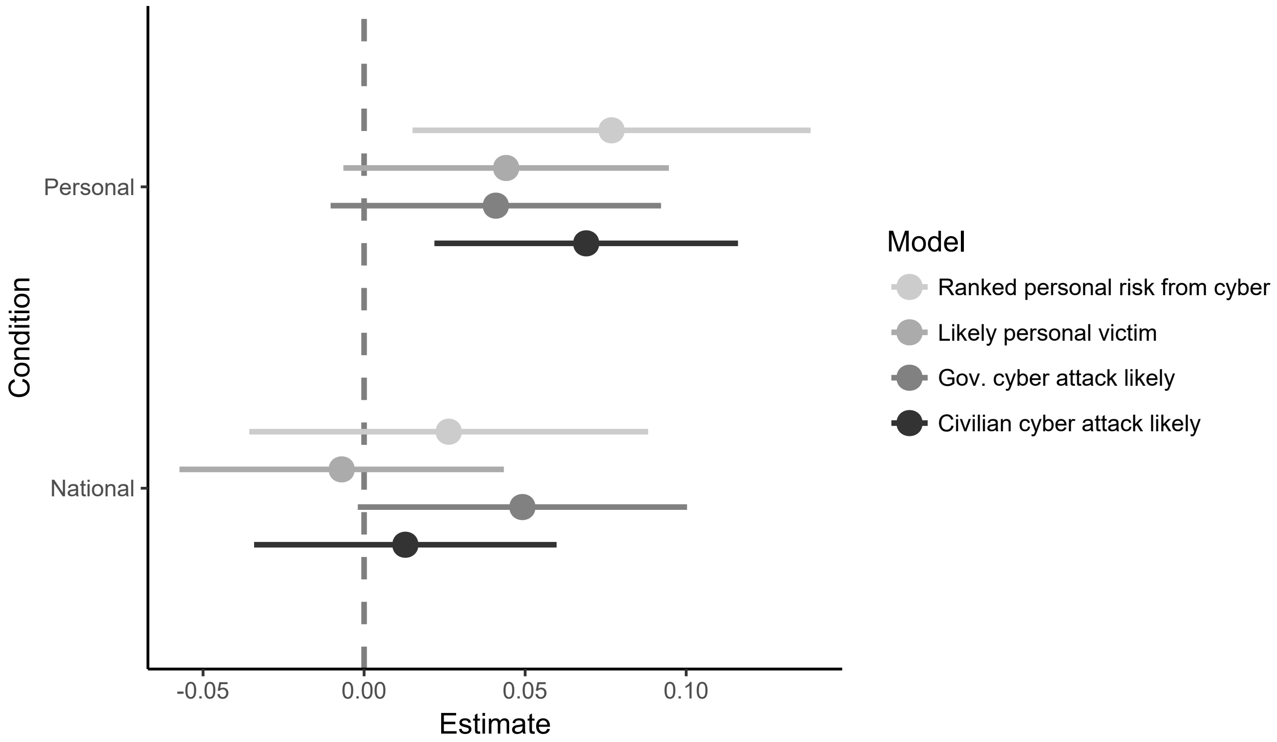
To begin, Figure 2 demonstrates that, as compared to respondents in the control, respondents in the national (but not personal) threat condition are marginally more likely to believe that another attack against the United States *government* will happen in the next year.[32] Likewise, as compared to respondents in the control condition, respondents in the personal (but not national) threat condition are significantly more likely to believe that another attack against *average citizens* of the United States will happen in the next year. Essentially, subjects are more likely to believe that an attack *similar to the one that just occurred* will happen in the future, but do not extrapolate from one type of threat to another.

Next, we examined whether exposure to a cyber operation could alter respondents' *personal* perceptions of threat. We found that, as compared to respondents in the control condition, respondents in the personal threat condition were marginally more likely to believe that they personally would be the victim of a cyber operation in the next year. Respondents in the personal threat condition were also significantly more likely to rank being the victim of a cyber operation as a higher personal risk, when compared to other risks such as terrorism, gun violence, or diseases like heart disease and cancer.[33] Respondents in the national threat condition were no more likely to believe that they personally would be the victim of a cyber operation in the next year or to rank being the victim of a cyber operation as a higher personal risk (Figure 2).

[32] We provide tables with coefficients in the Supplementary Information.

[33] Respondents in the personal threat condition mean rank of cyber threats was 3.99 on a scale from 1-8. In the control condition, the mean was 4.50 and in the national threat condition, 4.33. Thus, this shift is substantively large: a 6.25% change in ranking.

Figure 2: Changes in Perceived Cybesecurity Risk



In other words, a data breach that personally affected the individual impacted perceptions of future risk much more than a hack perpetrated against the government. This is striking since an operation on government databases arguably demonstrates higher capacity of the hackers to launch cyber operations in the future. But respondents do not appear to see it this way — they care more about who was attacked, rather than how difficult the operation may have been to perpetrate.

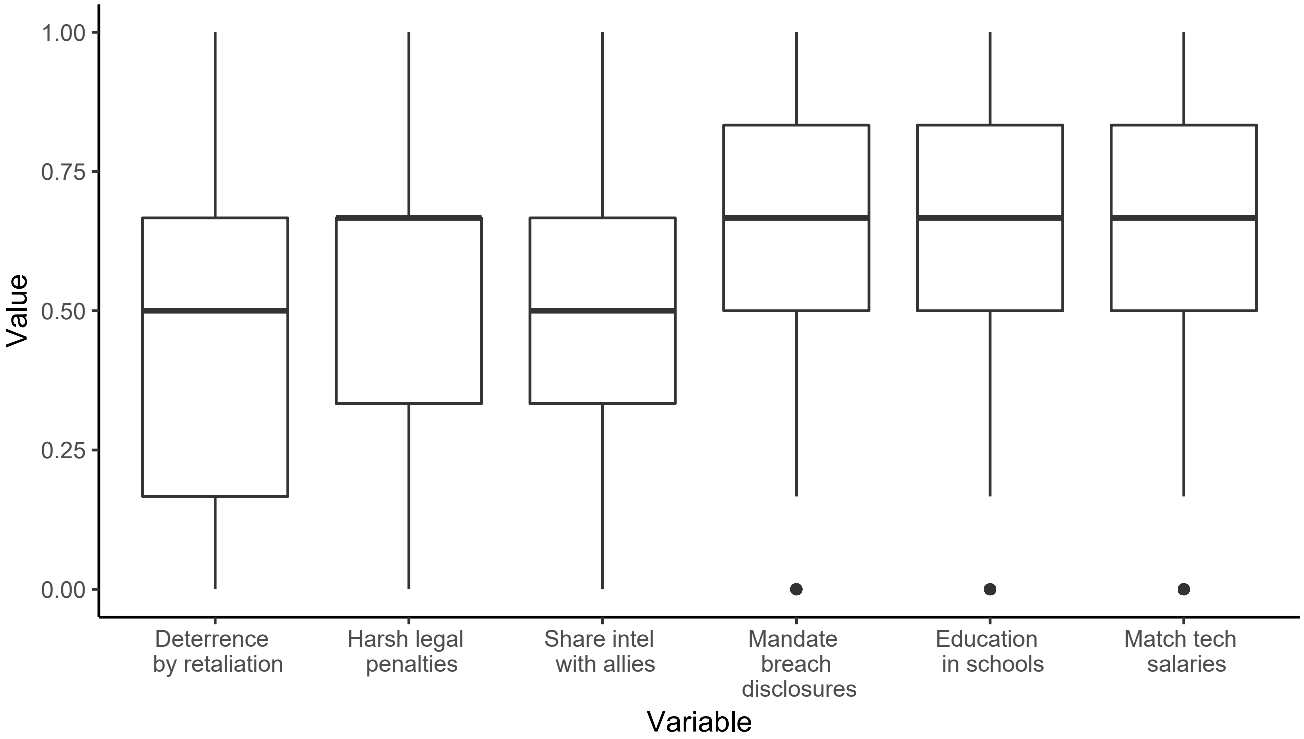
But what effect does this exposure and increased threat perception have on actual political attitudes? Surprisingly, not very much. As compared to respondents in the control condition, respondents in both the national and personal threat conditions were significantly more likely to support higher government spending on cybersecurity programs.[34] However, surprisingly, while support for cybersecurity *spending* was altered by exposure to new cyber threats, there was no effect of exposure on which *types* of cybersecurity policies respondents supported. In other words, we find that respondents in both the personal and national threat conditions were no more likely to support any of the specific cybersecurity policies suggested by experts.[35]

[34] See Tables 18 and 19 in the Supplementary Information.

[35] We assessed these policies each individually and collectively as a scale. See the Supplementary Information for full regression tables.

However, the mean level of support for different cybersecurity policies does reveal some important insights into respondents' attitudes towards these different proposals (Figure 3). First, support for each of these policies is not politicized. Of the eight policies tested, only one — sharing cyber intelligence with other allied nations — was significantly different support among Democrats and Republicans (Democrats were more supportive).[36] This is likely due to the 2016 news cycle, which focused heavily on the evidence the intelligence community had regarding cyber intrusion by Russia into the 2016 election, polarizing the electorate on this issue. Second, many of these policies already have broad support, despite their potential costs. For example, mandating disclosures by companies when a cyber breach has occurred, matching tech salaries in government hiring of computer experts, and diverting a portion of the education budget to cyber education in schools all received an average level support above 0.6 (on a $0-1$ scale). Respondents were more wary regarding retaliation by the United States against cyber operations by other states ($M = 0.48$) and of sharing cyber intelligence with allies ($M = 0.49$). Creating harsher legal penalties for cyber hacking received middling support ($M = 0.57$).

Figure 3: Distribution of Support for Cybersecurity Policies



[36] The regression tables illustrating these results are available in the Supplementary Information.

Finally, we found that, as compared to respondents in the control condition, respondents in the personal threat condition were marginally more likely to report that they would engage in a variety of safer online security behaviors (Table 2). Respondents in the national threat condition were, in contrast, no more likely to report a willingness to engage in safer online practices. Again, this result suggests that it is the personal relevance embodied in the exposure to a data breach that has the potential to change future behavior. Breaches of other targets simply do not have the same personal resonance.

However, though subjects in the personal threat condition *said* they would engage in safer online behaviors, they were, in fact, no more likely to seek out information on cybersecurity in response to our follow-up email (by opening the email or clicking the links) and were no less susceptible to spamming attempts.[37] This suggests that simple exposure to a cyber operation may not be enough to change actual online behavior, even if citizens' perception of risk was temporarily heightened and they expressed a willingness to change their behavior (see Table 2).

Table 2: Changes to Personal Online Behavior

	Willingness to Use Safer Online Behavior	**Open Email with Info about Online Security**	**Click Links to Access Info on Online Security**	**Susceptibility to Spam Email**
National	0.002	$-0.096^{\wedge}$	0.029	-0.005
	(0.023)	(0.052)	(0.031)	(0.048)
Personal	$0.040^{\wedge}$	0.012	-0.005	0.090
	(0.023)	(0.052)	(0.031)	(0.057)
Constant	0.457^{**}	0.753^{**}	0.067^{**}	0.180^{**}
	(0.016)	(0.036)	(0.022)	(0.032)
Observations	397	441	441	350
R^2	0.010	0.012	0.003	0.009
Adjusted R^2	0.005	0.007	-0.001	0.003
Residual Std. Error	0.184 (df = 394)	0.445 (df = 438)	0.264 (df = 438)	0.398 (df = 347)
F Statistic	1.913 (df = 2; 394)	$2.581^{\wedge}$ (df = 2; 438)	0.708 (df = 2; 438)	1.592 (df = 2; 347)

$^{\wedge}p<0.1$; $^{*}p<0.05$; $^{**}p<0.01$

[37] Interestingly, those subjects in the national threat condition were marginally *less* likely than those in the control to seek out information about online safety, perhaps because the data breach reinforced the perception that average citizens were not the target of data breaches.

6.3 Heterogeneous Treatment Effects

Finally, we turned to investigate potential heterogeneous effects of treatment based on preexisting behaviors and attitude structures. In particular, we explore four key potential sources of heterogeneity, all of which may impact our hypothesized causal mechanisms, existing knowledge about cybersecurity and the degree to which individuals feel dread and a sense of uncontrollability regarding cyber operations: 1) how concerned individuals are about privacy and surveillance online, 2) how comfortable they are with computers, 3) previous experience with a cyber-hack, and 4) whether they *already* practice cyber-hygiene.[38] We capture these effects using a model with interaction terms as follows:

$$Y_i = \alpha + \beta_1(T_i) + \beta_2(\gamma_i) + \beta_3[(T_i) * (\gamma_i)] + \epsilon_i,$$

In this regression, a moderator γ_i and an interaction term of the moderator and treatment condition $[(T_i) * (\gamma_i)]$ are introduced. If the interaction term β_3 is significant, marginal effects plots can then be used to make substantive interpretations regarding who is driving the treatment effect most — those high or low in γ_i.

We explore five potential heterogeneous treatment effects. If the causal mechanisms of knowledge, dread, and uncontrollability drive assessments of cyber risk and personal behavior, we expect the increase in personal risk perception from cyber operations[39] to be *largest* among those individuals who were previously 1) low in *Cyber Knowledge*; 2) low in *Privacy Concern*; 3) low in *Computer Safety*; 4) high in *Comfort with Computers*; and 5) with less *Previous Exposure to Cyber Operations*.

First, we expect that those with low knowledge about cybersecurity issues were previously less aware of the threat from cyber operations. Thus, they would likely have a lower perceived risk from cyber operations prior to treatment. Moreover, subjects who are less concerned about online privacy likely experience lower dread at the possibility of a data breach before they are exposed to our treatment. Exposure to this new threat to their online security should thus be more effective at changing views among this population. Third, those who are most comfort-

[38] There are, of course, other potential sources of heterogeneity in how individuals assess cyber-risk that might be interesting to explore in future studies, such as IQ, numeracy, and sensitivity to emotive imagery. Exploring more of these individual differences is an important step for future research.

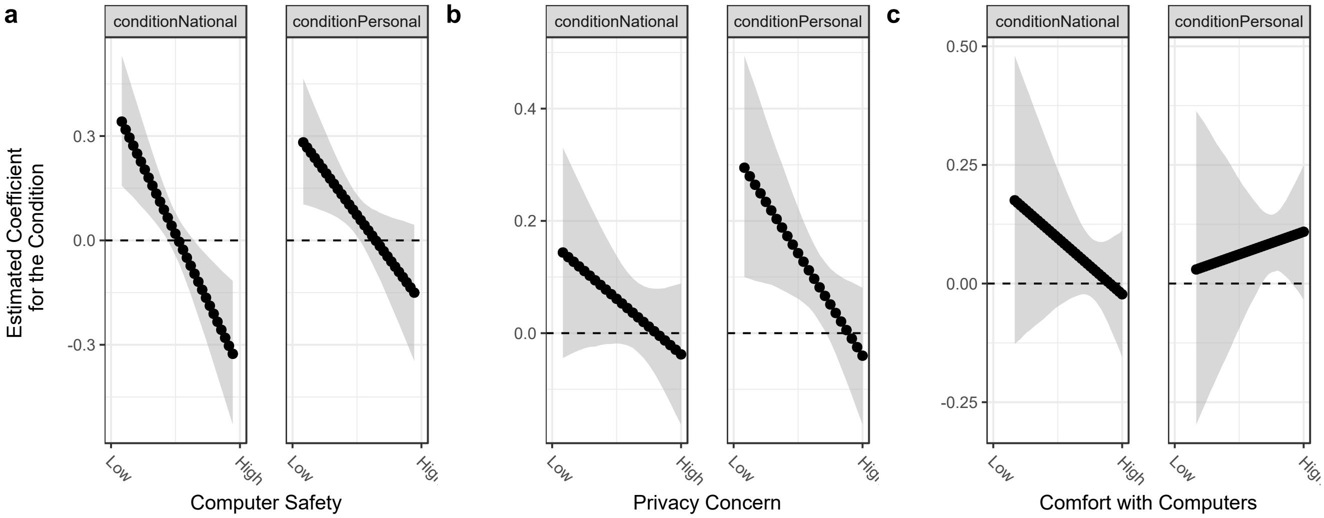
[39] Operationalized here as individuals' ranked personal risk from cyber operations versus other public health considerations.

able with computers feel a high degree of controllability over their online safety and should thus be most moved by exposure to a data breach (e.g., they would experience the largest shock to their preexisting beliefs). Fourth, we expect those who have been previously exposed to a cyber operation to *already* feel a high degree of dread regarding cyber operations, and so be less affected by exposure to *another* data breach. Finally, those subjects who already engage in safe computer usage will likely show less change in behavior after exposure to a new threat due to a a ceiling effect.

