Journal of the Midwest Association for Information Systems

Volume 2022 | Issue 1 Article 2

Date: 01-31-2022

Broadband Internet Access as a Localized Resource for Facilitating Information Security Knowledge

Kent Marett
Mississippi State University, kmarett@business.msstate.edu

Shan Xiao
Gonzaga University, xiao@gonzaga.edu

Abstract

With an increasing number of threats to cybersecurity, research continues to focus on methods and behaviors by which individuals may better protect themselves. The availability of broadband infrastructure has been proposed to improve city and regional economic, educational, and health-related prospects, but its impact on facilitating security knowledge gathering has yet to be studied. This study assesses the influence of broadband availability, using data collected from 894 Internet users from across the United States, with multiple analysis techniques supported by geographical information systems (GIS). The results indicate that broadband access, in addition to age and education level, is associated with higher levels of security knowledge. Moreover, geographical weighted regression analyses suggest that the significant variables vary in influence based on their locality.

Keywords: Broadband Internet, information security, GIS, rural technology.

DOI: 10.17705/3jmwa.000071

1. Introduction

No matter the locale, broadband Internet access provides substantial benefits to people such as convenience, entertainment, and knowledge, with the hope that the public embraces new technologies and takes advantage of interconnectivity and data. However, Internet users can ill-afford to remain ignorant of security issues while enjoying the benefits the technology offers them. Insufficient information security is a significant vulnerability for both individuals and organizations given the increasing trend of information security breaches over many years, such as data corruption, identify theft, and credit card fraud. Organizations make investments on information security management like traditional technical methods and organization insiders' education to mitigate potential risks. Information security knowledge has been considered as one of the most effective behavior controls (Van Niekerk & Von Solms, 2010) as it positively influences an individual's intentions to protect one's information, resulting in the adoption of secure behaviors and countermeasures. By and large, maintaining current knowledge on topics and issues involving information security decreases the likelihood and damage caused by a security breach (Safa & Von Solms, 2016).

However, little research has been devoted to how the possible obstacle of inadequate broadband Internet access may contribute to a dearth of security knowledge among Internet users. Broadband diffusion does not occur on a regular, orderly basis; rather, it is largely dependent on evolving technology and the availability of public infrastructure funding. The consequences of inadequate access are often most visible in rural areas in which the population may lack the basic abilities to retrieve timely information to complete tasks, to draw from online healthcare or governmental services, or to communicate remotely with others, not to mention the lacking the entertainment and recreational benefits their counterparts in more populated areas enjoy (Slavova & Karanasios, 2018). From all accounts, limited broadband access in rural areas is a global phenomenon. The question is whether the limitations also lead to less secure population when understanding potential threats becomes an issue.

In order to better understand whether access to broadband Internet affects one's level of security knowledge, we draw from Triandis's (1984) original conceptualization of facilitating conditions. With *security knowledge* broadly defined as accurate information or skills pertaining to information security practices (Karjalainen & Siponen, 2011), we sought to investigate the following research questions:

> RQ1. To what degree does broadband Internet serve as a facilitating condition for individuals to stay current on information security knowledge?
>
> RQ2. Does the level of security knowledge among Internet users cluster around specific locations based on the influence of broadband infrastructure and other geographical factors?

To answer the first research question, we used exploratory regression and ordinary least squares (OLS) analyses of data produced by a nationwide survey to examine the influence of broadband Internet on individual security knowledge. The results identified several variables, including two related to broadband access, that helped explain variance in security knowledge. Because broadband access is highly contingent on one's location, we used a number of analytical techniques associated with geographic information systems (GIS) which have been used previously to study the accessibility of services in rural areas (Higgs & White, 1997; Sipple, Francis, & Fiduccia, 2019) to answer the second research question. The spatial assessment included both hotspot analysis and geographically weighted regression (GWR). Based on the previously identified variables, we detected regional clusters of high and low security knowledge and determined that the influence of broadband access appeared to fluctuate based on location.

2. Theory Review

To our knowledge, there is little to no research examining the capabilities provided by broadband access to gain and maintain current knowledge of information security, with one exception. In an exploratory study, Grobler, van Vuuren, and Zaaiman (2011) observed that citizens in rural South Africa who are deprived of broadband access tend to lack sufficient cybersecurity awareness, putting them in a vulnerable position that could be prevented with further investment into network infrastructure. To expand theoretically on that previous study, we draw from the underpinnings of Perceived

Behavioral Control by positioning broadband access as a facilitating condition for improving one's security knowledge, followed by theoretical rationale laid out by Social Learning Theory.

