GFER Publishers

International Journal of Applied Service Marketing Perspectives

ISSN (Print) 2279-0977
ISSN (Online) 2279-0985
Volume 13 Issue 2, 2024
Pages 48-58

Open Access

Examining the Influence of Cybersecurity Awareness on Online Behavior

Publication Details

Paper Received:
August 11, 2024

Paper Accepted:
December 13, 2024

Paper Published:
December 30, 2024

Hania Afzal
Balochistan University of Information Technology,
Engineering and Management Sciences, Quetta, Pakistan

Email address: hania.afzal@buitms.edu.pk.

Abstract

Internet access is now a must for many companies; much like electricity, it is a basic necessity that cannot be done without it. However, protecting sensitive data is crucial in both personal and professional contexts. Information security cannot be ensured by technology alone, according to experts. The actions of users are crucial to take into account in this field. The Internet is a massive system where data breaches are highly probable. Users, whether malicious or careless, pose a significant danger to information security because they can compromise its confidentiality, integrity, and availability. Mistakes include using the same password for many accounts, downloading software from the internet, writing passwords on sticky paper, and utilising personal information such as a social security number. Most security incidents are caused by user error, whether accidental or malicious, or by their unwillingness to cooperate due to laziness or indifference. The provided model aims to mitigate the risk associated with the poor information security behaviour of users, which is the key issue in this space. Structural equation modelling (SEM) analyses revealed a positive correlation between user behaviour and several factors related to information security, including: awareness; organisation policy; experience and involvement; attitude towards information security; subjective norms; threat appraisal; and self-efficacy.

Keywords: attitude; behavior; cyber operations; cyber threat; online; risk perception

1. Introduction

1.1 The Paradox of Cyber Threat

The Paradox of Cyber threat Russia's cyber activities undertaken during the 2016 US presidential election have highlighted the growing role played by cyber operations 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", security experts contend that the origin and target of most cyberthreats 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 US 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. 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 toward the Democratic nominee and impacted the outcome of the 2016 US election. Indeed, according to NBC News, the Trump campaign mentioned

Wikileaks at least 145 times in the last month of the presidential race (Murray, 2017).

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 more than fifty-seven million drivers and riders, the 2017 Equifax hack compromised the financial records of 145.5 million US customers or about 45 percent of the US 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 cyberoperations: the WannaCry hackers used cybertools 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 cyberoperations and the primary reason the perpetrators were successful: user error. In other words, many of the most notable recent cyberoperations around the world have been as serious as they have been preventable. In fact, cybersecurity experts estimate that up to 93 percent of data breaches—a particularly prominent type of cyberoperation 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 cyberoperations, and data breaches in particular, could be vastly diminished, drastically reducing economic and security threats to both individuals and the state from cyberattacks.

However, despite these and other high-profile cyberoperations in recent years targeting government, corporate, and individual targets, many computer users still fail to engage in even the most basic cyberhygiene practices. This is problematic not just from a consumer or industry perspective, but also for national security writ large. Because cyberoperations 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 US federal government alone employs more than two 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 more than 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 percent of Internet users report using a password management software, 41 percent report sharing passwords with friends or family, and 54 percent use public Wi-Fi networks to conduct sensitive online activity, such as banking (Olmstead & Smith, 2017b). This is a major reason why up to 30 percent 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). 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. This lack of care in personal online behavior is striking because cybersecurity is often mentioned by citizens as an important security concern. In 2014, 91 percent of Americans surveyed by PEW felt that consumers had lost control over how their personal information was collected and used by companies, and 81 percent 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 cyberattacks will be a fact of life in the future" (Olmstead & Smith, 2017a). 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 cyberoperations are 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.

1.2 Risk Perception and Attitudes toward Cybersecurity

International political threats, including in the realm of cyberspace, 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, "[m]any 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, 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 (Jervis, 1976; Levy, 1983; Goldgeier & Tetlock, 2001; McDermott, 2001), affecting, for example, the conduct of crisis bargaining (Jervis 1992), preventative wars (Levy, 1992), hostage crises (McDermott, 2001), and deterrence (Stein, 1986).