The results largely support these hypotheses and are illustrated in Figures 4 and 5. On the one hand, those who engaged in the *least* safe computer practices prior to exposure to treatment were indeed the most likely to report an increased perceived personal risk from cyber after reading about both types of data breaches. Likewise, those who were the least concerned about privacy and surveillance online prior to treatment were also more likely to report heightened risk perceptions.[40] Thus, those who possessed relatively low dread prior to treatment appeared most likely to shift their views after witnessing a new threat.

However, comfort with computers — which we argue proxies for a high sense of controllability over online activities — did not have any interactive effect with treatment on threat perceptions. This may be due to the high level of computer comfort reported by our sample overall (e.g., there was little variation in users' reported comfort with computers).

Figure 4: Dread, Controllability, & Exposure on Perceived Personal Risk from Cyber



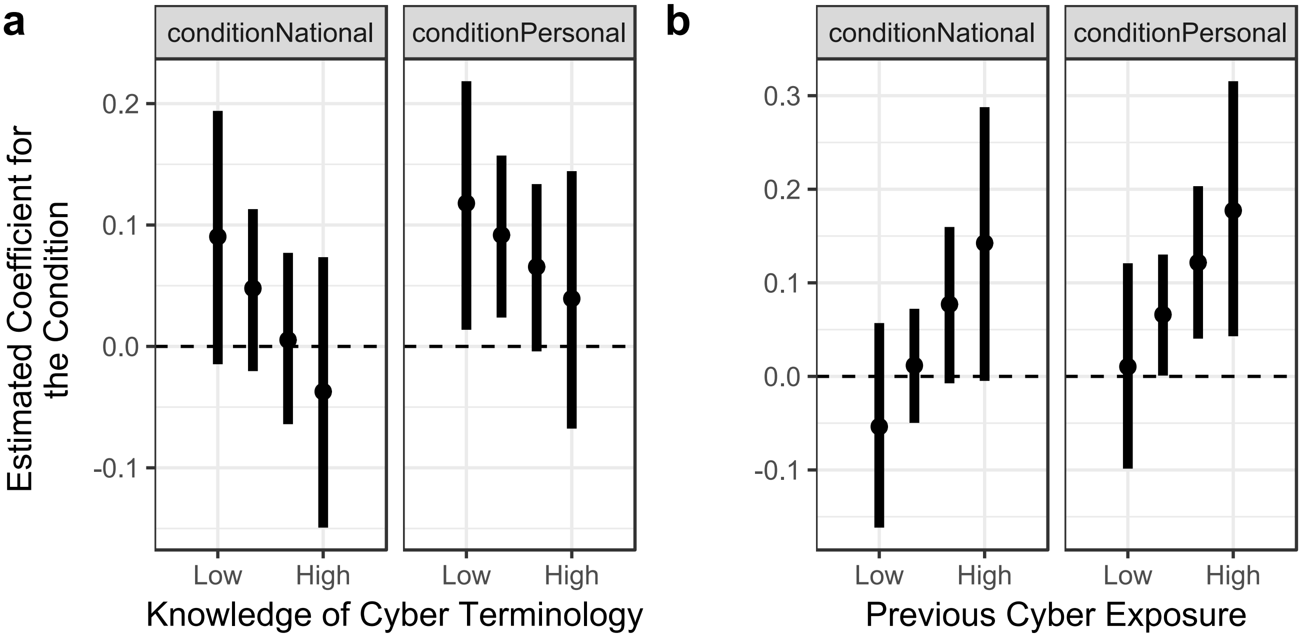
Turning to examine the impact of familiarity with cyber terminology or previous exposure to

[40] This interaction was significant only in the personal threat condition.

cyber operations (e.g., existing knowledge about risk to cybersecurity), we also find support for our hypothesized interaction. Those who were already able to identify different types of cyber operations (including phishing, distributed denial of service (DDoS), and a Trojan horse), were less likely to increase their risk estimates after exposure to a personal threat than were those who knew little about these types of cyber operations.

On the other hand, in contrast to our expectations, those who had previous personal experience with cyber operations (having their computer infected with a virus, having their accounts hacked, or their identity stolen) had even *more* heightened risk perceptions with those who had no previous experience with cyber operations, in contrast to our expectations. This finding suggests that exposure to cyber threats compounds preexisting risk perceptions. Each new cyber operation may further crystallize an individual's feeling of personal vulnerability and solidify a heightened sense of risk.

Figure 5: Cyber Knowledge & Exposure on Perceived Personal Risk from Cyber



7 Discussion and Implications

This study has revealed several important patterns in both citizens' baseline cyber knowledge, perceptions, and behaviors and in their responses to exposure to a new cyber threat. To begin, we find that knowledge about cyber issues and the use of basic computer safety practices is quite low. However, exposure to a *personally relevant* data breach leads to significantly higher perceptions of personal risk from hacking. In turn, subjects exposed to a data breach on their institution become at least marginally more likely to express a willingness to engage in safer online behaviors in the future. However, though subjects expressed a *willingness* to engage in safer online behavior, their actual online behavior remained unchanged. They were no more likely to seek out information on cybersecurity and were no less susceptible to spamming attempts after reading about a recent data breach. Exposure to a data breach also had a limited effect on respondents' political preferences. While subjects expressed significantly more support for increasing the cybersecurity budget in general after exposure to a breach of any type, their specific policy preferences remained unchanged. Finally, the effect of exposure to a cyber operation on risk perceptions was *highest* among those citizens who, prior to treatment, were 1) the least knowledgeable about cyber; 2) the least concerned about online privacy; and 3) the least likely to use safe online practices. These results have important theoretical and policy implications.

First, our results shed light on conflicting findings from across the social sciences regarding the role of personal threat in shaping behavior. For example, our finding that personal threat can motivate willingness to change behavior is consistent with research from the field of health and environmental economics that has found similar evidence that threats become a motivator of behavioral change when they appear personally relevant, whether these threats are about alcohol abuse, cocaine dependence, compulsive gambling, overeating, heroin addiction, smoking (DiClemente and Velasquez, 2002; Petty and Cacioppo, 1986; Prochaska and DiClemente, 1986), carbon pricing (Heiskanen et al., 2010), and pro environmental behavior (Kollmuss and Agyeman, 2002).[41] However, the gap between intentions and actual behavior that we discovered here also bolsters research in the field of public health that has shown how even major personal health shocks can fail to change actual ingrained behavior (Feldstein et al., 2008; Oster, 2012, 2017). Our findings that personal threat does not significantly shape policy attitudes also contributes to a growing body of political science literature that has questioned the role of personal threat versus more sociotrophic concerns in shaping attitudes on a host of issues, from immigration (Hainmueller and Hopkins, 2014) to terrorism (Huddy et al., 2005; Wayne, 2018).

Second, our findings reiterate the results of recent public opinion polls (Olmstead and Smith,

[41] McKenzie-Mohr and Smith (1999, p. 7), demonstrate that social marketing that targets a particular aspect of people's behavior making harm seem more relevant to them has been successful in narrowing the gap between knowledge and action in local environmental and sustainability projects.

2017*a,b*; Gao and Madden, 2015) indicating that citizens' understanding of cyber issues and familiarity with current events surrounding cyber is strikingly low. Despite espousing a high confidence in the use of computers, the majority of our sample was unable to correctly answer questions about very high-profile cyber operations and were unfamiliar with three of the most prevalent types of hacking. The low knowledge in our sample is even more surprising because we would expect the younger student sample used in our study to be *most* familiar with computer usage and terminology, as compared to the general population. It is likely that this lack of familiarity with cyber risks is a key factor contributing to the relatively poor computer safety practices of most computer users. Because cyber operations are designed to exploit the weakest link in an online system, the ill-preparedness of individual citizens to defend their computers from cyber threats increases the security challenges for states attempting to reduce the risk from these types of operations. The results of our study thus suggest that government and industry must do a lot more to improve baseline knowledge of how individuals can secure their computers and find ways to drive home this message.

Thus, policymakers face a similar challenge in cybersecurity as they do in many other security areas where threats feel remote and abstract (e.g., nuclear security, climate change, national debt). How do they convince their citizenry that these threats are immediate and important? Our study points to some rhetorical strategies leaders could use to more effectively communicate cyber threats (and cyber-safety) to the mass public. Namely, we demonstrate that only *personally relevant* data breaches can shift citizens' risk perceptions and behaviors. Interestingly, both personal *and* national cybersecurity threats may lead citizens to support greater state investment in cybersecurity. As such, messaging campaigns designed to increase citizens' cyber-preparedness should emphasize citizens' potential personal vulnerability, while also highlighting concrete steps individuals can take to better protect themselves online. This type of campaign would heighten risk perceptions, while also empowering individuals to take control of their security online. Importantly, our experiment also showed heterogeneity among respondents, such that the citizens most likely to alter their risk perceptions in the wake of exposure to cyber operations are those who previously possessed the least knowledge or concern about cyber issues. This is a somewhat encouraging result, suggesting that even those with little interest in the world of cyber can have their perceptions changed. Thus, messaging campaigns are likely to be particularly effective when targeted towards segments of the population that are the least knowledgeable computer users.

However, this study also demonstrates the limitations of *any* potential messaging campaign. While subjects exposed to a personally relevant data breach were more likely to *express* a willingness to change their online behavior, this willingness did not manifest itself in their actual behavior only one day later. These results suggest that steps by government and corporate actors to remove agency from individuals and automate cybersecurity — by enforcing mandatory password changes, not accepting any USB devices, or not accessing external hyperlinks or attachments, for example — are likely to be comparatively more efficacious than messaging campaigns to improve users' voluntary security practices. This so-called *security by design* may be a more effective cybersecurity method than placing the burden on average users, who appear — in our study at least — slow to educate themselves about various cyber threats and the ways to protect themselves from them, even after exposure to a data breach.

The lack of change in macro-level political attitudes we observe also has important implications for how governments might think about the role or importance of public opinion in constraining state cybersecurity policy. Though subjects exposed to data breaches expressed general support for a higher cybersecurity budget, they were not any more supportive of new, costly cybersecurity policies highlighted by national security experts as crucial in improving the United States' overall cybersecurity. This is in stark contrast to the changes in political attitudes engendered by other types of national security threat, whereby, exposure to — for example — terror attacks, has frequently been shown to increase public support for reactive counter-terror policies (Bueno de Mesquita, 2007; Sandler and Siqueira, 2006). This may be due to high levels of suspicion regarding government surveillance and reflect subjects' beliefs that cyber threats are just as likely to come from state actors as non-state ones. Exploring the extent to which individual citizens place responsibility for cybersecurity on private corporations versus the government is thus a fruitful direction for future research. It is possible that support for these cybersecurity policies remains static because respondents generally place the onus for cybersecurity on private companies, rather than the government.

Thus, political elites may face significant challenges in mobilizing the public in support of costly cybersecurity policies, even in the wake of a major cyber breach. Instead, it is possible that public-private partnerships between government and corporate stakeholders may be more effective in garnering support for (and implementation of) new state-of-the-art cybersecurity protocols. On the other hand, though public support for these various cybersecurity policies does not appreciably increase after exposure to a breach, it is notable that attitudes towards many of these policies are *already* quite positive. This may be due to their relative lack of politicization to date. This finding is somewhat encouraging and suggests that (many) cybersecurity policies may be able to be enacted by politicians without ideologically polarizing the electorate.

Finally, the results of our study point to some important future directions for research. In this study, we explore reactions to one specific type of cyber threat: a data breach that may lead to identity theft. However, other types of cyber operations also pose important threats to state cybersecurity and are potentially viewed very differently by the mass public. For example, in line with our theory of cyber-risk perception and the importance of "flash-bulb" memory, the public may respond much stronger to cyber threats against critical infrastructure than they do to data breaches, due to their sensationalist nature. Also, in the United States, it is likely that concerns about cybersecurity in general have now become intertwined with attitudes toward so-called "fake news" propagated by states like Russia during the 2016 election. As a result, the coming years may see a significant increase in the prevalence of polarized political attitudes toward cybersecurity policies designed to address these types of state misinformation campaigns. Exploring attitudinal and behavioral responses to these different types of cyber threats is thus an important direction for future study.

In sum, our research sheds light on a key challenge in the area of cybersecurity: data breaches with the potential for national, macro-level consequences are most likely to occur at the *micro*-level, originating through the security errors of individual computer users. As such, many aspects of state cybersecurity often directly rely on the personal attitudes and behavior of average citizens. However, the results of our study are not wholly encouraging in this regard. We find that baseline concerns about cybersecurity and knowledge about safe online practices are very low. Exposure to a *personally relevant* data breach can heighten risk perception and increases willingness to engage in safer online practices, suggesting that a sense of personal dread and knowledge about cyber operations may be important in changing intended behavior. But these effects are circumscribed — *actual* online behavior is more resistant to change. Together, these results suggest that policy-makers will continue to face an up-hill struggle in mobilizing the public to improve state cybersecurity. Rather, state-corporate partnerships with private sector stakeholders and automated security protocols that reduce individual agency online are likely to make for more effective cybersecurity strategies. This strategy may also prove effective in today's divisive political climate — reducing the potential politicization, and thus polarization, of effective cybersecurity policy.

References

Acquisti, Alessandro, Laura Brandimarte and George Loewenstein. 2015. "Privacy and human behavior in the age of information." *Science* 347(6221):509–514.

Altemeyer, Bob. 1996. *The Authoritarian Specter*. Cambridge University Press.

Asal, Victor, Jacob Mauslein, Amanda Murdie, Joseph Young, Ken Cousins and Chris Bronk. 2016. "Repression, Education, and Politically Motivated Cyberattacks." *Journal of Global Security Studies* 1(3):235–247.

Axelrod, Robert and Rumen Iliev. 2014. "Timing of cyber conflict." *Proceedings of the National Academy of Sciences* 111(4):1298–1303.

Bartels, Larry M. 2000. "Partisanship and voting behavior, 1952-1996." *American Journal of Political Science* pp. 35–50.

Baum, Matthew A and Philip BK Potter. 2015. *War and democratic constraint: How the public influences foreign policy*. Princeton University Press.

Bimber, Bruce. 2001. "Information and political engagement in America: The search for effects of information technology at the individual level." *Political Research Quarterly* 54(1):53–67.

Borghard, Erica D and Shawn W Lonergan. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26(3):452–481.

Bovens, Mark and Stavros Zouridis. 2002. "From street-level to system-level bureaucracies: how information and communication technology is transforming administrative discretion and constitutional control." *Public administration review* 62(2):174–184.

Brants, Kees, Martine Huizenga, R van Meerten et al. 1996. "The new canals of Amsterdam: an exercise in local electronic democracy." *Media, Culture & Society* 18(2):233–249.

Breckenridge, James N and Philip G Zimbardo. 2007. "The strategy of terrorism and the psychology of mass-mediated fear." *Psychology of terrorism* pp. 116–133.

Buchanan, Ben. 2017. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press.

Bueno de Mesquita, Ethan. 2007. "Politics and the Suboptimal Provision of Counterterror." *International Organization* 61:9.

Canes-Wrone, Brandice and Kenneth W Shotts. 2004. "The conditional nature of presidential responsiveness to public opinion." *American Journal of Political Science* 48(4):690–706.

Canetti, Daphna, Michael L Gross and Israel Waismel-Manor. 2016. "Immune from Cyberfire?" *Binary Bullets: The Ethics of Cyberwarfare* p. 157.

Cavelty, Myriam Dunn. 2010. "The reality and future of cyberwar." *Zurich, Switzerland: CSS Analysis in Security Policy* .

Cheung-Blunden, Violet and Jiarun Ju. 2015. "Anxiety as a Barrier to Information Processing in the Event of a Cyberattack." *Political Psychology* .

Coleman, Stephen, John Taylor and Wim van de Donk. 1999. *Parliament in the Age of the Internet*. Oxford University Press.

Deibert, Ronald and Rafal Rohozinski. 2010. "Liberation vs. control: The future of cyberspace." *Journal of Democracy* 21(4):43–57.

Denning, Dorothy E. 2001. "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy." *Networks and netwars: The future of terror, crime, and militancy* 239:288.

DiClemente, Carlo C and Mary Marden Velasquez. 2002. "Motivational interviewing and the stages of change." *Motivational interviewing: Preparing people for change* 2:201–216.

Dinev, Tamara, Paul Hart and Michael R Mullen. 2008. "Internet privacy concerns and beliefs about government surveillance–An empirical investigation." *The Journal of Strategic Information Systems* 17(3):214–233.

Druckman, James N and Cindy D Kam. 2009. "Students as experimental participants: A defense of the'narrow data base'." *Available at SSRN 1498843* .

Edwards, George C. 2006. *On deaf ears: The limits of the bully pulpit*. Yale University Press.

Egelman, Serge and Eyal Peer. 2015. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM pp. 2873–2882.