2.1 Perceived Behavioral Control and Facilitating Conditions

Ajzen's (2002) work on behavioral control stipulated that the absence of external resources could hinder performance no matter how high one's perceived efficacy and controllability may be. To that end, Triandis (1984) was among the first to put forth the notion of these external resources as "facilitating conditions" which, if present, would increase the likelihood of a behavior occurring, particularly when the party involved would need outside assistance in learning the behavior. This has often been operationalized in the IS literature as the degree of organizational support (i.e., company-based supervision and training) available to novices learning a new system (Thompson, Higgins, & Howell, 1991; Venkatesh, Brown, Maruping, & Bala, 2008), but Triandis posited that "the right equipment" also being available is crucial for success. In other words, the training and advice given in support of an attempt to improve one's skill set or increase one's knowledge is wasted if the tools and equipment needed for making the attempt are not present or are inadequate. Triandis' view of equipment and infrastructural support as being critical for facilitation parallels the development of perceived behavioral control by Taylor and Todd (1995a, 1995b). Their work partialed out the concept of "technology facilitating conditions" from other related constructs like self-efficacy and external support services. Taylor and Todd also made certain to note that, while the presence of facilitating conditions is no guarantee that intentions to use or to learn will be formed, the absence of facilitating conditions can impose barriers that prevent the formation of those intentions altogether.

In terms of maintaining a sufficient level of security knowledge to remain safe, the right equipment should include the support infrastructure that delivers current information to the individual. This is a sentiment that parallels work on technological factors necessary for facilitating statistics gathering by Anderson and Whitford (2017), who found that limited Internet availability in some global regions hinders governmental leaders' capacity to maintain timely information. Viewing broadband infrastructure as the "right equipment" for individuals to remain security aware necessarily follows in the spirit of Vourinen and Tetri's (2012) "security machine" and their description of subjection. By connecting one's home or business to the Internet, users are subjugated to security concepts and recommendations in order to keep the connection operational. As security is very much a dynamic exercise, with ever-changing threats, motives, and tools, maintaining an orderly information environment requires an equally dynamic pursuit of security concepts or recommendations. Failure to do so puts the user at a perpetual risk (Vuorinen & Tetri, 2012). As such, we expect that broadband access serves as the right equipment to facilitate staying current on topics and tools pertaining to one's information security.

2.2 Social Learning Theory

An additional theory is required to explain why people connected by broadband Internet would be expected to learn about information security. Social Learning Theory describes how individuals learn about their environment by vicariously observing how others behave within it and the consequences resulting from it, in addition to their own direct exposure to the same environmental conditions (Bandura, 1977). There are two facets of social learning theory that support our expectations that broadband users are likely to learn about information security. The first reason involves the learner's level of self-efficacy, or the level of one's belief to he or she is capable of performing a task. Where learning how to successfully manage a specific technology is concerned, repeated interaction with the technology along with a goal-oriented desire to master its management can motivate the learning process in order to increase one's self-efficacy (Marakas, Yi, & Johnson, 1998). Research on online education utilizes social learning theory to explain, among other facets of learning, how students naturally learn about the tools available to them and how they work by actively interacting with the facilitating technology (Johnson & Aragon, 2003). In a similar vein, we expect that broadband users will have an interest in staying current on how to safely and securely interact with the Internet access they have at their disposal.

The second reason we find social learning theory applicable to this study is the interaction with one's environment and the other people within as motivation for learning. This is the "viacarious capability" that Bandura (1985) models as a useful complement to experiential learning. Acquiring information from observing others' behavior allows for learning that is less constrained by limited time, resources, and mobility needed for personal trial-and-error. As we discuss later, broadband access occurs in geographical pockets with a dense population base. In these geographical areas, Internet providers have made investments in their network infrastructures with the expectation that a significant number of residents and businesses will be interested in subscribing to reliable broadband access. This results in a proximate peer group of Internet users that, while not including everyone within a locale, will have a personal interest in better understanding the access they are subscribing to. In a proximate environment filled with like-minded users, learning about and staying current on a new technology is more readily embraced (Tsai, Shillair, & Cotten, 2017). Within the information security sphere, vicarious learning capabilities have been applied to employees learning about security through their membership in work groups composed of their peers (Abraham & Chengalur-Smith, 2019). We expect that in geographical locales that have broadband infrastructure available, people will have an osmosis-like opportunity to remain security knowledgable that does not exist in non-broadband-provisioned areas.

While organizations are commonly thought to provide much of the information security awareness, training, and knowledge needed by Internet users, efforts to do so are often irregularly offered and differ widely in quality (Hanus & Wu, 2016). Instead, individuals are often on their own for gaining security knowledge. According to previous research (Rader & Wash, 2015) and practitioner survey efforts (Olmstead & Smith, 2017), the main sources of personal security knowledge used by most individuals, for good or bad, frequently exist outside the workplace and include sources found online via social media and security websites. Online sources of security information also include streaming video services like YouTube (Eghan, Moslehi, Rilling, & Adams, 2020) which, by their very nature, require more bandwidth than static webpages. In a similar way in which broadband Internet aids in the conveyence of rich educational and telecommuting opportunities (Kinsell & DaCosta, 2014), broadband users are better equipped to explore and navigate multiple sources of security content than individuals utilizing lower bandwidth. Coupled with the geographic-based inequities of broadband access, we expect that individuals living in “digital deserts” lacking the facilitating infrastructure have relative difficulty maintaining their security knowledge.