However, we know surprisingly little about how the public views risk in the so-called "fifth domain," cyberspace (Heal & Bunker, 2014). That is because, to date, most academic work on cybersecurity has focused on the macrosecurity dynamics of cyberwarfare rather than a bottom-up perspective investigating the attitudes of individual citizens. While this macroapproach has shed important light on the overall strategic and technical environments in which cyberoperations are used, it does not delve into the attitudes and behavior of individual computer users or the implications this may have for macrolevel national security. Thus, we do not have strong empirical evidence regarding how individuals assess the risk from cyberoperations 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, patterns of collective action (Lupia & Sin, 2003), and the transformation of the citizen-bureaucrat relationship (Scavo & Shi, 2000; Bovens & Zouridis, 2002; Mossberger, Tolbert, & Stansbury, 2003; Welch & Fulla, 2005). 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 user or engineer error (Libicki, 2007; Gartzke & Lindsay, 2015), as this is thought to represent the greatest vulnerability to 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 in US history, the personal data of 22.1 million people, including federal employees, contractors, families, and friends from security clearance forms dating back to 1985, were stolen. Security experts have cited "sloppy cyberhygiene" 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 itself 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 large potential consequences that the lack of individual cyberhygiene 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 (Zaller, 1992; Bartels, 2000; Lenz, 2013), others emphasize the conditions under which bottom-up processes predominate (Edwards. 2006; Gelpi, 2010; Levendusky & Horowitz, 2012; Kertzer & Zeitzoff, 2017). 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 & Shotts, 2004), when elections are close (Canes-Wrone & Shotts, 2004), and when there is a robust opposition and independent media (Baum & 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, 2019). These attitudes thus form the political climate in which politicians then operate. If the public is already broadly concerned or in favor of 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 cyberthreats. First, overall cyberknowledge appears to be relatively low, at least in the American electorate. A 2017 PEW poll finds that the median respondent was able to correctly answer only five out of thirteen cyberknowledge questions, and fewer than 20 percent were able to correctly answer more than half (Olmstead & Smith, 2017b). At the same time, the American public does tend to believe that a major cyberoperation against the United States will be coming in the next five years— against national infrastructure (70 percent) or the banking system (66 percent) (Olmstead & Smith, 2017a). This finding is mirrored globally—in 2016, 51 percent of respondents across thirty-eight countries named cyberoperations as an important threat to their country, just behind ISIS (62 percent) and climate change (61 percent) (Poushter &

Manevich, 2017). However, at the same time, a full 69 percent of US adults say they are not at all worried about how secure their own online accounts are (Olmstead & Smith, 2017a). 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 & Loewenstein, 2015). We contend that the contradictory nature of citizens' attitudes and behavior toward cyberthreats, 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 cyberoperations—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 cyberoperations. Exposure to very specific stories about acts of cyberterrorism have been shown to increase anxiety (Jarvis, Macdonald & Whiting, 2017). Some politically motivated cyberoperations have even been shown to cause as much emotional distress as typical physical terrorist violence (Canetti, Gross, & Waismel-Manor, 2016) and can lead to a hardening of militant political attitudes in conflict contexts. Essentially, when cyberoperations 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, & 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 cyberthreats (Cheung-Blunden & Ju, 2015), leading individuals to shut down and adopt a fatalistic attitude toward their cybersecurity (Lawson et al., 2016). Thus, in the absence of personal efficacy, information about cyberthreats may simply demobilize citizens.

1.3 Defining Cyberoperations

The world of cyberoperations is incredibly broad and varied. Thus, before proceeding to our study, we provide a brief typology of existing definitions of cyberoperations and clarify which is the primary focus of the present study. While several existing classifications of cyberoperations mainly emphasize goals, we focus on both the motives and effects associated with various types of cyberoperations. Specifically, we distinguish between political and criminal goals of cyberoperations, 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 shut down. For example, during the 2015 attacks 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 & Rohozinski, 2010; MacKinnon, 2013; King, Pan, & Roberts, 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. 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 "cyberweapon," because it caused substantial damage to Iran's nuclear program, destroying one-fifth of its nuclear centrifuges (Lindsay, 2013). Stuxnet was the first known cyberattack to actually destroy physical infrastructure, demonstrating how activities in the cybersphere can spill over into real-world destruction (Kostyuk & 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 cyberoperation 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 & Lindsay, 2015), influence their targets through propaganda efforts (Lindsay forthcoming), or use blackmail to leverage stolen assets for coercive gain (Poznansky & 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 an example of such operations.

References

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillanceAn empirical investigation. *The Journal of Strategic Information Systems, 17*(3), 214-233.

Egelman, S., & Peer, E. (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. 28732882.

Gadarian, S. K. (2010). The politics of threat: How terrorism news shapes foreign policy attitudes. *The Journal of Politics, 72*(02), 469483.

Huddy, L., Feldman, S., Taber, C., & Lahav, G. (2005). Threat, anxiety, and support of antiterrorism policies. *American Journal of Political Science, 49*(3), 593-608.

Politics, U.S. and Policy. (2016). Party a-liation among voters: 1992-2016. Pew Research Center Shaft.

Teresa, M., Sharfman, M. P., & Wu, W. W. (2004). Reliability assessment of the attitude towards computers instrument (ATCI). *Computers in Human Behavior, 20*(5), 661-689.