Eng, James. 2015. "OPM Hack: Government Finally Starts Notifying 21.5 Million Victims." *NBC News* .

Feldstein, Adrianne C, Gregory A Nichols, David H Smith, Victor J Stevens, Keith Bachman, A Gabriela Rosales and Nancy Perrin. 2008. "Weight change in diabetes and glycemic and blood pressure control." *Diabetes care* .

Franzen, Axel. 2000. "Does the Internet make us lonely?" *European Sociological Review* 16(4):427–438.

Gadarian, Shana Kushner. 2010. "The politics of threat: How terrorism news shapes foreign policy attitudes." *The Journal of Politics* 72(2):469–483.

Gaissmaier, Wolfgang and Gerd Gigerenzer. 2012. "9/11, Act II A Fine-Grained Analysis of Regional Variations in Traffic Fatalities in the Aftermath of the Terrorist Attacks." *Psychological science* pp. 1449–54.

Gao, George and Mary Madden. 2015. "Privacy and Cybersecurity: Key findings from Pew Research." *Pew Research Center* .

Gartzke, Erik. 2013. "The myth of cyberwar: bringing war in cyberspace back down to Earth." *International Security* 38(2):41–73.

Gartzke, Erik and Jon R Lindsay. 2015. "Weaving tangled webs: offense, defense, and deception in cyberspace." *Security Studies* 24(2):316–348.

Gelpi, Christopher. 2010. "Performing on cue? The formation of public opinion toward war." *Journal of Conflict Resolution* 54(1):88–116.

Goldgeier, James M and Philip E Tetlock. 2001. "Psychology and international relations theory." *Annual Review of Political Science* 4(1):67–92.

Hafner-Burton, Emilie M, Stephan Haggard, David A Lake and David G Victor. 2017. "The Behavioral Revolution and International Relations." *International Organization* 71(S1):S1–S31.

Hainmueller, Jens and Daniel J Hopkins. 2014. "Public attitudes toward immigration." *Annual Review of Political Science* 17:225–249.

Harris, Elizabeth. 2014. "Data breach hurts profit at target." *New York Times* .

Haynes, Audrey A and Brian Pitts. 2009. "Making an impression: New media in the 2008 presidential nomination campaigns." *PS: Political Science & Politics* 42(01):53–58.

Heal, Charles and Robert Bunker. 2014. *Fifth Dimensional Operations: Space-Time-Cyber Dimensionality in Conflict and WarA Terrorism Research Center Book*. iUniverse.

Heiskanen, Eva, Mikael Johnson, Simon Robinson, Edina Vadovics and Mika Saastamoinen. 2010. "Low-carbon communities as a context for individual behavioural change." *Energy Policy* 38(12):7586–7595.

Herring, Susan C. 2008. "Questioning the generational divide: Technological exoticism and adult constructions of online youth identity." *Youth, identity, and digital media* pp. 71–94.

Horgan, John et al. 2004. *The psychology of terrorism*. Routledge.

Howard, Philip E.N., Less Rainie and Steve Jones. 2001. "Days and nights on the Internet." *American Behavioral Scientist* 45(3):383–404.

Huddy, Leonie, Stanley Feldman, Charles Taber and Gallya Lahav. 2005. "Threat, anxiety, and support of antiterrorism policies." *American Journal of Political Science* 49(3):593–608.

Jarvis, Lee, Stuart Macdonald and Andrew Whiting. 2017. "Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat." *European Journal of International Security* 2(1):64–87.

Jervis, Robert. 1976. *Perception and Misperception in International Politics*. Princeton, Princeton University Press.

Jervis, Robert. 1992. "Political implications of loss aversion." *Political Psychology* pp. 187–204.

Joint Publication 3 13 Information Operations. 2014.

Kahneman, Daniel. 2011. *Thinking, fast and slow*. Macmillan.

Kertzer, Joshua D. 2017. "Resolve, time, and risk." *International Organization* 71(S1):S109–S136.

Kertzer, Joshua D, Kathleen E Powers, Brian C Rathbun and Ravi Iyer. 2014. "Moral support: How moral values shape foreign policy attitudes." *The Journal of Politics* 76(3):825–840.

Kertzer, Joshua D and Thomas Zeitzoff. 2017. "A Bottom-Up Theory of Public Opinion about Foreign Policy." *American Journal of Political Science* 61(3):543–558.

King, Gary, Jennifer Pan and Margaret E Roberts. 2013. "How censorship in China allows government criticism but silences collective expression." *American Political Science Review* 107(2):326–343.

King, Gary, Jennifer Pan and Margaret E Roberts. 2017. "How the Chinese government fabricates social media posts for strategic distraction, not engaged argument." *American Political Science Review* 111(3):484–501.

Kluver, Randolph. 2004. "Political culture and information technology in the 2001 Singapore general election." *Political Communication* 21(4):435–458.

Kollmuss, Anja and Julian Agyeman. 2002. "Mind the gap: why do people act environmentally and what are the barriers to pro-environmental behavior?" *Environmental education research* 8(3):239–260.

Kostyuk, Nadiya and Yuri M. Zhukov. 2019. "Invisible Digital Front: Can cyber attacks shape battlefield events?" *Journal of Conflict Resolution* 63:317–347.

Kreps, Sarah E and Jacquelyn Schneider. 2018. "Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics.".

Lawson, Sean T, Sara K Yeo, Haoran Yu and Ethan Greene. 2016. The cyber-doom effect: The impact of fear appeals in the US cyber security debate. In *Cyber Conflict (CyCon), 2016 8th International Conference on*. IEEE pp. 65–80.

Lenz, Gabriel S. 2013. *Follow the leader?: how voters respond to politicians' policies and performance*. University of Chicago Press.

Levendusky, Matthew S and Michael C Horowitz. 2012. "When backing down is the right decision: Partisanship, new information, and audience costs." *The Journal of Politics* 74(2):323–338.

Levin, Adam. 2015. "Wetware: The Major Data Security Threat You've Never Heard Of." *Forbes Magazine* .

Levy, Jack S. 1983. "Misperception and the causes of war: Theoretical linkages and analytical problems." *World Politics* 36(1):76–99.

Levy, Jack S. 1992. "An introduction to prospect theory." *Political Psychology* pp. 171–186.

Libicki, Martin C. 2007. *Conquest in cyberspace: national security and information warfare*. Cambridge University Press.

Libicki, Martin C. 2009. *Cyberdeterrence and cyberwar*. RAND Corporation.

Lindsay, Jon R. 2013. "Stuxnet and the limits of cyber warfare." *Security Studies* 22(3):365–404.

Lindsay, Jon R. 2017. Cyber Espionage. In *The Oxford Handbook of Cyber Security*, ed. Paul N Cornish. New York: Oxford University Press.

Lindsay, Jon R and Erik Gartzke. 2016. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." *The Power to Hurt: Coercion in Theory and in Practice, Greenhill KM and Krause PJP (eds.). New York: Oxford University Press, Forthcoming* .

Lowry, Dennis T, Tarn Ching Josephine Nio and Dennis W Leitner. 2003. "Setting the public fear agenda: A longitudinal analysis of network TV crime reporting, public perceptions of crime, and FBI crime statistics."

Journal of Communication 53(1):61–73.

Lupia, Arthur and Gisela Sin. 2003. "Which public goods are endangered?: How evolving communication technologies affect the logic of collective action." *Public Choice* 117(3-4):315–331.

MacKinnon, Rebecca. 2013. *Consent of the networked: The worldwide struggle for Internet freedom*. Basic Books (AZ).

Madden, Mary. 2014. "Public Perceptions of Privacy and Security in the Post-Snowden Era." *Pew Research Center* .

Manworren, Nathan, Joshua Letwat and Olivia Daily. 2016. "Why you should care about the Target data breach." *Business Horizons* 59(3):257–266.

Marcus, George E, W Russell Neuman and Michael MacKuen. 2000. *Affective intelligence and political judgment*. University of Chicago Press.

McDermott, Rose. 2001. *Risk-taking in international politics: Prospect theory in American foreign policy*. University of Michigan Press.

McKenzie-Mohr, Doug and William Smith. 1999. "Fostering sustainable development. An introduction to community-based social marketing." *Canadá: New Society Publishers* .

McKew, Molly. 2018. "Did Russia Affect the 2016 Election? Its Now Undeniable.".

Mossberger, Karen, Caroline J Tolbert and Mary Stansbury. 2003. *Virtual inequality: Beyond the digital divide*. Georgetown University Press.

Mullinix, Kevin J, Thomas J Leeper, James N Druckman and Jeremy Freese. 2015. "The generalizability of survey experiments." *Journal of Experimental Political Science* 2(02):109–138.

Nakashima, Ellen. 2017. "The NSA has linked the WannaCry computer worm to North Korea." *The Washington Post* 14.

Norberg, Patricia A, Daniel R Horne and David A Horne. 2007. "The privacy paradox: Personal information disclosure intentions versus behaviors." *Journal of Consumer Affairs* 41(1):100–126.

Nye Jr, Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41(3):44–71.

Olmstead, Kenneth and Aaron Smith. 2017*a*. "Americans and Cybersecurity." *Pew Research Center* .

Olmstead, Kenneth and Aaron Smith. 2017*b*. "What the Public Knows About Cybersecurity." *Pew Research Center* .

OnlineTrustAlliance. 2018. "Cyber Incident and breach Trends Report: Review and analysis of 2017 cyber incidents, trends and key issues to address.". Online; accessed 18 September 2018.

Oster, Emily. 2012. "HIV and sexual behavior change: Why not Africa?" *Journal of health economics* 31(1):35–49.

Oster, Emily. 2017. "Diabetes and Diet: Purchasing Behavior Change in Response to Health Information." *American Economic Journal: Applied Economics* .

Petty, Richard E and John T Cacioppo. 1986. The elaboration likelihood model of persuasion. In *Communication and persuasion*. Springer pp. 1–24.

Pham, Thu. 2016. "What Really Happened in the OPM Breach." *Duo Securty* .

Polat, Rabia Karakaya. 2005. *European Journal of Communication* 20(4):435–459.

Poushter, Jacob and Dorothy Manevich. 2017. "Globally, People Point to ISIS and Climate Change as Leading Security Threats." *Pew Research Center* .

Poznansky, Michael and Evan Perkoski. 2018. "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution." *Journal of Global Security Studies* 3(4):402–416.

Prochaska, James O and Carlo C DiClemente. 1986. Toward a comprehensive model of change. In *Treating addictive behaviors*. Springer pp. 3–27.

Rid, Thomas. 2013. *Cyber war will not take place*. Oxford University Press.

Rid, Thomas and Ben Buchanan. 2015. "Attributing cyber attacks." *Journal of Strategic Studies* 38(1-2):4–37.

Robinson, John P, Meyer Kestnbaum, Alan Neustadtl and Anthony Alvarez. 2000. "Mass media use and social life among Internet users." *Social Science Computer Review* 18(4):490–501.

Saeki, Manabu. 2013. "The Myth of the Elite Cue: Influence of Voters Preferences on the US Congress." *Public opinion quarterly* 77(3):755–782.

Sandler, Todd and Kevin Siqueira. 2006. "Global terrorism: deterrence versus pre-emption." *Canadian Journal of Economics/Revue canadienne d'économique* 39(4):1370–1387.

Sanger, David E. 2012. *Confront and conceal: Obama's secret wars and surprising use of American power*. Crown Pub.

Sanovich, Sergey, Denis Stukal, Duncan Penfold-Brown and Joshua Tucker. 2015. Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia. In *Annual Conference of the International Society of New Institutional Economics*.

Scavo, Carmine and Yuhang Shi. 2000. "Public Administration The Role of Information Technology in the Reinventing Government ParadigmŠNormative Predicates and Practical Challenges." *Social Science Computer Review* 18(2):166–178.

Schneider, Jacquelyn. 2017. Cyber and crisis escalation: insights from wargaming. In *USASOC Futures Forum*.

Shaft, Teresa M, Mark P Sharfman and Wilfred W Wu. 2004. "Reliability assessment of the attitude towards computers instrument (ATCI)." *Computers in human behavior* 20(5):661–689.

Sharp, Travis. 2017. "Theorizing cyber coercion: The 2014 North Korean operation against Sony." *Journal of Strategic Studies* pp. 1–29.

Siddiqui, Aisha P and Nash Unsworth. 2011. "Investigating the role of emotion during the search process in free recall." *Memory & cognition* 39(8):1387–1400.

Slovic, Paul. 2016. *The perception of risk*. Routledge.

Stavroulakis, Peter and Mark Stamp. 2010. *Handbook of information and communication security*. Springer Science & Business Media.

Stein, Janice Gross. 1985. "Calculation, miscalculation, and conventional deterrence I: The view from Cairo." *Psychology and deterrence* pp. 34–59.

Sunstein, Cass R. 2003. "Terrorism and probability neglect." *Journal of Risk and Uncertainty* 26(2-3):121–136.

Tversky, Amos and Daniel Kahneman. 1973. "Availability: A heuristic for judging frequency and probability." *Cognitive psychology* 5(2):207–232.

Valeriano, Brandon, Jensen Bejnamin and Ryan C Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press.

Valeriano, Brandon and Ryan C Maness. 2014. "The dynamics of cyber conflict between rival antagonists, 2001–11." *Journal of Peace Research* 51(3):347–360.

Valeriano, Brandon and Ryan C Maness. 2015. "Cyber Hype versus Cyber Reality: Restraint and Norms in Cyber Conflict.".

Wayne, Carly. 2018. Risk or Retribution: How Citizens Respond to Terror. American Political Science Association Annual Meeting Boston, MA: .

Weber, Lori M, Alysha Loumakis and James Bergman. 2003. "Who participates and why? An analysis of citizens on the Internet and the mass public." *Social Science Computer Review* 21(1):26–42.

Weeks, Jessica L. 2012. "Strongmen and straw men: Authoritarian regimes and the initiation of international conflict." *American Political Science Review* 106(02):326–347.

Welch, Eric W and Shelley Fulla. 2005. "Virtual interactivity between government and citizens: The Chicago Police Department's citizen ICAM application demonstration case." *Political communication* 22(2):215–236.

Zaller, John. 1992. *The nature and origins of mass opinion*. Cambridge university press.

Zetter, Kim. 2016. "Inside the Cunning, Unprecedented Hack of Ukraines Power Grid." *Wired. com* .

Online Appendix: Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats

Nadiya Kostyuk & Carly Wayne
University of Michigan, Ann Arbor

June 13, 2019

Contents

1 Power Analysis 2

2 Participants 2

3 Measures 3
- 3.1 Moderators 3
- 3.2 Manipulations 5
- 3.3 Dependent Variables 7

4 Cyber Risk Study Coding Variables: Codebook 8

5 Follow-up Email 22

6 Spam Email 23

7 Additional Results 24
- 7.1 Correlations between Variables 24
- 7.2 Main Effects: Regression Tables 24
- 7.3 Heterogeneous Treatment Effects: Regression Tables 28

8 Robustness Checks 31
- 8.1 Including Participants who Failed Data Checks 31
- 8.2 Correlation of Party ID and Ideology with Cybersecurity Policy Preferences 34

1 Power Analysis

A power analysis, assuming a two-tailed t-test with significance levels of 0.05 and a power of 0.8, suggests that each condition will require approximately 176 participants, if the anticipated difference between the means of the compared conditions is 0.3 (e.g. an effect size or δ of 0.3, which is an approximately 7% difference between conditions). This leads to a suggested sample size of 525 subjects. Our sample was 436 subjects, after attrition (58 subjects who dropped out and 7 who failed multiple attention checks). Thus, our study will be able to pick up effects that are moderate to large, but may miss some very small effects.

This hypothesized difference between control and manipulation conditions has been estimated based on the results of past experimental studies in the field of terrorism and public opinion, as there have been few studies that look directly at public attitudes toward cyber terrorism or cyber operations in particular. For example, Huddy et al. (2005) found that perceived threat was associated with a difference of $\beta = .028$ in subjects' support for military intervention in Afghanistan. Similarly, Gadarian (2010) found that participants with high preexisting levels of threat perception were 6% more likely to support hawkish foreign policies when exposed to fearful messages about terrorism.

2 Participants

To test our hypotheses, we recruited five hundred and eight students from the University of Michigan (211 males and 268 females), ages ranging from eighteen to fifty-eight ($M = 21.9957$, standard deviation [SD]=5.95), to participate in an online study in February 2017. Respondents were entered into a raffle to win $50 USD for their participation. After attrition, our affective n was 436.

72% of the sample was White, followed by Asians (19%) and Hispanics (3%).[1] 60% of our participants grew up in suburban areas, and one-third in cities. The median household income of our sample was more than $150,000 (and the mean household income was $80,000 - $89,999).[2] Politically, the sample leaned to the left, with 70.95% of the participants identifying themselves as some type of Democrat, 6.5% identifying themselves as an Independent, and 21.4% identifying themselves as Republican.[3] The median age was less than twenty-five years old.