2.3 Two Measures of Broadband Access

Though the ultimate focus of this study is determining whether a lack of broadband access could lead to unsatisfactory levels of security knowledge in a deprived locale, a dichotomous measure of broadband access or usage (either present or absent) is insufficient for a few reasons. First, the mere presence of broadband availability does not mean that residents are assured of accessing it. The cost of access may be too expensive to be practical, the individual may not own compatible technology, or the individual may simply be satisfied with existing non-broadband service (Horrigan & Duggan, 2015; Whitacre, Strover, & Gallardo, 2015). Second, we propose that one’s interest in information security will be, at least partially, influenced by one’s neighbors and fellow community members (D'Arcy & Lowry, 2019). In communities in which technology and information security are appreciated and possibly even prioritized, an individual’s awareness may remain better attuned to security topics by virtue of his/her proximity to other aware individuals. Finally, the availability of broadband Internet would be better represented by a continuous measure rather than a binary measure in order to account for the competitive environment within a locale. A larger number of options also helps individuals overcome obstacles like affordability and compatibility (Gulati & Yates, 2012).

3. Method

This study involved the use of both primary and secondary data. The primary data was collected by surveying individual Internet users from across the United States. Government-led studies have concluded that broadband access in the United States is most likely to correlate with population clusters and urban densities (Copps, 2009; Stenberg et al., 2009). Indeed, the Federal Communications Commission (FCC) estimates that one-quarter living in areas defined as “rural” lacked a single fixed broadband provider. This percentage does not include people living in impoverished urban communities (Pick & Nishida, 2015).

Two methods of surveys were conducted in order to procure responses from people across a diverse geographical area in locales ranging in broadband availability. The first round consisted of online survey responses collected through a panel arranged by Qualtrics. Responses were elicited from Internet users living in the United States over the age of 18. A second round of responses was collected via paper surveys administered to Internet users residing in rural areas across seven US states. By administering the instrument in both online and paper versions, reaching a more diverse sample of respondents becomes more likely (Crossler, Bélanger, & Ormond, 2018), particularly when part of the sample is expected to have limited broadband access. T-tests indicated no significant differences in key variables based on the survey method used, and Levene’s tests of inequality showed no significant demographic differences between the two methods. Incomplete surveys were rejected, as were those from respondents who failed an attention check item on the instrument. This method resulted in 894 usable responses.

Overall, the sample was 64 percent composed of female respondents. The mean age of the respondents was 45.5 years, with a mean of 16.5 years living in their current communities. Forty percent of the sample held either a bachelor's or graduate degree, with an additional 34 percent reported having attended some college. In terms of their primary Internet connection, 49 percent used cable modem, with 25 percent subscribing via DSL, 9 percent used their mobile devices, and 6 percent used FTTH (Fiber to the Home). The secondary data was obtained from publicly-available sources in the U.S. federal government, primarily the Federal Communications Commission (the FCC) and the US Census Bureau. The measures collected from both primary and secondary data sources are described in the following section.

3.1 Measures

Based on Triandis's discussion of objective facilitating factors, we represented the "equipment" with two measures of broadband infrastructure. As the zip code and ISP subscription information were reported by survey respondents, as well as the coordinate data associated with each response, we were able to ascertain both (a) the number of broadband options and (b) the potential downstream data rate for each response using the most recent Broadband Progress Report maintained by the FCC. The report tallies the number of Internet service providers for a given location by reporting ISP data rates meeting the FCC standard for broadband, 25 mbps downstream and 3 mbps upstream. 419 respondents lived in areas with one broadband option, with 277 having two options, 112 having no options available, and 86 with three or more (up to six) options.

Other variables pertaining to location and demographics were among the other possible candidate driving factors selected for the study. The FCC report also provided the reported data rate associated with the ISP each respondent subscribed to. For respondents who responded having access through more than one provider (including their Internet connection at work), the largest potential data rate among their providers was used, allowing for more conservative estimates. Some respondents indicated that their mobile device was their sole connection to the Internet, and in those cases we used the 4G potential data rate of 12 mbps (Fleishman, 2010), which was standard most widely available during the data collection period. Demographic variables, including the respondent's age, sex, race, and education level, are thought to associate with broadband usage (Sarkar, Pick, & Rosales, 2016) and were self-reported by the survey respondents. Location-based data, including the population of a resident's community, its population density, and the local median income were all collected from US Census Estimate Reports.

The dependent variable, security knowledge ("SECKNOW"), was assessed using a ten question quiz modeled similarly to knowledge assessments found in other security research (Giboney, Proudfoot, Goel, & Valacich, 2016). Each quiz question regarded a particular threat or countermeasure that relates to implementing one's own personal information security, with the questions drawn from existing security literature (Crossler et al., 2018). Quiz scores ranged from 0 to 10, and the overall mean for SECKNOW was 3.60 correct answers. An ANOVA indicated significant differences in SECKNOW (F=28.04; p<.001) based on the number of broadband options available, ranging from a mean of 6.20 for individuals with five or more options to a means of 4.84 for 2 options, 2.90 for one option, and 2.17 for no broadband option available. A similar statistical difference was found when grouping respondents by downstream data rates (F=24.77; p<.001). The 340 respondents who do not have a rate of 25 mbps had a mean of 2.65 for SECKNOW, which a Bonferroni comparison found to be significantly lower than respondents with 25-100 mbps (M=4.00), respondents between 100-500 mbps (M=4.31), and respondents with downstream rates over 500 mbps (M=4.94).