Figure 1 displays some basic descriptive statistics about the sample.

[1] The ethnic distribution in the United States according to the 2016 census is 76% White, 13% African American, 6% Asian, and 18% Hispanic. Thus, our sample does not oversample whites, but does undersample African Americans and Hispanics, while oversampling Asians.

[2] Thus, our sample was much wealthier than the median American (median household income in the U.S. in 2016 was approximately $55,000).

[3] Our sample is skewed towards individuals that identify themselves as Democrats, compared to the national partisan distribution, which, in 2016, was 48% Democratic or lean Democrat, and 44% Republican or lean Republican (Politics and Policy, 2016).

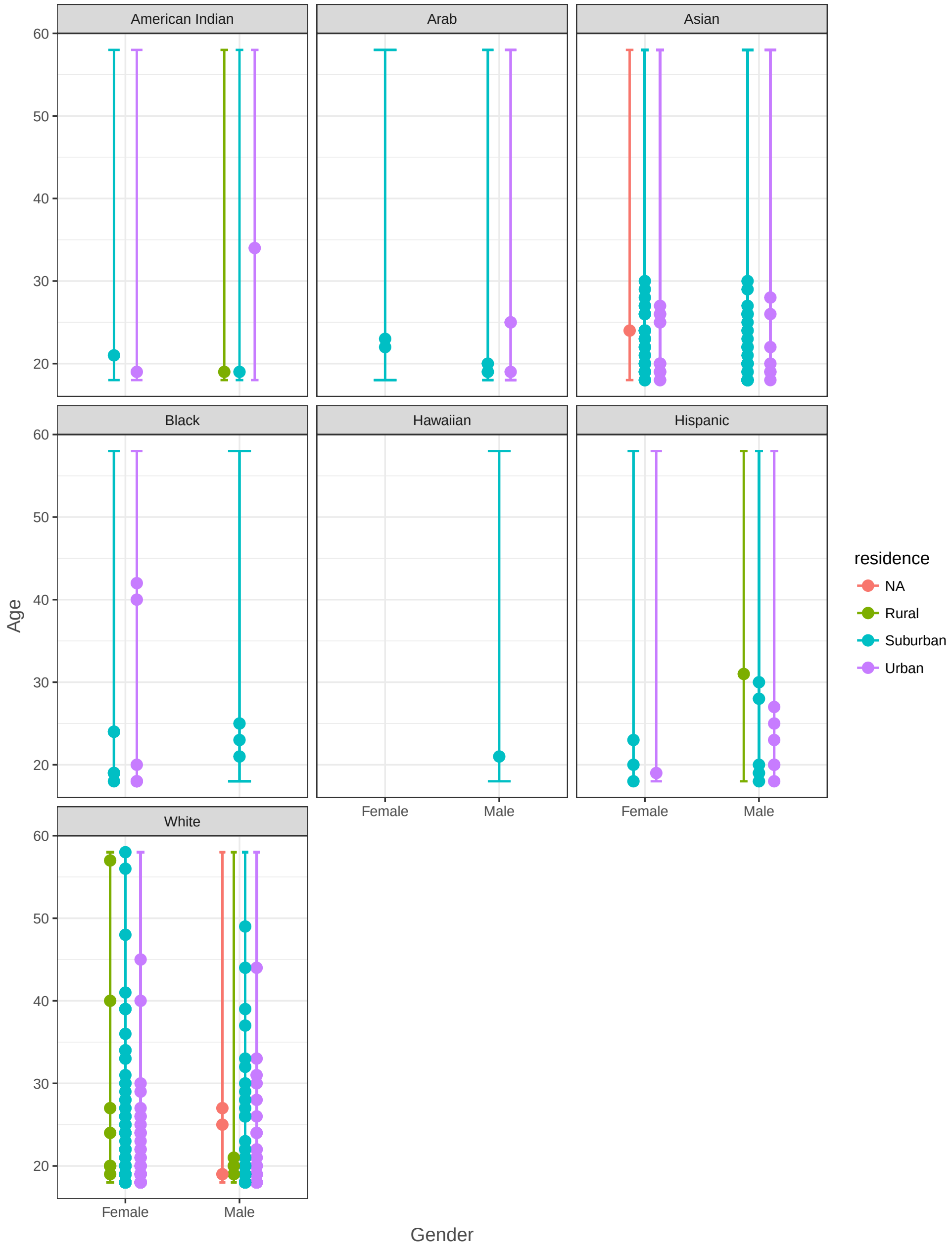


Figure 1: Sample Demographics

3 Measures

3.1 Moderators

Ideology was assessed using a 7-point scale from the American National Election Study, ranging from extremely liberal (1) to extremely conservative (7).

Party Identification was assessed using a two-part question used in the American National

Election Study to assess party identification on a 7-point scale from strong Democrat to strong Republican.

To measure *Privacy Concerns*, we used a six-question agree-disagree scale that measures respondents' concerns about government surveillance (Dinev, Hart and Mullen, 2008). Questions included the items, "The government needs to have greater access to personal information," "I am concerned about the power the government has to wiretap Internet activities," "The government needs broader wiretapping authority," "I am concerned that my Internet accounts and database information (e.g., e-mails, shopping records, tracking my Internet surfing, etc.) will be more open to government/business scrutiny," "The government needs to have more authority to use high tech surveillance tools for Internet eavesdropping," "I am concerned about the government's ability to monitor Internet activities." A high score on this scale represents individuals' higher level of concerns about government violating their privacy, while a low score represents an individual's support of government's surveillance.

To measure *Computer Safety*, we use an eight-question scale (Egelman and Peer, 2015). Questions included the items, "When I'm prompted about a software update, I install it right away," "I manually lock my computer screen when I step away from it," "I use a PIN or passcode to unlock my mobile phone," "I verify that my anti-virus software has been regularly updating itself," "When browsing websites, I mouseover links to see where they go before clicking them," "I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar," "I do not change my passwords unless I have to," "When I create a new online account, I try to use a password that goes beyond the site's minimum requirements," "I submit information to websites without first verifying that it will be sent securely (e.g., SSL, https://, a lock icon)."[4] A high score on this scale represents individuals' more secure/careful online behavior.

Comfort with Computers measures these attitudes towards computers using an eight-item bipolar scale developed by Shaft, Sharfman and Wu (2004). Questions contained eight pairs of adjectives that were used to describe computers. Some example of such pairs include: "Restrain creativity" vs. "Enhance creativity"; "Helpful" vs. "Harmful."[5] A high score on this scale represents individuals' high level of comfort using computers.

We use a newly developed battery of questions in which we ask respondents two types of questions to assess *Cyber Knowledge*: 1) Knowledge of recent real-world cyber operations (e.g., Stuxnet virus, Sony Pictures Hack, WikiLeaks); and 2) Familiarity with different types of cyber operations and what they do (for example, what a DDoS attack is, what phishing means, how to define a Trojan Horse). A high score on this scale represents individuals' better familiarity with cyber operations and cyber terminology.[6]

We also measure *Previous Exposure to Cyber Operations*, asking respondents if (to their knowledge) they had ever had their online accounts hacked, had their computer infected with a virus, or had their personal information stolen. Respondents with prior experience of cyber operations may already be hyper-aware of the threat as compared to respondents with no past history of being victimized online.

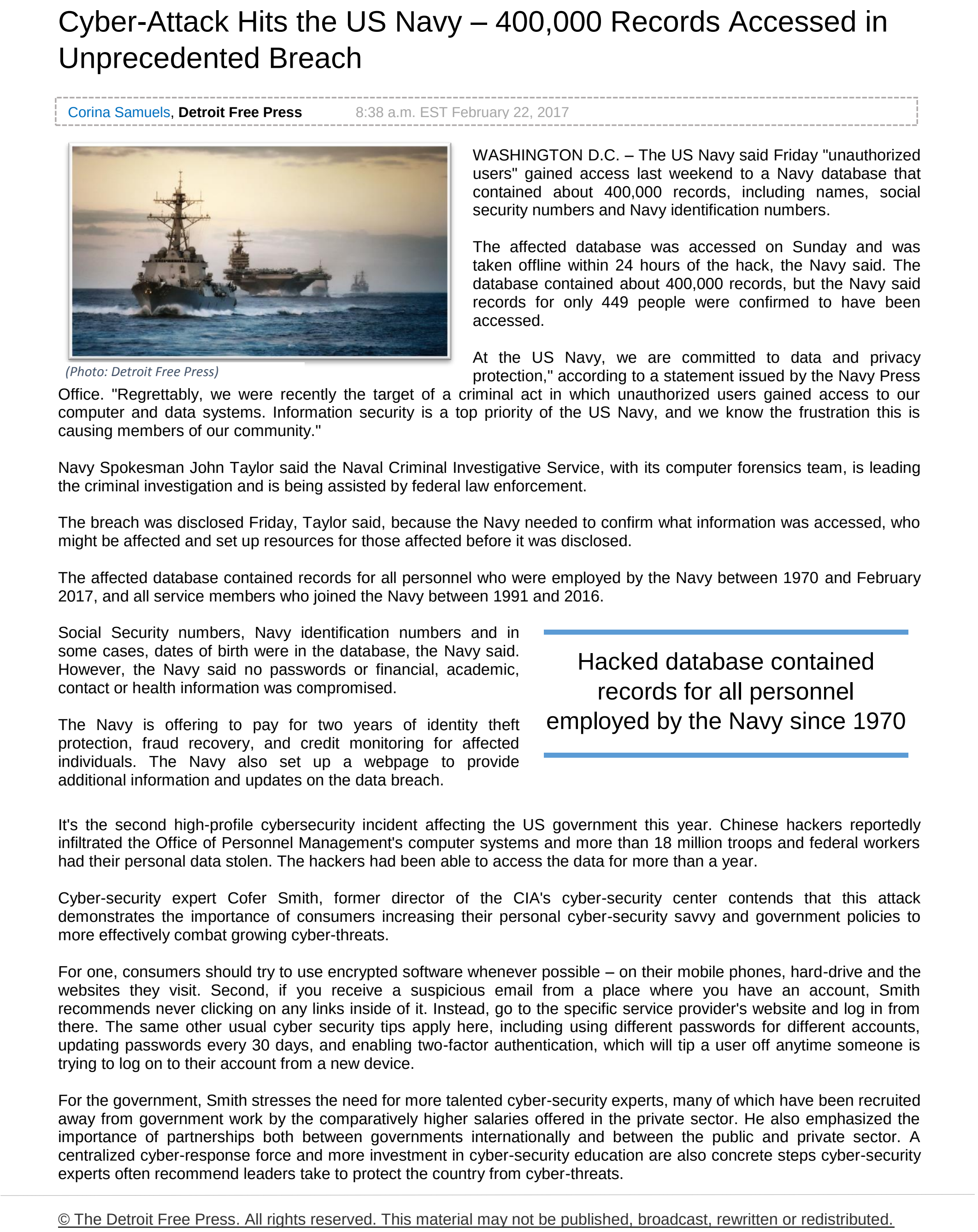
[4] Respondents could mark 5 options from "never" to "always." Each question also includes a "I'm not familiar with this" option which we code as "never."

[5] A complete list of adjectives can be found in Section 4.

[6] We also create two sub-scales, since knowledge about types of attacks versus real-world examples may not be highly correlated.

3.2 Manipulations

Participants in our control condition, did not read any article. Participants in the *national* condition were assigned to read the article displayed in Figure 2. Participants in the *personal* condition were assigned to read the article in Figure 3.



Cyber-Attack Hits the US Navy – 400,000 Records Accessed in Unprecedented Breach

Corina Samuels, **Detroit Free Press** 8:38 a.m. EST February 22, 2017

(Photo: Detroit Free Press)

WASHINGTON D.C. – The US Navy said Friday "unauthorized users" gained access last weekend to a Navy database that contained about 400,000 records, including names, social security numbers and Navy identification numbers.

The affected database was accessed on Sunday and was taken offline within 24 hours of the hack, the Navy said. The database contained about 400,000 records, but the Navy said records for only 449 people were confirmed to have been accessed.

At the US Navy, we are committed to data and privacy protection," according to a statement issued by the Navy Press Office. "Regrettably, we were recently the target of a criminal act in which unauthorized users gained access to our computer and data systems. Information security is a top priority of the US Navy, and we know the frustration this is causing members of our community."

Navy Spokesman John Taylor said the Naval Criminal Investigative Service, with its computer forensics team, is leading the criminal investigation and is being assisted by federal law enforcement.

The breach was disclosed Friday, Taylor said, because the Navy needed to confirm what information was accessed, who might be affected and set up resources for those affected before it was disclosed.

The affected database contained records for all personnel who were employed by the Navy between 1970 and February 2017, and all service members who joined the Navy between 1991 and 2016.

Social Security numbers, Navy identification numbers and in some cases, dates of birth were in the database, the Navy said. However, the Navy said no passwords or financial, academic, contact or health information was compromised.

The Navy is offering to pay for two years of identity theft protection, fraud recovery, and credit monitoring for affected individuals. The Navy also set up a webpage to provide additional information and updates on the data breach.

Hacked database contained records for all personnel employed by the Navy since 1970

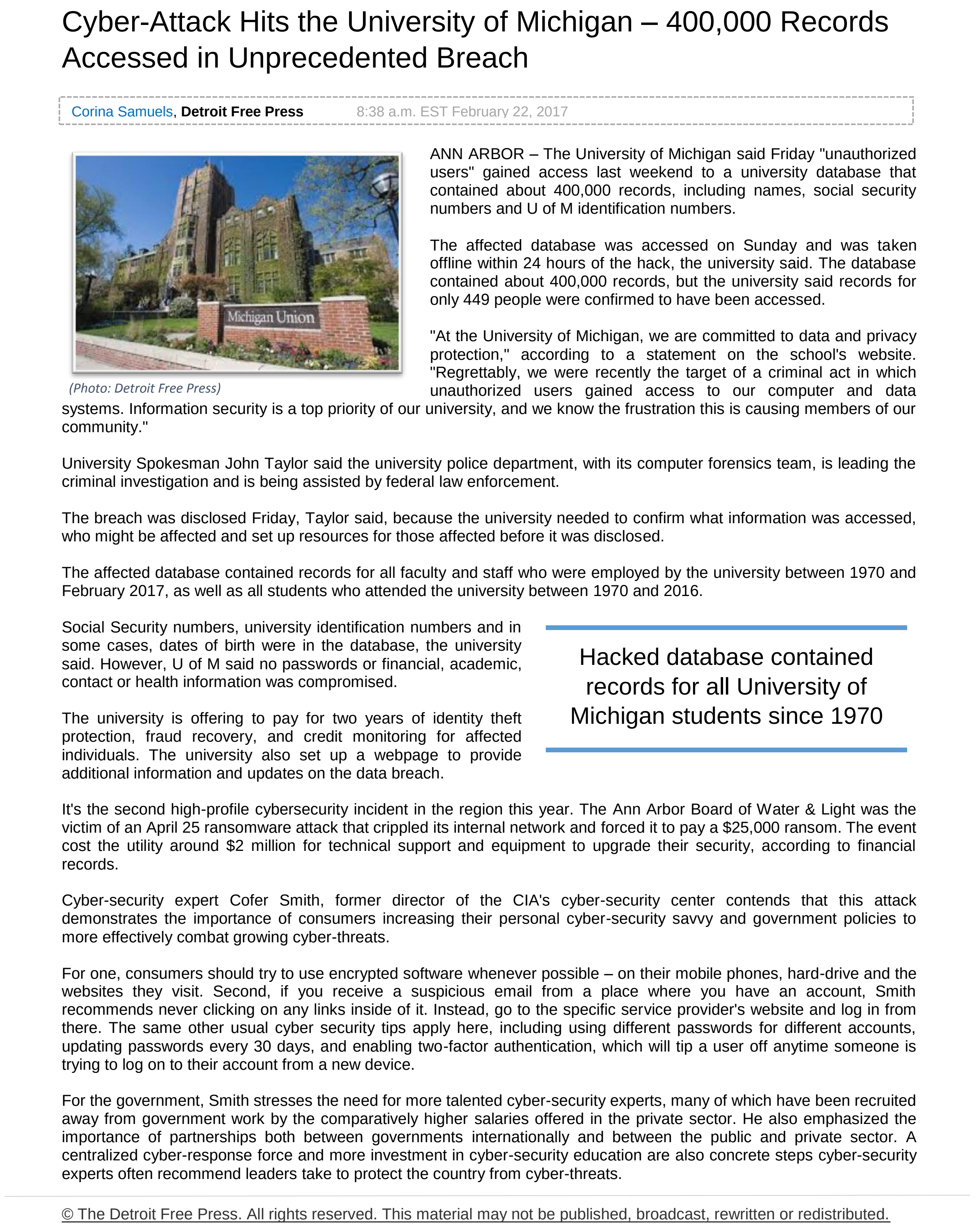
It's the second high-profile cybersecurity incident affecting the US government this year. Chinese hackers reportedly infiltrated the Office of Personnel Management's computer systems and more than 18 million troops and federal workers had their personal data stolen. The hackers had been able to access the data for more than a year.

Cyber-security expert Cofer Smith, former director of the CIA's cyber-security center contends that this attack demonstrates the importance of consumers increasing their personal cyber-security savvy and government policies to more effectively combat growing cyber-threats.

For one, consumers should try to use encrypted software whenever possible – on their mobile phones, hard-drive and the websites they visit. Second, if you receive a suspicious email from a place where you have an account, Smith recommends never clicking on any links inside of it. Instead, go to the specific service provider's website and log in from there. The same other usual cyber security tips apply here, including using different passwords for different accounts, updating passwords every 30 days, and enabling two-factor authentication, which will tip a user off anytime someone is trying to log on to their account from a new device.

For the government, Smith stresses the need for more talented cyber-security experts, many of which have been recruited away from government work by the comparatively higher salaries offered in the private sector. He also emphasized the importance of partnerships both between governments internationally and between the public and private sector. A centralized cyber-response force and more investment in cyber-security education are also concrete steps cyber-security experts often recommend leaders take to protect the country from cyber-threats.

Figure 2: *National Condition*



Cyber-Attack Hits the University of Michigan – 400,000 Records Accessed in Unprecedented Breach

Corina Samuels, **Detroit Free Press** 8:38 a.m. EST February 22, 2017

(Photo: Detroit Free Press)

ANN ARBOR – The University of Michigan said Friday "unauthorized users" gained access last weekend to a university database that contained about 400,000 records, including names, social security numbers and U of M identification numbers.

The affected database was accessed on Sunday and was taken offline within 24 hours of the hack, the university said. The database contained about 400,000 records, but the university said records for only 449 people were confirmed to have been accessed.

"At the University of Michigan, we are committed to data and privacy protection," according to a statement on the school's website. "Regrettably, we were recently the target of a criminal act in which unauthorized users gained access to our computer and data systems. Information security is a top priority of our university, and we know the frustration this is causing members of our community."

University Spokesman John Taylor said the university police department, with its computer forensics team, is leading the criminal investigation and is being assisted by federal law enforcement.

The breach was disclosed Friday, Taylor said, because the university needed to confirm what information was accessed, who might be affected and set up resources for those affected before it was disclosed.

The affected database contained records for all faculty and staff who were employed by the university between 1970 and February 2017, as well as all students who attended the university between 1970 and 2016.

Hacked database contained records for all University of Michigan students since 1970

Social Security numbers, university identification numbers and in some cases, dates of birth were in the database, the university said. However, U of M said no passwords or financial, academic, contact or health information was compromised.

The university is offering to pay for two years of identity theft protection, fraud recovery, and credit monitoring for affected individuals. The university also set up a webpage to provide additional information and updates on the data breach.

It's the second high-profile cybersecurity incident in the region this year. The Ann Arbor Board of Water & Light was the victim of an April 25 ransomware attack that crippled its internal network and forced it to pay a $25,000 ransom. The event cost the utility around $2 million for technical support and equipment to upgrade their security, according to financial records.

Cyber-security expert Cofer Smith, former director of the CIA's cyber-security center contends that this attack demonstrates the importance of consumers increasing their personal cyber-security savvy and government policies to more effectively combat growing cyber-threats.

For one, consumers should try to use encrypted software whenever possible – on their mobile phones, hard-drive and the websites they visit. Second, if you receive a suspicious email from a place where you have an account, Smith recommends never clicking on any links inside of it. Instead, go to the specific service provider's website and log in from there. The same other usual cyber security tips apply here, including using different passwords for different accounts, updating passwords every 30 days, and enabling two-factor authentication, which will tip a user off anytime someone is trying to log on to their account from a new device.

For the government, Smith stresses the need for more talented cyber-security experts, many of which have been recruited away from government work by the comparatively higher salaries offered in the private sector. He also emphasized the importance of partnerships both between governments internationally and between the public and private sector. A centralized cyber-response force and more investment in cyber-security education are also concrete steps cyber-security experts often recommend leaders take to protect the country from cyber-threats.

Figure 3: *Personal Condition*

3.3 Dependent Variables

Moving to our dependent variables, we have three concepts of interest: 1) threat or risk perceptions, 2) personal security behaviors; and 3) policy preferences. We operationalize each as follows:

First, we measure individuals' *Threat Perception*, using four questions. Subjects were asked to estimate the likelihood of 1) cyber-attacks against the U.S government or infrastructure happening in the next year; 2) cyber-attacks against average American citizens happening in the next year; 3) they or someone they know being a victim of cyber-attacks in the next year; and 4) "the risk posed to their or their family's well-being" from a host of potential public health threats: gun violence, terrorism, heart disease, cancer, natural disasters, traffic accidents, cyber-attacks, or military conflict with nuclear powers. To the extent that exposure to a personally relevant attacks heightens knowledge, dread, and perceived uncontrollability of cyber-attacks, threat perceptions should increase after exposure.

Next, our *Policy Scale* measures an individual's preferences for various potential cybersecurity policies that have been suggested by national security professionals. We asked a series of six newly developed questions regarding potential policy responses that the government could engage in with regards to cyber threats, all of which are costlier than the status quo (on some dimension) and all of which have been recommended by cybersecurity experts. These questions asked participants' opinion on whether the government should 1) match salaries of Silicon Valley companies; 2) transfer some of the Department of Education budget into computer safety programs; 3) require private companies to disclose cyber-attacks; 4) share classified intelligence information on hackers with other countries; 5) adopt harsher legislation on cyber crimes; 6) respond to every cyber-attack with retaliation for the purposes of deterrence. A high score on this scale represents individuals' higher support for these policies. We also asked a separate question regarding cybersecurity spending, whether (and by how much) it should be increased or decreased. We expect support for these policies to increase after exposure due to increase risk perceptions.[7]

Third, our *Online Behaviors* scale measures whether exposure to cyber threats increased citizens' willingness to engage in costly or time-consuming cyber-protective behaviors. To assess this question, we asked seven questions, developed based on recommendations from cybersecurity professionals. Specifically, we asked subjects how likely they were to start 1) using encrypted mobile messaging software; 2) using an encryption software on their computers; 3) using secure passwords; 4) updating their passwords more frequently; 5) using two-factor authentication; 6) covering their web-cameras; or 7) using only the secure versions of websites. A high score on this scale represents individuals' higher willingness to engage in safe online behavior. Here too, we expect support for these policies to increase after exposure due to increase risk perceptions.[8]

Our final dependent variable is *Actual Cyber-Protective Behavior.* Thus far, the experiment is designed as a lab experiment – subjects realize they are participating in a study and are answering attitudinal and hypothetical behavioral questions accordingly. However, we are also interested in seeing if our small manipulation – exposure to a news story about a type of cyber operation – can impact real future behavior, outside of the context of the lab experiment. Our behavioral outcome thus tracks 1) whether subjects opened our email about security tips online and how many links they clicked to find out more information; and 2) whether subjects opened or responded to our 'spam' email sent from a fake email address. These measures thus track actual behavioral outcomes

[7] In our analyses, we assess each of these policies both separately and as part of a scale.

[8] Respondents could mark 7 options from "extremely unlikely" to "extremely likely." Each question also includes a "I'm not familiar with this" option.

outside of the lab setting.

4 Cyber Risk Study Coding Variables: Codebook

We coded the variables from our survey using the following scheme:

1. **Basic Data Checks**
   - (a) *Consent* - whether a participant has agreed to participate in the study or not
     - 1 - Yes
     - 0 - No
   - (b) *Complete* - whether a participant has reached the end survey screen
     - 1 - Yes
     - 0 - No
   - (c) *Attention* - attention check
     - 1 - if a participant gave a correct answer to our *attention check* question. The correct answer was 2. If they skipped the question, they receive no value (e.g., they are not marked as getting it wrong if they simply did not answer it)
     - 0 - if a participant gave an incorrect answer to our *attention check* question. The correct answer was 2 and a participant answered 1, 3, 4, or 5.
   - (d) *Read_Manip* – time spent on article reading (manipulation condition) (in seconds)
   - (e) *Stim_time* - categories created based on the time it took a participant to read the article (manipulation condition) (in seconds)
     - 0 - if time is less than 5 seconds
     - 1 - if time is more than or equal to 5 seconds but less than 16 seconds
     - 2 - if time is more than or equal to 16 seconds but less than 31 seconds
     - 3 - if time is more than or equal to 31 seconds but less than 181 seconds
     - 4 - if time is more than or equal to 181 seconds but less than 300 seconds
     - 5 - if time is more than 300 seconds
     - . - if time is "." (control condition)
   - (f) *Survey_Qual* - survey quality
     - 1 - poor quality if Attention=0 and *Stim_time*=0
     - 0 - otherwise
2. **Demographics**
   - (a) *Age* - participant's age (in years)
   - (b) *Age_scale* - participant's age (in years)
     - i. 1 – if participant's age is less than 25 years
     - ii. 2 – if participant's age is more than or equal to 25 years or less than 35 years
     - iii. 3 – if participant's age is more than or equal to 35 years or less than 45 years
     - iv. 4 – if participant's age is more than or equal to 45 years or less than 55 years
     - v. 5 – if participant's age is more than or equal to 55 years or less than 65 years

vi. 6 – if participant's age is more than 65 years

(c) *Gender_G* - participant's gender is male

- 1 - participant is a male
- 0 - participant is not a male

(d) *Gender_F* - participant's gender is female

- 1 - participant is a female
- 0 - participant is not a female

(e) *Ethnicity* - participant's ethnicity. Respondents could check multiple boxes. If they checked a box *in addition* to "White," they were coded as that additional box, not "White."

- 1 - if participant identifies their ethnicity as "White"
- 2 - if participant identifies their ethnicity as "Black"
- 3 - if participant identifies their ethnicity as "American Indian"
- 4 - if participant identifies their ethnicity as "Asian"
- 5 - if participant identifies their ethnicity as "Hawaiian"
- 6 - if participant identifies their ethnicity as "Hispanic"
- 7 - if participant identifies their ethnicity as "Arab"

(f) *White_Eth_Dummy* - a dummy variable that identifies whether a participant identifies at least one of their ethnicities as "White"

- 1 - yes
- 0 - no

(g) *Black_Eth_Dummy* - a dummy variable that identifies whether a participant identifies at least one of their ethnicities as "Black"

- 1 - yes
- 0 - no

(h) *Hispanic_Eth_Dummy* - a dummy variable that identifies whether a participant identifies at least one of their ethnicities as "Hispanic"

- 1 - yes
- 0 - no

(i) *Other_Eth_Dummy* - a dummy variable that identifies whether a participant identifies at least one of their ethnicities other than "White" or "Black"

- 1 - yes
- 0 - no

(j) *Residence* - participant's place of residence:

- 1 - Urban
- 2 - Suburban
- 3 - Rural

(k) *Residence_Urb* - if participant identifies their place of residence as "urban"

- 1 - yes
- 0 - no

(l) *Residence_Suburb* - if participant identifies their place of residence as "suburban"

- 1 - yes

- 0 - no

(m) *Residence_Rur* - if participant identifies their place of residence as "rural"

- 1 - yes
- 0 - no

(n) *Income* - participant's current annual income (in U.S. dollars) for their household. This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 11.

- 0 - if participant identifies their income as less than $10,000
- 1 - if participant identifies their income between $10,000 - $19,999
- 2 - if participant identifies their income between $20,000 - $29,999
- 3 - if participant identifies their income between $30,000 - $39,999
- 4 - if participant identifies their income between $40,000 - $49,999
- 5 - if participant identifies their income between $50,000 - $59,999
- 6 - if participant identifies their income between $60,000 - $69,999
- 7 - if participant identifies their income between $70,000 - $79,999
- 8 - if participant identifies their income between $80,000 - $89,999
- 9 - if participant identifies their income between $90,000 - $99,999
- 10 - if participant identifies their income between $100,000 - $149,999
- 11 - if participant identifies their income as more than $150,000

(o) *Party ID* – participant's party ID. We contracted this 7-point scale on which the political views arranged from *strong Democrat* to *strong Republican* using two questions. The first question asked whether a participant viewed themselves as a Democrat, Republican, or Independent. Based on the participant's answer, they were re-directed to the second question on whether they considered themselves as a strong (or not) Democrat/Republican/Independent. This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 6.

- 0 - if participant's answer is 1
- 1 - if participant's answer is 2
- 2 - if participant's answer is 3
- 3 - if participant's answer is 4
- 4 - if participant's answer is 5
- 5 - if participant's answer is 6
- 6 - if participant's answer is 7

(p) *Ideology* – participant's partisanship, using a 7-point scale on which the political ideology is arranged from *extremely liberal* to *extremely conservative*. This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 6.

- 0 - if participant's answer is 1
- 1 - if participant's answer is 2
- 2 - if participant's answer is 3
- 3 - if participant's answer is 4
- 4 - if participant's answer is 5
- 5 - if participant's answer is 6
- 6 - if participant's answer is 7

3. **Moderators**

   (a) *Internet Privacy Concerns and Belief about Government Surveillance*

   - Privacy_Concern1 - participant's agreement with the following statement: "The government needs to have greater access to personal information." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4. *The answers are arranged in a reverse order.*
     - 0 - Strongly agree
     - 1 - Somewhat agree
     - 2 - Neither agree nor disagree
     - 3 - Somewhat disagree
     - 4 - Strongly disagree
   - Privacy_Concern2 - participant's agreement with the following statement: "I am concerned about the power the government has to wiretap Internet activities." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4.
     - 0 - Strongly disagree
     - 1 - Somewhat disagree
     - 2 - Neither agree nor disagree
     - 3 - Somewhat agree
     - 4 - Strongly agree
   - Privacy_Concern3 - participant's agreement with the following statement: "The government needs broader wiretapping authority." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4. *The answers are arranged in a reverse order.*
     - 0 - Strongly agree
     - 1 - Somewhat agree
     - 2 - Neither agree nor disagree
     - 3 - Somewhat disagree
     - 4 - Strongly disagree
   - Privacy_Concern4 - participant's agreement with the following statement: "I am concerned that my Internet accounts and database information is too open to government/business scrutiny." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4.
     - 0 - Strongly disagree
     - 1 - Somewhat disagree
     - 2 - Neither agree nor disagree
     - 3 - Somewhat agree
     - 4 - Strongly agree
   - Privacy_Concern5 - participant's agreement with the following statement: "The government needs to have more authority to use high tech surveillance tools for Internet eavesdropping." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4. *The answers are arranged in a reverse order.*
     - 0 - Strongly agree
     - 1 - Somewhat agree
     - 2 - Neither agree nor disagree

    - 3 - Somewhat disagree
    - 4 - Strongly disagree
- Privacy_Concern6 - participant's agreement with the following statement: "I am concerned about the government's powerful ability to monitor Internet activities." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4.
    - 0 - Strongly disagree
    - 1 - Somewhat disagree
    - 2 - Neither agree nor disagree
    - 3 - Somewhat agree
    - 4 - Strongly agree
- Privacy_Concern_Scale - "privacy concern" scale. This variable is normalized to be between 0 and 1. It was created by adding the values for Privacy_Concern1-Privacy_Concern6 and dividing that value by 6. *Note: if there is a missing value on any one of the questions, the individual does not receive a score for that scale.*

(b) *Computer Safety*

- Computer_Safety1 - participant's response to the following statement: "When I'm prompted about a software update, I install it right away." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4.
    - 0 - Not familiar with this; Never
    - 1 - Rarely
    - 2 - Sometimes
    - 3 - Often
    - 4 - Always
- Computer_Safety2 - participant's response to the following statement: "I manually lock my computer screen when I step away from it." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4.
    - 0 - Not familiar with this; Never
    - 1 - Rarely
    - 2 - Sometimes
    - 3 - Often
    - 4 - Always
- Computer_Safety3 - participant's response to the following statement: "I use a PIN or passcode to unlock my mobile phone." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4.
    - 0 - Not familiar with this; Never
    - 1 - Rarely
    - 2 - Sometimes
    - 3 - Often
    - 4 - Always
- Computer_Safety4 - participant's response to the following statement: "I verify that my anti-virus software has been regularly updating itself." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4.
    - 0 - Not familiar with this; Never