Comparisons of other measures collected in this study point to differences in the manner in which security knowledge is sought out. Overall, survey respondents reported using online sources (M=4.69) for seeking out security knowledge slightly more frequently than friends (M=4.35) and news media (M=4.51), and roughly equal to accessing sources at work (M=4.71). However, when comparing groups differentiated by the broadband measures, both individuals with access to three or more broadband options (F=6.18; p<.001) and individuals with high downstream data rates (F=3.03; p=.029) were more likely to use online sources for staying current on the latest security information than their broadband-deprived counterparts. Responses to open-ended questions about their information seeking often pointed out the convenience and ability to work alone in private when using online venues like security websites and social media.

The survey instrument was designed following suggestions made by Gregor and Klein (2014) to reduce the chances for common method bias. The dependent variable SECKNOW was collected independently from several of the independent variables, including the broadband access measures. No contextual cues about the nature of the study were provided to the participants prior to the survey's administration; they were merely told the survey asked about their feelings for broadband Internet. Further, the items on the survey instrument itself were randomized and participants were assured of their anonymity.

3.2 Analysis and Results

For data analysis, we followed a similar sequential procedure used in previous spatial analysis research (Feng & Tong, 2017; Marett & Nabors, 2021). First, the potential influence of variables of interest on the dependent variable, SECKNOW, were assessed using exploratory regression. Once variables appearing to have a significant influence were identified, Ordinary Least Squares (OLS) was used to assess their relative strengths of association. Then, the spatial relationships of the variables were examined first using a hot spot analysis to determine spatial clustering of the regression residuals, followed by a geographically weighted regression (GWR) to assess the localized weights of the influential variables. All data analyses described below were performed using ArcMap 10.3.1, though the GWR procedure was replicated using GWR4, a software tool specializing in that analysis.

Table 1 below reports the inter-construct correlations between SECKNOW and the variables described in the preceding section. Specifically, the number of available broadband options ("BROADOPT") and downstream data rate ("DOWN"), demographic variables like the age, sex, race, and education level of the participant, and location-based variables like the population, density, and median income of the participant's resident municipality were considered. SECKNOW was significantly correlated with several of the potential explanatory variables.

	SK	BO	DOWN	Age	Sex	Race	Ed	Pop	Dens
SECKNOW									
BROADOPT	.36**								
DOWN	.17**	.23**							
Age	.07*	-.07*	.01						
Sex	-.11**	-.05	-.01	-.12**					
Race	.03	.10**	-.01	-.06	-.01				
Ed Level	.15**	.15**	.08*	.03	-.11**	.08*			
Population	.02	.15**	.12**	-.08*	-.01	.03	.10**		
Density	-.01	.32**	.05	-.10**	-.04	-.01	.08*	.41**	
Md Income	.06*	.40**	.08*	-.09**	-.06	.06	.18**	.12**	.35**

Table 1. Inter-construct Correlations (two-tailed). NOTE: ** p<.01, * p<.05

First, the exploratory regression included all of the variables described previously, regardless of correlation. None of the exploratory models violated the Jarque-Bera test for normality nor the Global Moran's I test for residual spatial autocorrelation. BROADOPT, DOWN, age, and education level were consistently significant and exclusively positive influences for all tested models, whereas the other variables were mixed influences if significant at all. None of the tested variables showed signs of multicollinearity. Thus, the four significant explanatory variables were included in the subsequent analysis using Ordinary Least Squares (OLS).

The results of the OLS analysis are summarized in Table 2 below. As hinted by the earlier exploratory regression phase, BROADOPT, DOWN, age, and educational level were all found to be significant influences. While age and higher educational levels seem to impact security knowledge to a certain extent, the model explained 15.6 percent of the variance in SECKNOW, with the BROADOPT variable explaining 12 percent on its own. *Post hoc* Global Moran's I tests were conducted to ensure no significant spatial autocorrelation bias was present in the dependent variable. The Variance Inflation Factor (VIF) statistics were also examined in order to assess redundancy among the variables, which is signaled by values over 7.5. None of the variables violated these assumptions.