- 1 - Rarely
- 2 - Sometimes
- 3 - Often
- 4 - Always

- Computer_Safety5 - participant's response to the following statement: "When browsing websites, I mouseover links to see where they go before clicking them." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4.
  - 0 - Not familiar with this; Never
  - 1 - Rarely
  - 2 - Sometimes
  - 3 - Often
  - 4 - Always
- Computer_Safety6 - participant's response to the following statement: "I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4. *The answers are arranged in a reverse order.*
  - 0 - Not familiar with this; Never
  - 1 - Always
  - 2 - Often
  - 3 - Sometimes
  - 4 - Rarely
- Computer_Safety7 - participant's response to the following statement: "I do not change my passwords unless I have to." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4. *The answers are arranged in a reverse order.*
  - 0 - Not familiar with this; Never
  - 1 - Always
  - 2 - Often
  - 3 - Sometimes
  - 4 - Rarely
- Computer_Safety8 - participant's response to the following statement: "When I create a new online account, I try to use a password that goes beyond the site's minimum requirements." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4.
  - 0 - Not familiar with this; Never
  - 1 - Rarely
  - 2 - Sometimes
  - 3 - Often
  - 4 - Always
- Computer_Safety9 - participant's response to the following statement: "I submit information to websites without first verifying that it will be sent securely (e.g., SSL, https://, a lock icon)." This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 4. *The answers are arranged in a reverse order.*

  - 0 - Not familiar with this; Never
  - 1 - Always
  - 2 - Often
  - 3 - Sometimes
  - 4 - Rarely
- Computer_Safety_Scale - "computer safety" scale. This variable is normalized to be between 0 and 1. It was created by adding the values for Computer_Safety1-Computer_Safety9 and dividing that value by 9. *Note: if there is a missing value on any one of the questions, the individual does not receive a score for that scale.*

(c) *Comfort with Computers*

- Comfort_Computers1 - participant's opinion of the adjectives that best describe computers using a 7-point scale from "Restrain creativity" (1) to "Enhance creativity" (7). This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 6.
  - 0 - if participant's answer is 1
  - 1 - if participant's answer is 2
  - 2 - if participant's answer is 3
  - 3 - if participant's answer is 4
  - 4 - if participant's answer is 5
  - 5 - if participant's answer is 6
  - 6 - if participant's answer is 7
- Comfort_Computers2 - participant's opinion of the adjectives that best describe computers using a 7-point scale from "Helpful" (1) to "Harmful" (7). This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 6. *The answers are arranged in a reverse order.*
  - 0 - if participant's answer is 7
  - 1 - if participant's answer is 6
  - 2 - if participant's answer is 5
  - 3 - if participant's answer is 4
  - 4 - if participant's answer is 3
  - 5 - if participant's answer is 2
  - 6 - if participant's answer is 1
- Comfort_Computers3 - participant's opinion of the adjectives that best describe computers using a 7-point scale from "Enjoyable to Use" (1) to "Frustrating to Use" (7). This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 6. *The answers are arranged in a reverse order.*
  - 0 - if participant's answer is 7
  - 1 - if participant's answer is 6
  - 2 - if participant's answer is 5
  - 3 - if participant's answer is 4
  - 4 - if participant's answer is 3
  - 5 - if participant's answer is 2
  - 6 - if participant's answer is 1

- Comfort_Computers4 - participant's opinion of the adjectives that best describe computers using a 7-point scale from "Boring" (1) to "Intriguing" (7). This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 6.
  - 0 - if participant's answer is 1
  - 1 - if participant's answer is 2
  - 2 - if participant's answer is 3
  - 3 - if participant's answer is 4
  - 4 - if participant's answer is 5
  - 5 - if participant's answer is 6
  - 6 - if participant's answer is 7
- Comfort_Computers5 - participant's opinion of the adjectives that best describe computers using a 7-point scale from "Sound investment" (1) to "Waster of money" (7). This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 6. *The answers are arranged in a reverse order.*
  - 0 - if participant's answer is 7
  - 1 - if participant's answer is 6
  - 2 - if participant's answer is 5
  - 3 - if participant's answer is 4
  - 4 - if participant's answer is 3
  - 5 - if participant's answer is 2
  - 6 - if participant's answer is 1
- Comfort_Computers6 - participant's opinion of the adjectives that best describe computers using a 7-point scale from "Difficult to Use" (1) to "Easy to Use" (7). This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 6.
  - 0 - if participant's answer is 1
  - 1 - if participant's answer is 2
  - 2 - if participant's answer is 3
  - 3 - if participant's answer is 4
  - 4 - if participant's answer is 5
  - 5 - if participant's answer is 6
  - 6 - if participant's answer is 7
- Comfort_Computers7 - participant's opinion of the adjectives that best describe computers using a 7-point scale from "Not threatening" (1) to "Threatening" (7). This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 6. *The answers are arranged in a reverse order.*
  - 0 - if participant's answer is 7
  - 1 - if participant's answer is 6
  - 2 - if participant's answer is 5
  - 3 - if participant's answer is 4
  - 4 - if participant's answer is 3
  - 5 - if participant's answer is 2
  - 6 - if participant's answer is 1

- Comfort_Computers8 - participant's opinion of the adjectives that best describe computers using a 7-point scale from "Decrease productivity" (1) to "Increase Productivity" (7). This variable is normalized to be between 0 and 1. It was created using the score assigned below divided by 6.
  - 0 - if participant's answer is 1
  - 1 - if participant's answer is 2
  - 2 - if participant's answer is 3
  - 3 - if participant's answer is 4
  - 4 - if participant's answer is 5
  - 5 - if participant's answer is 6
  - 6 - if participant's answer is 7
- Comfort_Computers_Scale - "comfort with computers" scale. This variable is normalized to be between 0 and 1. It was created by adding the values for Comfort_Computers1-Comfort_Computers8 and dividing that value by 8. *Note: if there is a missing value on any one of the questions, the individual does not receive a score for that scale.*

(d) *Familiarity with Cyber Operations*

- Cyber_Knowledge1 - participant's knowledge of current events related to cybersecurity issues.
  - 1- if participant answers this question correctly
  - 0 - otherwise
- Cyber_Knowledge2
- Cyber_Knowledge3
- Cyber_Knowledge4
- Cyber_Knowledge5
- Cyber_Knowledge6
- Cyber_Knowledge_Scale - "cyber knowledge" scale. This variable is normalized to be between 0 and 1. It was created by adding the values for Cyber_Knowledge1-Cyber_Knowledge6 and dividing that value by 6.

(e) *Previous Exposure to Cyber Operations*

- Previous_Exposure1 - previous exposure to cyber attacks
  - 1 - if participant has been a victim of cyber attacks
  - 0 - otherwise
- Previous_Exposure2
- Previous_Exposure3
- Previous_Exposure_Scale - "previous exposure" scale. This variable is normalized to be between 0 and 1. It was created by adding the values for Previous_Exposure1-Previous_Exposure3 and dividing that value by 3.

4. **Manipulations**

(a) *Condition* - manipulation condition that a participant was randomly assigned to

- 1 - if a participant was assigned to the *control* condition
- 2 - if a participant was assigned to the *national* condition
- 3 - if a participant was assigned to the *personal* condition

(b) *Control_Dummy* - if a participant was assigned to the *control* condition
- 1 - yes
- 0 - no

(c) *National_Dummy* - if a participant was assigned to the *national* condition
- 1 - yes
- 0 - no

(d) *Personal_Dummy* - if a participant was assigned to the *personal* condition
- 1 - yes
- 0 - no

5. **Threat Perception**

(a) *Gcyb_Likely* - participant's evaluation of how likely is that a cyber-attack will take place targeting the United States' government or infrastructure next year. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 4.
- 0 - Not likely at all
- 1 - Not very likely
- 2 - Somewhat unlikely
- 3 - Somewhat likely
- 4 - Extremely likely

(b) *Ccyb_Likely* - participants' evaluation of how likely is that a cyber-attack will take place targeting U.S. citizens or consumers next year. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 4.
- 0 - Not likely at all
- 1 - Not very likely
- 2 - Somewhat unlikely
- 3 - Somewhat likely
- 4 - Extremely likely

(c) *Victim_Likely* - participants' evaluation of how likely is that them personally or someone they know will be affected by a cyber attack in the next year. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 4.
- 0 - Not likely at all
- 1 - Not very likely
- 2 - Somewhat unlikely
- 3 - Somewhat likely
- 4 - Extremely likely

(d) *Ranking of Risks* - we are interested in where cyber ranks on this list.
- Gunviolence - participant's ranking of the risk that gun violence presents to them and their family's personal well-being, using an 8-point scale from *highest* (8) to *lowest* (1). This variable is normalized to be between 0 and 1. It was created using a participant's assigned rank divided by 7.
- Terrorism - participant's ranking of the risk that terrorism presents to them and their family's personal well-being, using an 8-point scale from *highest* (8) to *lowest* (1). This variable is normalized to be between 0 and 1. It was created using a participant's assigned rank divided by 7.

- Heart_Disease - participant's ranking of the risk that heart disease presents to them and their family's personal well-being, using an 8-point scale from *highest* (8) to *lowest* (1). This variable is normalized to be between 0 and 1. It was created using a participant's assigned rank divided by 7.
- Cancer - participant's ranking of the risk that cancer presents to them and their family's personal well-being, using an 8-point scale from *highest* (8) to *lowest* (1). This variable is normalized to be between 0 and 1. It was created using a participant's assigned rank divided by 7.
- Nat_Disaster - participant's ranking of the risk that a natural disaster presents to them and their family's personal well-being, using an 8-point scale from *highest* (8) to *lowest* (1). This variable is normalized to be between 0 and 1. It was created using a participant's assigned rank divided by 7.
- Car_Accident - participant's ranking of the risk that getting into a car accident presents to them and their family's personal well-being, using an 8-point scale from *highest* (8) to *lowest* (1). This variable is normalized to be between 0 and 1. It was created using a participant's assigned rank divided by 7.
- Cyber_Hacking - participant's ranking of the risk that cyber attacks or hacking of personal information presents to them and their family's personal well-being, using an 8-point scale from *highest* (8) to *lowest* (1). This variable is normalized to be between 0 and 1. It was created using a participant's assigned rank divided by 7.
- Nuclear_War - participant's ranking of the risk that a military conflict with nuclear powers presents to them and their family's personal well-being, using an 8-point scale from *highest* (8) to *lowest* (1). This variable is normalized to be between 0 and 1. It was created using a participant's assigned rank divided by 7.

6. **Public Opinion on Cybersecurity Policy**

(a) *Cyber_Budget* - participant's opinion on whether government funding for countering cyberattacks should be increased, decreased or kept the same. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Greatly decreased
- 1 - Moderately decreased
- 2 - Slightly decreased
- 3 - Kept the same
- 4 - Slightly increased
- 5 - Moderately increased
- 6 - Greatly increased

(b) *Tech_Sal* - participant's opinion on whether the U.S. government should attempt to pay its own cybersecurity employees as much as they are able to make working for a private sector. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Completely oppose
- 1 - Mainly oppose
- 2 - Somewhat oppose
- 3 - Neither favor nor oppose
- 4 - Somewhat favor
- 5 - Mainly favor

- 6 - Completely favor

(c) *Cyb_Ed* - participant's opinion on whether the U.S. government should transfer a portion of the Department of Education's school programming budget into a new, mandatory program for schools to teach about "cyber hygiene." This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Completely oppose
- 1 - Mainly oppose
- 2 - Somewhat oppose
- 3 - Neither favor nor oppose
- 4 - Somewhat favor
- 5 - Mainly favor
- 6 - Completely favor

(d) *Priv_Comp* - participant's opinion on whether the U.S. government should require private companies to disclose cyber-attacks that the latter suffers to the former. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Completely oppose
- 1 - Mainly oppose
- 2 - Somewhat oppose
- 3 - Neither favor nor oppose
- 4 - Somewhat favor
- 5 - Mainly favor
- 6 - Completely favor

(e) *Intel_Sharing* - participant's opinion on whether the U.S. government should share classified intelligence information with other countries. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Completely oppose
- 1 - Mainly oppose
- 2 - Somewhat oppose
- 3 - Neither favor nor oppose
- 4 - Somewhat favor
- 5 - Mainly favor
- 6 - Completely favor

(f) *Adopt_Law* - participant's opinion on whether the U.S. government adopt harsher legislature on cyber-crimes. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Completely oppose
- 1 - Mainly oppose
- 2 - Somewhat oppose
- 3 - Neither favor nor oppose
- 4 - Somewhat favor
- 5 - Mainly favor
- 6 - Completely favor

(g) *Cyber_Deterrence* - participant's opinion on whether the U.S. government respond to every cyber-attack against it with retaliation. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Completely oppose
- 1 - Mainly oppose
- 2 - Somewhat oppose
- 3 - Neither favor nor oppose
- 4 - Somewhat favor
- 5 - Mainly favor
- 6 - Completely favor

(h) *Policy_Scale* - policy scale created using participant's answers to questions b-e of this section and diving it by 6.

7. **Behavioral changes**

(a) *Encypt_Mobile* – participant's response on how likely they will start using encrypted mobile messaging software. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Extremely unlikely
- 1 - Pretty unlikely
- 2 - Somewhat unlikely
- 3 - Neither likely nor unlikely
- 4 - Somewhat likely
- 5 - Pretty likely
- 6 - Extremely likely

(b) *Encypt_Software* – participant's response on how likely they will start using an encryption software on their computers. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Extremely unlikely
- 1 - Pretty unlikely
- 2 - Somewhat unlikely
- 3 - Neither likely nor unlikely
- 4 - Somewhat likely
- 5 - Pretty likely
- 6 - Extremely likely

(c) *Secure_Password* – participant's response on how likely they will start using secure passwords. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Extremely unlikely
- 1 - Pretty unlikely
- 2 - Somewhat unlikely
- 3 - Neither likely nor unlikely
- 4 - Somewhat likely
- 5 - Pretty likely
- 6 - Extremely likely

(d) *Update_Password* – participant's response on how likely they will start updating their passwords more frequently. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Extremely unlikely
- 1 - Pretty unlikely
- 2 - Somewhat unlikely
- 3 - Neither likely nor unlikely
- 4 - Somewhat likely
- 5 - Pretty likely
- 6 - Extremely likely

(e) *TwoFactor_Auth* – participant's response on how likely they will start using two-factor authentication. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Extremely unlikely
- 1 - Pretty unlikely
- 2 - Somewhat unlikely
- 3 - Neither likely nor unlikely
- 4 - Somewhat likely
- 5 - Pretty likely
- 6 - Extremely likely

(f) *Cover_WebCam* – participant's response on how likely they will start covering your webcamera. This variable is normalized to be between 0 and 1. It was created using a score assigned below divided by 6.

- 0 - Extremely unlikely
- 1 - Pretty unlikely
- 2 - Somewhat unlikely
- 3 - Neither likely nor unlikely
- 4 - Somewhat likely
- 5 - Pretty likely
- 6 - Extremely likely

(g) *Behavior_Scale* - behavior scale created using participant's answers to questions a-f of this section and diving it by 6.

8. **Behavioral Measures**

(a) *Open_Mail* - whether a participant has opened our email with cybersecurity tips

- 1 - yes
- 0 - no

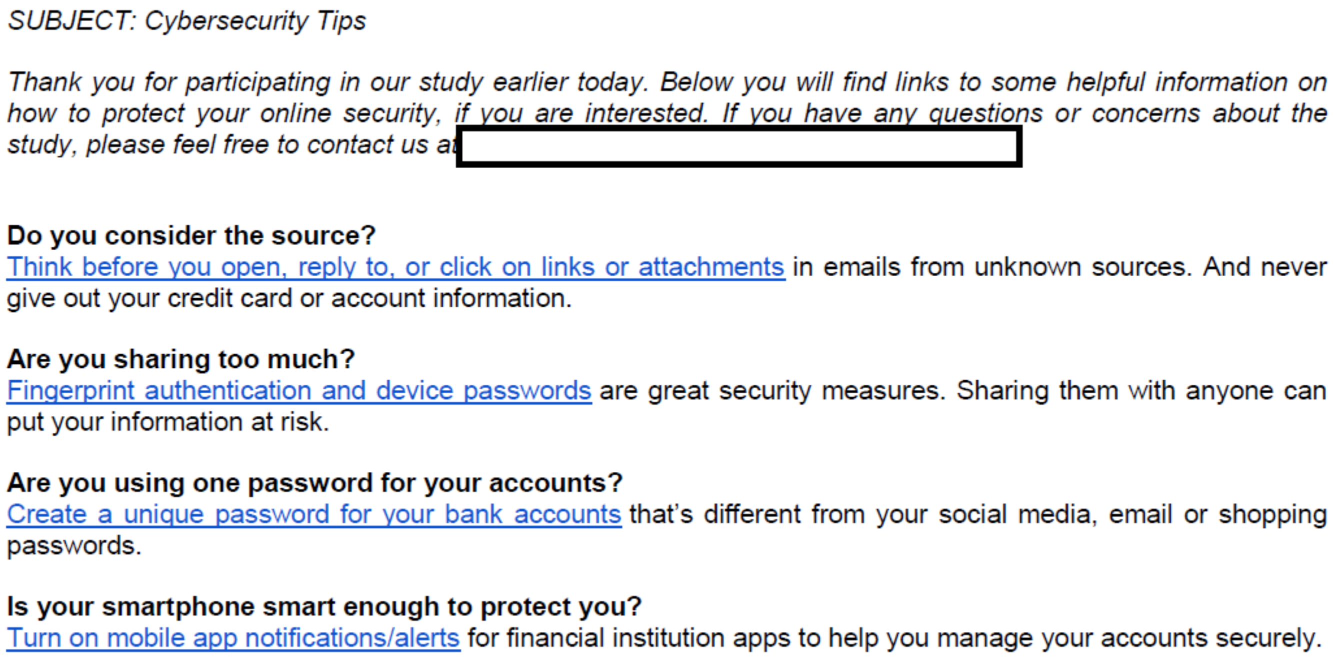
(b) *Num_Links* - a number of links that a participant has clicked on, from 0-4

(c) *Spam_Open* - whether a participant has opened our spam email

- 1 - yes
- 0 - no

5 Follow-up Email

We sent the email below (Figure 4) to all participants the evening they participated in the study. The links are safe and lead to real articles about how individuals can protect their cybersecurity.