To identify any possible spatial differences in security knowledge, two separate analysis techniques were undertaken. First, a clustering technique known as a hotspot analysis was conducted on the OLS residuals to determine whether spatial concentrations of security knowledge could be determined. Residuals represent the deviation from security knowledge expectations (based on the variables used in the OLS model) displayed by each respondent. Positive residuals between the observed and expected SECKNOW scores suggest an unexpected "overachievement" for an individual, and

	Unstandardized Coefficient	Standard Error	t-statistic	VIF	Variance Explained
BROADOPT	1.000	0.11	9.31***	1.08	0.12
DOWN	0.002	0.00	2.80***	1.06	0.02
Age	0.018	0.01	3.34***	1.01	0.01
Education	0.233	0.08	2.87***	1.03	0.01
F = 41.07*** Wald-Stat = 161.05*** R^2 = 0.156 Adjusted R^2 = 0.152	*** p < .001 ** p < .01 * p < .05				

Table 2. Results of OLS Analysis.

vice versa for negative residuals. The hotspot analysis calculated Getis-Ord G* statistics, which suggest whether the security knowledge exhibited by geographical neighbors was higher (a "hot spot") or lower (a "cold spot") than would be expected (the global mean based on the regression model) or resulting by random chance. Thus, a statistically significant result identifies a spatial area (here, a US county) that is not only above or below the expected average, it must also be located in a "neighborhood" of counties that show a similar high/low result. The results are graphically represented in Figure 1 below. Several regional clusters of significant hot- and cold spots were revealed, suggesting a localized influence for one or more of the variables.

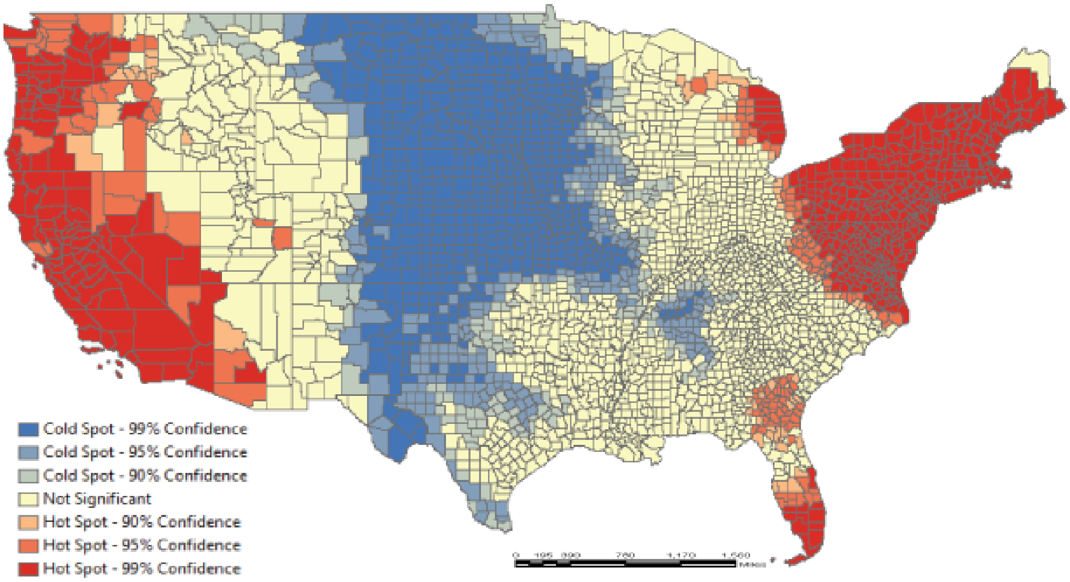
Cold Spot - 99% Confidence
Cold Spot - 95% Confidence
Cold Spot - 90% Confidence
Not Significant
Hot Spot - 90% Confidence
Hot Spot - 95% Confidence
Hot Spot - 99% Confidence
0 195 390 780 1,170 1,560
Miles

Figure 1. Hotspots and Coldspots of Security Knowledge at the County Level.

Thus, a GWR analysis was conducted to determine the level of spatial nonstationarity, i.e., the extent to which the global regression model might be calibrated for a particular locality (Fotheringham, Charlton, & Brunsdon, 1996). GWR supplements OLS by regressing the variables using a local model (i.e., the influence of a data point's neighbors is weighted higher than more distant observations) rather than a global model. By doing so, the resulting model identifies which variables are more influential, depending on their location. GWR has been demonstrated to be robust to all but the most extreme cases of multicollinearity (Fotheringham & Oshan, 2016), which appears not to have been an issue in this study.

A comparison of the OLS and GWR results suggests that the GWR model represents an improvement. The AICc value, which estimates the goodness of fit, was reduced from 4200.0 for the OLS model to 4176.7 for the GWR model, indicating a better model fit. The R^2 improved from 0.156 explained by the OLS model to 0.224 for the GWR model, suggesting a nonstational influence for one or more of the explanatory variables. The largest influence was provided by

BROADOPT with an R^2 of 0.184, with the additional variance explained by DOWN (0.02), education (0.01), and age (0.01). As a test for robustness, the GWR was also tested using an adaptive kernel, which further accounts for locales with different densities of observations (Du, Wu, Zhang, Liu, & Zhou, 2018), with the resulting R^2 lowering to just 0.213 and a slightly lower AICc (4176.0). Neither GWR model exhibited significant spatial autocorrelation. To provide a measure of robustness, the GWR analysis was replicated using GWR4 (Nakaya, 2016), and the results were consistent with those produced in ArcMap. A comparison of the overall GWR results with those from the OLS model is provided in Table 3.