SUBJECT: Cybersecurity Tips

Thank you for participating in our study earlier today. Below you will find links to some helpful information on how to protect your online security, if you are interested. If you have any questions or concerns about the study, please feel free to contact us at [redacted]

Do you consider the source?
Think before you open, reply to, or click on links or attachments in emails from unknown sources. And never give out your credit card or account information.

Are you sharing too much?
Fingerprint authentication and device passwords are great security measures. Sharing them with anyone can put your information at risk.

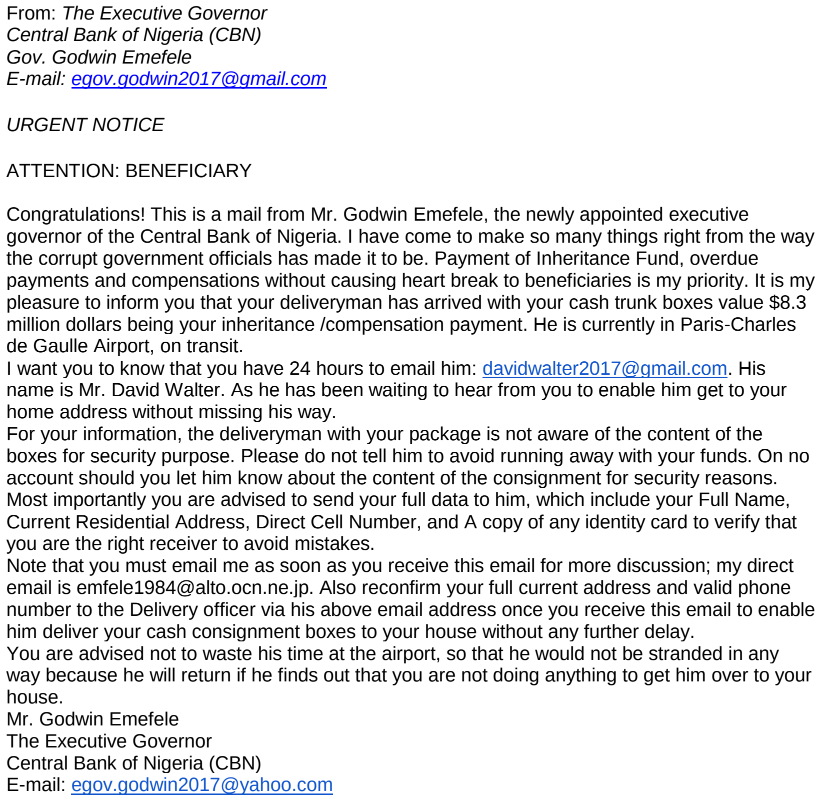
Are you using one password for your accounts?
Create a unique password for your bank accounts that's different from your social media, email or shopping passwords.

Is your smartphone smart enough to protect you?
Turn on mobile app notifications/alerts for financial institution apps to help you manage your accounts securely.

Figure 4: *Follow-up Email*

6 Spam Email

We sent the email below (Figure 5) to all participants a week after they participated in the study.



From: *The Executive Governor*
Central Bank of Nigeria (CBN)
Gov. Godwin Emefele
E-mail: *egov.godwin2017@gmail.com*

URGENT NOTICE

ATTENTION: BENEFICIARY

Congratulations! This is a mail from Mr. Godwin Emefele, the newly appointed executive governor of the Central Bank of Nigeria. I have come to make so many things right from the way the corrupt government officials has made it to be. Payment of Inheritance Fund, overdue payments and compensations without causing heart break to beneficiaries is my priority. It is my pleasure to inform you that your deliveryman has arrived with your cash trunk boxes value $8.3 million dollars being your inheritance /compensation payment. He is currently in Paris-Charles de Gaulle Airport, on transit.
I want you to know that you have 24 hours to email him: davidwalter2017@gmail.com. His name is Mr. David Walter. As he has been waiting to hear from you to enable him get to your home address without missing his way.
For your information, the deliveryman with your package is not aware of the content of the boxes for security purpose. Please do not tell him to avoid running away with your funds. On no account should you let him know about the content of the consignment for security reasons.
Most importantly you are advised to send your full data to him, which include your Full Name, Current Residential Address, Direct Cell Number, and A copy of any identity card to verify that you are the right receiver to avoid mistakes.
Note that you must email me as soon as you receive this email for more discussion; my direct email is emfele1984@alto.ocn.ne.jp. Also reconfirm your full current address and valid phone number to the Delivery officer via his above email address once you receive this email to enable him deliver your cash consignment boxes to your house without any further delay.
You are advised not to waste his time at the airport, so that he would not be stranded in any way because he will return if he finds out that you are not doing anything to get him over to your house.
Mr. Godwin Emefele
The Executive Governor
Central Bank of Nigeria (CBN)
E-mail: egov.godwin2017@yahoo.com

Figure 5: *Follow-up Spam Email*

7 Additional Results

7.1 Correlations between Variables

This section analyzes some basic correlation patterns among our variables. Figure 6 displays a correlation matrix between our moderators and dependent variables (DV).

Computer Safety is positively correlated with both *Cyber Knowledge* and *Behavior Scale*, suggesting that people who care about their online safety are *already* more knowledgeable about current cyber threats and are, perhaps, not as likely to be affected by our manipulation. *Cyber Knowledge* is also positively correlated with both *Privacy Concerns* and *Behavior Scale*, suggesting that the respondents who follow the news about cyber operations are more concerned about their privacy at baseline and, thus, are already involved in more careful online behavior.

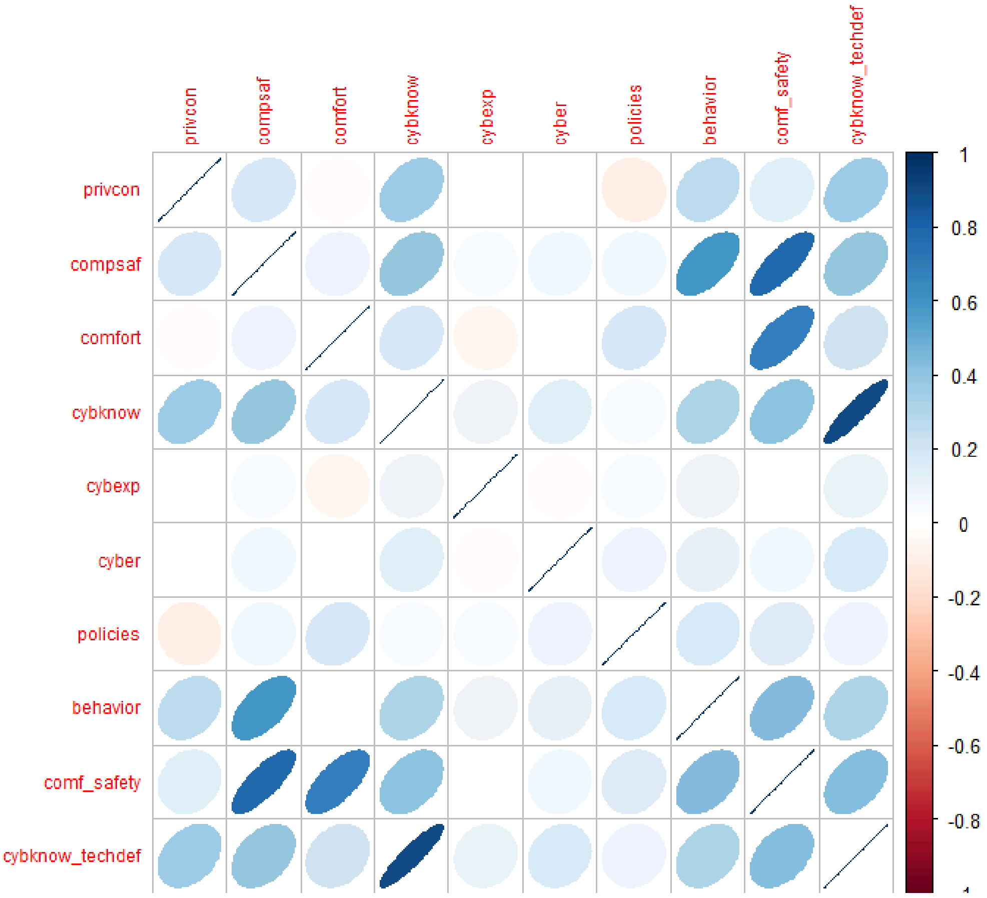


Figure 6: Correlation Matrix between Moderators and DVs

7.2 Main Effects: Regression Tables

This section provides the regression tables corresponding to each main effect described in the text. These tables include the tests of the main effect of treatment on each policy independently, as well as the policies together as one scale. Since different types of cybersecurity policies will confront different types of cybersecurity issues, this allows us to test whether support for certain types of cybersecurity policies changes in response to exposure. For example, it is possible that, because the prompt discusses a data-breach, support for policies having to do specifically with data-breaches of this sort are most likely to increase. However, we do not find support for this hypothesis — support for each cybersecurity policy was indistinguishable from the control condition (Table 3).

Table 1: Threat perceptions

	Gov. cyber attack likely	**Civilian cyber attack likely**	**Personal victim**	**Assessed cyber risk**
National	0.051^	0.013	−0.005	0.032
	(0.026)	(0.024)	(0.026)	(0.032)
Personal	0.041	0.069**	0.044^	0.082**
	(0.026)	(0.024)	(0.026)	(0.031)
Constant	0.730**	0.779**	0.681**	0.497**
	(0.018)	(0.017)	(0.018)	(0.022)
N	437	437	437	435
R-squared	0.010	0.021	0.010	0.016
Adj. R-squared	0.005	0.016	0.005	0.011
Residual Std. Error	0.224 (df = 434)	0.206 (df = 434)	0.221 (df = 434)	0.269 (df = 432)
F Statistic	2.151 (df = 2; 434)	4.640* (df = 2; 434)	2.196 (df = 2; 434)	3.465* (df = 2; 432)

**p < .01; *p < .05; ^p < .1

Table 2: Spending preferences

	Support for increased budget
National	0.052**
	(0.019)
Personal	0.046*
	(0.020)
Constant	0.723**
	(0.014)
N	436
R-squared	0.020
Adj. R-squared	0.015
Residual Std. Error	0.167 (df = 433)
F Statistic	4.306* (df = 2; 433)

**p < .01; *p < .05; ^p < .1

Table 3: Support for cybersecurity policies

	All Policies	**Deterrence by retaliation**	**Harsh legal penalties**	**Share intel with allies**	**Mandate breach disclosures**	**Education in schools**	**Match tech salaries**
National	0.011	0.030	0.021	−0.017	0.013	0.032	−0.015
	(0.017)	(0.031)	(0.028)	(0.029)	(0.026)	(0.028)	(0.026)
Personal	0.003	0.017	−0.010	−0.011	−0.006	0.030	−0.001
	(0.017)	(0.031)	(0.028)	(0.029)	(0.026)	(0.028)	(0.026)
Constant	0.555**	0.414**	0.566**	0.498**	0.619**	0.595**	0.638**
	(0.012)	(0.022)	(0.020)	(0.020)	(0.018)	(0.019)	(0.018)
N	433	434	434	433	434	435	434
R-squared	0.001	0.002	0.003	0.001	0.001	0.004	0.001
Adj. R^2	-0.004	-0.002	-0.002	-0.004	-0.003	-0.001	-0.004
Res.Std.Error	0.145 (df = 430)	0.267 (df = 431)	0.239 (df = 431)	0.248 (df = 430)	0.223 (df = 431)	0.237 (df = 432)	0.225 (df = 431)
F Statistic	0.239 (df = 2; 430)	0.470 (df = 2; 431)	0.630 (df = 2; 431)	0.167 (df = 2; 430)	0.272 (df = 2; 431)	0.833 (df = 2; 432)	0.200 (df = 2; 431)

**p < .01; *p < .05; $^{\wedge}$p < .1

Table 4: Support for cybersecurity policies

	Deterrence by retaliation	Legal penalties	Share intelligence	Breach disclosures	School education	Match tech salaries
National	0.030	0.021	−0.017	0.013	0.032	−0.015
	(0.031)	(0.028)	(0.029)	(0.026)	(0.028)	(0.026)
Personal	0.017	−0.010	−0.011	−0.006	0.030	−0.001
	(0.031)	(0.028)	(0.029)	(0.026)	(0.028)	(0.026)
Constant	0.414**	0.566**	0.498**	0.619**	0.595**	0.638**
	(0.022)	(0.020)	(0.020)	(0.018)	(0.019)	(0.018)
N	434	434	433	434	435	434
R-squared	0.002	0.003	0.001	0.001	0.004	0.001
Adj. R-squared	-0.002	-0.002	-0.004	-0.003	-0.001	-0.004
Residual Std. Error	0.267 (df = 431)	0.239 (df = 431)	0.248 (df = 430)	0.223 (df = 431)	0.237 (df = 432)	0.225 (df = 431)
F Statistic	0.470 (df = 2; 431)	0.630 (df = 2; 431)	0.167 (df = 2; 430)	0.272 (df = 2; 431)	0.833 (df = 2; 432)	0.200 (df = 2; 431)

$^{**}p < .01$; $^{*}p < .05$; $^{\wedge}p < .1$

Table 5: Online Behavior

	Willingness to Use Safer Online Behavior
National	0.002
	(0.023)
Personal	0.040^
	(0.023)
Constant	0.457**
	(0.016)
N	397
R-squared	0.010
Adj. R-squared	0.005
Residual Std. Error	0.184 (df = 394)
F Statistic	1.913 (df = 2; 394)

**p < .01; *p < .05; ^p < .1

Table 6: Behavior Measures

	Open Email with Info about Online Security	**Click Links to Access Info on Online Security**	**Susceptibility to Spam Email**
National	−0.096^	0.029	−0.005
	(0.052)	(0.031)	(0.048)
Personal	0.012	−0.005	0.090
	(0.052)	(0.031)	(0.057)
Constant	0.753**	0.067**	0.180**
	(0.036)	(0.022)	(0.032)
Observations	441	441	350
R^2	0.012	0.003	0.009
Adjusted R^2	0.007	−0.001	0.003
Residual Std. Error	0.445 (df = 438)	0.264 (df = 438)	0.398 (df = 347)
F Statistic	2.581^ (df = 2; 438)	0.708 (df = 2; 438)	1.592 (df = 2; 347)

^p<0.1; *p<0.05; **p<0.01

7.3 Heterogeneous Treatment Effects: Regression Tables

This section provides the regression tables corresponding to each heterogeneous effect described in the text: 1) *Cyber Knowledge*; 2) *Privacy Concern*; 3) *Computer Safety*; 4) *Comfort with Computers*, and 5) *Previous Exposure to Cyber Operations.*

Table 7: Heterogeneous treatment effects: Cyber (Tech) knowledge

	Assessed cyber risk
National	0.090^
	(0.052)
Personal	0.118*
	(0.052)
Cyber knowledge	0.188**
	(0.059)
National X Cyber knowledge	−0.127
	(0.087)
Personal X Cyber knowledge	−0.077
	(0.085)
Constant	0.406**
	(0.036)
N	435
R-squared	0.048
Adj. R-squared	0.036
Residual Std. Error	0.266 (df = 429)
F Statistic	4.282** (df = 5; 429)