	F	AICc	R^2	Adjusted R^2
OLS	41.07***	4200.0	0.156	0.152
GWR ArcMap (fixed kernel)	n/a	4176.7	0.224	0.185
GWR GWR4 (fixed Euclidean)	n/a	4178.8	0.220	0.181

Table 3. Comparison of OLS and GWR Models.

In sum, the results from the GWR suggest that the variables used in the OLS regression model can vary in their influence on SECKNOW based on the location of a particular observation. A subsequent test of geographical variability using GWR4 indicated that both BROADOPT (-15.81) and DOWN (-4.92) produced negative values when comparing the original regression model and the localized model, as opposed to the positive values for age and education, suggesting that the two broadband access factors contribute the most to localized variability differences.

4. Discussion

The results of the GIS analyses performed in this study can be summarized in the following ways. First, the exploratory regression analysis of both objective "equipment" measures and demographic variables identified variables like the number of available broadband options, the downstream data rate, and the age and educational levels of the respondent as being potentially significant influences on one's level of security knowledge. A follow-up OLS analysis confirmed these four variables as being influential, with BROADOPT contributing the most toward the model's explained variance. This result suggests that, as our first research question asked, broadband Internet can very much be viewed as a facilitating condition for improving one's security knowledge. As we expected, a hotspot analysis revealed geographic areas in the United States where respondents' security knowledge differed significantly from national averages and from what could be predicted by random chance. Finally, by constructing local regression equations via geographically weighted regression, we determined that the regression model demonstrates better fit when accounting for one's location. Variability tests comparing the original regression model and the geographically-weighted model suggest that the two broadband variables are responsible for the majority of any localized variability. Taken together, the results of the hotspot analysis and geographically-weighted regression support the notion that security knowledge can cluster around areas in which broadband Internet access is abundant and competitive, following up on the second research question. The results also support assertions made by social learning theory in which learning is more likely to occur vicariously due to a desire to know more about managing resources (here, the broadband connection and devices connected to it) that are a part of the local environment. The hot spots (and cold spots) identified by the geographical analysis suggest that learning and staying current on information security is very much localized to areas catered to by broadband providers.

In terms of implications for research, we believe the results of this study complements research on broadband investment that speaks to the assumed causality that infrastructure buildout will produce both immediate and long-term societal benefits without first influencing attitudes and behaviors by the newly-connected citizenry. As Pant and Odame (2017) point out, the benefits of improving broadband access will be maximized when technological improvements co-evolve with learning and innovation by customers. Our results highlight one area of this co-evolution. As broadband opportunities improve within an area, the population seems to engage in the learning that will help them take full advantage of the access while protecting them from evolving threats as well. Moreover, we suggest that there may well be a geographical factor to information security that has seldom (if ever) been accounted for. A recent examination of IS artifacts (Lowry, Dinev, & Willison, 2017) thought to be pivotal for security researchers to consider includes a number of social factors, such as cultural, organizational, and group-level influences on individuals. To that list of factors, we would add the need to account for geographical influences, including the availability of broadband connectivity. If there are truly isolated hot spots and cold spots of security knowledge that are, at least partially, related to the relative accessibility of broadband Internet, it would seem to be an oversight to expect that the location of individuals and the organizations they work for will have the same priority on improving security knowledge.

This study also has implications for practitioners, starting with those who are involved with policy-making and investing in the broadband sector. As more communities and providers become involved in expanding broadband into underserved areas, whether through fiber initiatives (George & Petter, 2016) or an inclusive national 5G cellular network, the well-advertised economic, educational, and health benefits associated with broadband access are further bolstered by the results of this study. For business owners and managers, the results of this study take on additional meaning when considering that, despite their efforts to harden their own internal networks and systems, successful security often comes down to the practices of business partners and customers in a "lowest common denominator" environment (Lankton, McKnight, & Tripp, 2017). That is, managers have a vested interest in raising the levels of security education and awareness among members of the public that may have a current (or future) business relationship with. In addition to the other societal benefits discussed earlier in the paper, we believe that the business community should be among the strongest proponents for improving broadband access for their own security.

4.1 Limitations

The results reported here should not be assessed without acknowledging the limitations of this study. First, the data used in this study was collected entirely from Internet users in the United States. While limiting the data collection to one country made the geographical analysis presented here more practical, the cultural differences between nations make the results difficult to compare with cross-national studies on broadband penetration (Gulati & Yates, 2012). However, future research may find that the results here could apply to other geographically large countries or in nations in which the population is sparsely or unevenly distributed across wide areas.