**p < .01; *p < .05; ^p < .1

Table 8: Heterogeneous treatment effects: Privacy concerns

	Assessed cyber risk
National	0.160
	(0.108)
Personal	0.325**
	(0.112)
Privacy concerns	0.223^
	(0.116)
National X Privacy concerns	−0.196
	(0.157)
Personal X Privacy concerns	−0.364*
	(0.160)
Constant	0.351**
	(0.079)
N	433
R-squared	0.028
Adj. R-squared	0.017
Residual Std. Error	0.269 (df = 427)
F Statistic	2.464* (df = 5; 427)

**p < .01; *p < .05; ^p < .1

Table 9: Heterogeneous treatment effects: Computer Safety

	Assessed cyber risk
National	0.407**
	(0.111)
Personal	0.323**
	(0.108)
Computer safety	0.569**
	(0.151)
National X Computer safety	−0.774**
	(0.217)
Personal X Computer safety	−0.499*
	(0.208)
Constant	0.221**
	(0.077)
N	427
R-squared	0.052
Adj. R-squared	0.041
Residual Std. Error	0.264 (df = 421)
F Statistic	4.663** (df = 5; 421)

**p < .01; *p < .05; ^p < .1

Table 10: Heterogeneous treatment effects: Comfort Using Computers

	Assessed cyber risk
National	0.090^
	(0.052)
Personal	0.118*
	(0.052)
Comfort	0.188**
	(0.059)
National X Comfort	−0.127
	(0.087)
Personal X Comfort	−0.077
	(0.085)
Constant	0.406**
	(0.036)
N	435
R-squared	0.048
Adj. R-squared	0.036
Residual Std. Error	0.266 (df = 429)
F Statistic	4.282** (df = 5; 429)

**p < .01; *p < .05; ^p < .1

Table 11: Heterogeneous treatment effects: Previous Exposure to Cyber Operations

	Assessed cyber risk
National	−0.054
	(0.056)
Personal	0.011
	(0.055)
Previous Exposure	−0.102
	(0.079)
National X Previous Exposure	0.198^
	(0.112)
Personal X Previous Exposure	0.168
	(0.106)
Constant	0.541**
	(0.040)
N	435
R-squared	0.025
Adj. R-squared	0.014
Residual Std. Error	0.270 (df = 429)
F Statistic	2.190^ (df = 5; 429)

**p < .01; *p < .05; ^p < .1

8 Robustness Checks

Here, we perform additional robustness checks. First, we include those seven participants that fail two of our data checks (Section 8.1). Second, we check the correlation between participant's party ID, their ideology, and their support for cybersecurity policies (Section 8.2). If the correlation is relatively high, we then run an interaction model to determine if respondents' policy views post-treatment are bifurcated by ideology or party ID.

8.1 Including Participants who Failed Data Checks

In our original analysis, we excluded seven participants from our analyses because they fail two of our data checks: 1) they did not answer our attention question correctly; and 2) they spent less than five seconds on article reading. In this section, we present our results for the sample that contains those seven participants.

Table 12 confirms our earlier findings. As compared to respondents in the control condition, respondents in the national (but not personal) threat condition are significantly more likely to believe that another attack against the United States government will happen in the next year ($\beta = 0.05, p < 0.05$). Likewise, as compared to respondents in the control condition, respondents in the personal (but not national) threat condition are significantly more likely to believe that another attack against citizens of the United States will happen in the next year ($\beta = 0.06, p < 0.05$). Moreover, as compared to respondents in the control condition, respondents in the personal threat condition were marginally more likely to believe that they personally would be the victim of a cyber operation in the next year ($\beta = 0.04, p < .1$). Lastly, as compared to respondents in the control condition, respondents in the personal threat condition were also significantly more likely to rank being the victim of a cyber operation as a higher personal risk, when compared to other risks such as terrorism, gun violence, etc. ($\beta = 0.08, p < 0.05$). In contrast, respondents in the national threat condition were no more likely to rank being the victim of a cyber operation as a higher personal risk.

Table 12: Robustness Checks: Threat perceptions

	Gov. cyber attack likely	**Civilian cyber attack likely**	**Personal victim**	**Assessed cyber risk**
National	0.054*	0.016	−0.003	0.031
	(0.026)	(0.024)	(0.026)	(0.032)
Personal	0.035	0.064**	0.043^	0.078*
	(0.026)	(0.024)	(0.026)	(0.031)
Constant	0.730**	0.779**	0.681**	0.497**
	(0.019)	(0.017)	(0.018)	(0.022)
N	444	444	444	440
R-squared	0.010	0.017	0.009	0.014
Adj. R-squared	0.005	0.013	0.005	0.010
Residual Std. Error	0.227 (df = 441)	0.207 (df = 441)	0.221 (df = 441)	0.270 (df = 437)
F Statistic	2.178 (df = 2; 441)	3.891* (df = 2; 441)	2.038 (df = 2; 441)	3.128* (df = 2; 437)

**p < .01; *p < .05; ^p < .1

We then examine what effects this exposure and increased threat perception have on actual political attitudes. Similarly, this analysis confirms our earlier findings. Specifically, as compared to respondents in the control condition, respondents in both the national ($\beta = 0.05, p < 0.05$) and personal threat ($\beta = 0.05, p < 0.05$) conditions were significantly more likely to support higher government spending on cybersecurity programs (Table 13).

Table 13: Robustness Checks: Spending preferences

	Support for increased budget
National	0.052**
	(0.019)
Personal	0.047*
	(0.019)
Constant	0.723**
	(0.014)
N	443
R-squared	0.020
Adj. R-squared	0.015
Residual Std. Error	0.167 (df = 440)
F Statistic	4.396* (df = 2; 440)

**p < .01; *p < .05; ^p < .1

Similarly, the respondents in both personal ($\beta = -0.001, p = NA$) and national ($\beta = 0.011, p = NA$) threat conditions were no more likely to support any of the cybersecurity policies suggested by experts (Table 14).

Table 14: Robustness Checks: Support for cybersecurity policies

	Support for cybersecurity policies
National	0.011
	(0.017)
Personal	−0.001
	(0.017)
Constant	0.555**
	(0.012)
N	439
R-squared	0.001
Adj. R-squared	-0.003
Residual Std. Error	0.148 (df = 436)
F Statistic	0.267 (df = 2; 436)

**p < .01; *p < .05; ^p < .1

Unlike in the main analysis, the respondents in *both* personal ($\beta = 0.034, p = NA$) and national ($\beta = 0.004, p = NA$) threat condition were no more likely to report that they would engage in a variety of safer online security behaviors. (Table 15).

Table 15: Robustness Checks: Online Behavior

	Safer online behavior
National	0.004
	(0.023)
Personal	0.034
	(0.023)
Constant	0.457**
	(0.016)
N	402
R-squared	0.007
Adj. R-squared	0.002
Residual Std. Error	0.185 (df = 399)
F Statistic	1.360 (df = 2; 399)

**p < .01; *p < .05; ^p < .1

Lastly, as compared to the subjects in the control group, respondents in the national threat condition were marginally less likely to open an email, which provided cybersecurity tips ($\beta = -0.091, p < 0.1$). Though subjects in the personal threat condition *said* they would engage in safer online behaviors, they, again, did not. They were no more likely to seek out information on cybersecurity in response to our follow-up email (by opening the email or clicking the links) but were, interestingly, marginally *more* susceptible to spamming attempts ($\beta = 0.106, p < 0.1$), as compared to the control group (Table 16).

Table 16: Robustness Checks: Behavior Measures

	Open	**Links**	**Spam**
National	−0.091^	0.028	−0.007
	(0.051)	(0.030)	(0.048)
Personal	0.020	−0.007	0.106^
	(0.051)	(0.030)	(0.056)
Constant	0.753**	0.067**	0.180**
	(0.036)	(0.021)	(0.033)
Observations	441	441	350
R^2	0.012	0.003	0.009
Adjusted R^2	0.007	−0.001	0.003
Residual Std. Error	0.445 (df = 438)	0.264 (df = 438)	0.398 (df = 347)
F Statistic	2.581^ (df = 2; 438)	0.708 (df = 2; 438)	1.592 (df = 2; 347)

**p < .01; *p < .05; ^p < .1

8.2 Correlation of Party ID and Ideology with Cybersecurity Policy Preferences

Since party affiliation can potentially affect respondent's support for governmental policies, we first check to see if these views are in fact correlated. Figure 7 demonstrates, however, that correlations between party ID and cybersecurity policies, and ideology and cybersecurity policies are rather low, confirming that respondents' party affiliation is *not* strongly associated with their support for cybersecurity policies.

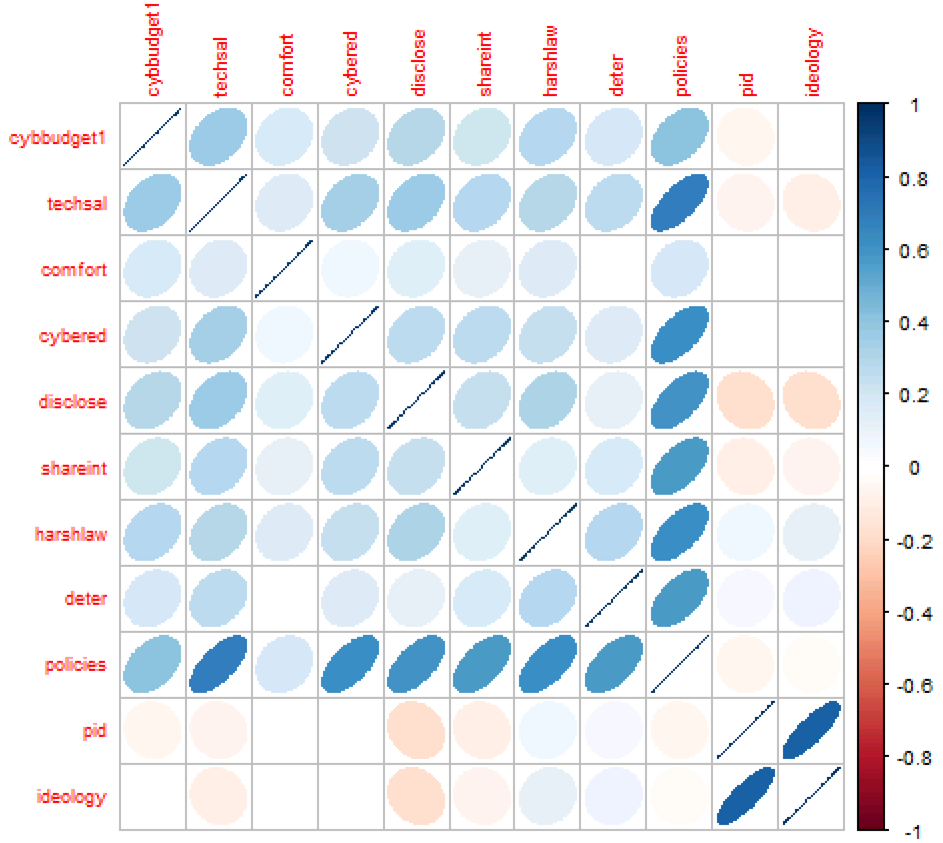


Figure 7: Correlation Matrix between Party ID and Cybersecurity Policies

Since there are a few variable which are correlated with partisanship and ideology, we run our regression analysis using these cybersecurity policies as our dependent variable with an interaction term between *party ID* and the treatment condition (and again with *ideology*). Table 17 demonstrates that party ID has no effect on the respondent's support of requiring private companies to disclose information on their data breaches to the government. Table 18 demonstrates that after exposure to the personal cyber operations, liberals are somewhat more likely to support all cybersecurity policies, in particular the U.S. government's decision to transfer a portion of the Department of Education's school programming budget into a new, mandatory program for schools to teach about cyber hygiene.

Table 17: Robustness Checks: Party ID & Support for cybersecurity policies

	All Policies	**Deterrence by retaliation**	**Harsh legal penalties**	**Share intel with allies**	**Mandate breach disclosures**	**Education in schools**	**Match tech salaries**
National	0.017	0.032	0.020	0.012	−0.023	0.050	0.009
	(0.023)	(0.042)	(0.037)	(0.039)	(0.034)	(0.037)	(0.035)
Personal	0.021	0.030	−0.005	0.037	0.017	0.041	0.008
	(0.023)	(0.043)	(0.038)	(0.039)	(0.035)	(0.038)	(0.036)
PartyID	0.007	0.063	0.065	0.021	−0.122*	0.026	−0.008
	(0.037)	(0.068)	(0.061)	(0.063)	(0.056)	(0.060)	(0.057)
Nat. X PartyID	−0.021	−0.003	0.009	−0.101	0.125	−0.065	−0.085
	(0.052)	(0.096)	(0.086)	(0.089)	(0.079)	(0.085)	(0.081)
Pers. X PartyID	−0.055	−0.047	−0.020	−0.148^	−0.056	−0.038	−0.029
	(0.051)	(0.094)	(0.084)	(0.086)	(0.077)	(0.083)	(0.079)
Constant	0.553**	0.395**	0.547**	0.492**	0.654**	0.587**	0.640**
	(0.016)	(0.030)	(0.026)	(0.027)	(0.024)	(0.026)	(0.025)
N	433	434	434	433	434	435	434
R-squared	0.006	0.006	0.010	0.015	0.038	0.005	0.008
Adj. R-squared	-0.006	-0.005	-0.001	0.004	0.026	-0.006	-0.003
Residual Std. Error	0.15(df = 427)	0.27(df=428)	0.24(df=428)	0.25(df=427)	0.22(df=428)	0.24(df=429)	0.23(df=428)
F Statistic	0.507 (df=5;427)	0.53(df=5;428)	0.90(df=5;428)	1.34(df=5;427)	3.34**(df=5;428)	0.46(df=5;429)	0.70(df=5;428)

**p < .01; *p < .05; ^p < .1

Table 18: Robustness Checks: Ideology & Support for cybersecurity policies

	All **Policies**	**Deterrence** **by retaliation**	**Harsh legal** **penalties**	**Share intel** **with allies**	**Mandate breach** **disclosures**	**Education** **in schools**	**Match tech** **salaries**
National	0.035	0.074	0.017	0.020	−0.034	0.098*	0.034
	(0.031)	(0.056)	(0.050)	(0.051)	(0.046)	(0.050)	(0.047)
Personal	0.049	0.054	0.023	0.046	0.037	0.105*	0.034
	(0.030)	(0.055)	(0.049)	(0.050)	(0.045)	(0.048)	(0.046)
Ideology	0.041	0.163^	0.157^	0.020	−0.168^	0.102	−0.025
	(0.051)	(0.093)	(0.083)	(0.085)	(0.077)	(0.082)	(0.078)
Nat. X Ideology	−0.065	−0.103	0.007	−0.100	0.144	−0.190	−0.151
	(0.075)	(0.138)	(0.123)	(0.125)	(0.114)	(0.122)	(0.115)
Pers. X Ideology	−0.124^	−0.093	−0.099	−0.171	−0.110	−0.188^	−0.095
	(0.070)	(0.129)	(0.115)	(0.117)	(0.106)	(0.113)	(0.108)
Constant	0.541**	0.354**	0.512**	0.498**	0.677**	0.557**	0.649**
	(0.021)	(0.039)	(0.034)	(0.035)	(0.032)	(0.034)	(0.032)
N	419	420	420	419	420	421	420
R-squared	0.010	0.013	0.020	0.011	0.045	0.014	0.018
Adj. R-squared	-0.002	0.001	0.008	-0.001	0.034	0.003	0.006
Residual Std. Error	0.15(df=413)	0.27(df=414)	0.24(df= 414)	0.24(df=413)	0.22(df=414)	0.24(df=415)	0.22(df=414)
F Statistic	0.86(df=5;413)	1.11(df=5;414)	1.67(df=5;414)	0.91(df=5;413)	3.95**(df=5;414)	1.22(df=5;415)	1.49 (df=5;414)

**p < .01; *p < .05; ^p < .1

References

Dinev, Tamara, Paul Hart and Michael R Mullen. 2008. "Internet privacy concerns and beliefs about government surveillance–An empirical investigation." *The Journal of Strategic Information Systems* 17(3):214–233.

Egelman, Serge and Eyal Peer. 2015. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM pp. 2873–2882.

Gadarian, Shana Kushner. 2010. "The politics of threat: How terrorism news shapes foreign policy attitudes." *The Journal of Politics* 72(02):469–483.

Huddy, Leonie, Stanley Feldman, Charles Taber and Gallya Lahav. 2005. "Threat, anxiety, and support of antiterrorism policies." *American journal of political science* 49(3):593–608.

Politics, U.S. and Policy. 2016. "Party affiliation among voters: 1992-2016." *Pew Research Center* .

Shaft, Teresa M, Mark P Sharfman and Wilfred W Wu. 2004. "Reliability assessment of the attitude towards computers instrument (ATCI)." *Computers in human behavior* 20(5):661–689.