Caution should also be taken when interpreting the results of a hotspot analysis conducted across a wide geographical area, as the physical distance between neighbors could weaken any cultural commonalities existing between data points. The results are the product of analyzing a sample of under 1000 Internet users. Although efforts were made to elicit a diverse geographical sample, we acknowledge there is no guarantee the sample was not fully representative. Also, the results should be assessed with the acknowledgement that sources of security knowledge are not mutually exclusive. While the availability of high-speed Internet might make the use of online sources of information convenient and more easily perused, knowledgeable individuals may have accumulated their information from a number of possible sources over time. As noted by Sandeep and Ravishankar (2018), employees frequently bring job-related information in through semi-permeable organizational boundaries from outside sources, and vice versa. Accordingly, it is increasingly difficult to know what security knowledge came from which source. This issue becomes more concerning as new technologies emerge and become available to consumers (Conger, Pratt, & Loch, 2013), especially rural users, who may not have equal access to security recommendations as others with better broadband.

One additional concern revolves around whether the results potentially suffer from endogeneity due to reverse causality. In other words, does an individual's security knowledge precede subscribing to broadband Internet because he or she feels safe from online threats? Or similarly, would broadband providers seek to develop in areas with existing, highly-knowledgeable Internet users? Van der Stede (2014) suggests reviewing the theoretical causal model to see if results are consistent with the explanation, determining if (at least) a correlational relationship between key variables exists, and then attempt to rule out plausible alternative explanations in order to make a confident, if not assured, argument against reverse causality. Here, our results indicate that the two broadband access variables do correlate significantly with security knowledge and that the OLS analysis supports the theoretical foundation for this study, that broadband Internet serves as a facilitating condition for acquiring security knowledge and that Internet users are better equipped to learn about securing their information due to the presence of their broadband access. The alternative argument for reverse causality suggesting that Internet providers seek out geographical pockets of highly knowledgeable users before building out broadband infrastructure does not seem plausible. Multiple reports and articles spanning the era in which broadband Internet has been commonly available in the United States (Beede & Neville, 2013; Copps, 2009; GAO, 2006; Grubesic & Murray, 2004; Lee, Brown, & Lee, 2011; Stenberg et al., 2009) claim the leading factors for buildout are population density, socioeconomic status, education level, regulatory right-of-way policies, existing or potential competition, and lack of obstruction due to the terrain. The security knowledge of the existing population base does not factor in to broadband infrastructure expansion, to the best of our knowledge.

5. Conclusion

This study represents a first attempt to examine an unexplored consequence of the digital divide in the United States –

a lack of information security knowledge found in areas underserved by broadband access. Ongoing efforts continue to improve broadband accessibility in rural areas of the United States, but the results of this study suggest that there is more to gain from doing so than the well-publicized educational, health, employment, and commercial benefits that individuals desire. Better exposure to information and tools necessary for protecting oneself while online also hangs in the balance, and we hope our results will encourage policy makers to continue deploying broadband access to underserved areas.

6. References

Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the Effectiveness of Learning Controlled Information Security Training. *Computers & Security, 87*.

Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior. *Journal of Applied Social Psychology, 32*(4), 665-683.

Anderson, D., & Whitford, A. (2017). Developing Knowledge States: Technology and the Enhancement of National Statistical Capacity. *Review of Policy Research, 34*(3), 400-420.

Bandura, A. (1977). *Social Learning Theory*. Englewood Cliffs, NJ: Prentice-Hall.

Bandura, A. (1985). Model of Causality in Social Learning Theory. In M. Mahoney & A. Freeman (Eds.), *Cognition and Psychotherapy* (pp. 81-100). Boston MA USA: Springer.

Beede, D., & Neville, A. (2013). Broadband Availability Beyond the Rural/Urban Divide. Washington DC USA: U.S. Department of Commerce.

Conger, S., Pratt, J., & Loch, K. (2013). Personal Information Privacy and Emerging Technologies. *Information Systems Journal*, *23*(5), 401-417.

Copps, M. (2009). *Bringing Broadband to Rural America*. Washington, DC: Federal Communications Commission.

Crossler, R., Bélanger, F., & Ormond, D. (2018). The Quest for Complete Security: An Empirical Analysis of Users' Multi-Layered Protection from Security Threats. *Information Systems Frontiers*, *21*(2), 343-357.

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study. *Information Systems Journal, 29*(1), 43-69.

Du, Z., Wu, S., Zhang, F., Liu, R., & Zhou, Y. (2018). Extending Geographically and Temporally Weighted Regression to Account for Both Spatiotemporal Heterogeneity and Seasonal Variations in Coastal Seas. *Ecological Informatics, 43*, 185-199.

Eghan, E., Moslehi, P., Rilling, J., & Adams, B. (2020). The Missing Link–a Semantic Web Based Approach for Integrating Screencasts with Security Advisories. *Information and Software Technology, 117*(in press).

Feng, Y., & Tong, X. (2017). Using Exploratory Regression to Identify Optimal Driving Factors for Cellular Automaton Modeling of Land Use Change. *Environmental Monitoring and Assessment, 189*(10), 515-532.

Fleishman, G. (2010). The State of 4G: It's All About Congestion, Not Speed. Retrieved 9/10/2020 from https://arstechnica.com/tech-policy/2010/03/faster-mobile-broadband-driven-by-congestion-not-speed/2/

Fotheringham, A. S., Charlton, M., & Brunsdon, C. (1996). The Geography of Parameter Space: An Investigation of Spatial Non-Stationarity. *International Journal of Geographical Information Systems, 10*(5), 605-627.

Fotheringham, A. S., & Oshan, T. (2016). Geographically Weighted Regression and Multicollinearity: Dispelling the Myth. *Journal of Geographical Systems, 18*(4), 303-329.

GAO. (2006). Broadband Deployment Is Extensive Throughout the United States, but It Is Difficult to Assess the Extent of Deployment Gaps in Rural Areas. Washington DC USA: United States Government Accountability Office.

George, J., & Petter, S. (2016). *The Poor Get Poorer and the Rich Get Fiber: Why Free/Low-Cost Internet Might Not Bridge the Digital Divide.* Paper presented at the Twenty-Second Americas Conference on Information Systems, San Diego, CA.

Giboney, J., Proudfoot, J., Goel, S., & Valacich, J. (2016). The Security Expertise Assessment Measure (SEAM): Developing a Scale for Hacker Expertise. *Computers & Security, 60*, 37-51.

Gregor, S., & Klein, G. (2014). Eight Obstacles to Overcome in the Theory Testing Genre. *Journal of the Assocation for Information Systems, 15*(11).

Grobler, M., van Vuuren, J. J., & Zaaiman, J. (2011). *Evaluating Cyber Security Awareness in South Africa.* Paper presented at the 10th European Conference on Cyber Warfare and Security.

Grubesic, T., & Murray, A. (2004). Waiting for Broadband: Local Competition and the Spatial Distribution of Advanced Telecommunication Services in the United States. *Growth & Change, 35*(2), 139-165.

Gulati, G. J., & Yates, D. (2012). Different Paths to Universal Access: The Impact of Policy and Regulation on Broadband Diffusion in the Developed and Developing Worlds. *Telecommunications Policy*, *36*(9), 749-761.

Hanus, B., & Wu, Y. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management, 33*(1), 2-16.

Higgs, G., & White, S. D. (1997). Changes in service provision in rural areas. Part 1: The use of GIS in analysing accessibility to services in rural deprivation research. *Journal of Rural Studies*, 13(4), 441-450.

Horrigan, J., & Duggan, M. (2015). Home Broadband 2015. *Pew Research Center* (Vol. 21). Washington DC.

Johnson, S., & Aragon, S. (2003). An Instructional Strategy Framework for Online Learning Environments. *New Directions for Adult & Continuing Education, 2003*(100), 31-43.

Karjalainen, M., & Siponen, M. (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. *Journal of the Association for Information Systems, 12*(8), article 3.

Kinsell, C., & DaCosta, B. (2014). A 15 Factor and 157 Item Checklist for Assessing Website Usability and Accessibility. In B. DaCosta & S. Seok (Eds.), *Assistive Technology Research, Practice, and Theory* (pp. 252-276). Hershey, PA: IGI Global.

Lankton, N., McKnight, D. H., & Tripp, J. (2017). Facebook Privacy Management Strategies: A Cluster Analysis of User Privacy Behaviors. *Computers in Human Behavior, 76*, 149-163.

Lee, S., Brown, J., & Lee, S. (2011). A Cross-Country Analysis of Fixed Broadband Deployment: Examination of Adoption Factors and Network Effect. *Journalism & Mass Communication Quarterly, 88*(3), 580-596.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda. *European Journal of Information Systems, 26*(6), 546-563.

Marakas, G., Yi, M., & Johnson, R. (1998). The Multilevel and Multifaceted Character of Computer Self-Efficacy: Toward Clarification of the Construct and an Integrative Framework for Research. *Information Systems Research, 9*(2), 126-163.

Marett, K., & Nabors, M. (2021). Local Learning from Municipal Ransomware Attacks: a Geographically Weighted Analysis. *Information & Management*, *58*(7), in press.

Nakaya, T. (2016). Geographically Weighted Generalised Linear Modelling. In C. Brunsdon & A. Singleton (Eds.), *Geocomputation: A Practical Primer* (pp. 201-220). Thousand Oaks, CA: Sage Publications.

Olmstead, K., & Smith, A. (2017). Americans and Cybersecurity. Pew Research Center report.

Pant, L. P., & Odame, H. H. (2017). Broadband for a Sustainable Digital Future of Rural Communities: A Reflexive Interactive Assessment. *Journal of Rural Studies*, 54, 435-450.

Pick, J., & Nishida, T. (2015). Digital Divides in the World and Its Regions: A Spatial and Multivariate Analysis of Technological Utilization. *Technological Forecasting and Social Change, 91*, 1-17.

Rader, E., & Wash, R. (2015). Identifying Patterns in Informal Sources of Security Information. *Journal of Cybersecurity, 1*(1), 121-144.

Safa, N. S., & Von Solms, R. (2016). An Information Security Knowledge Sharing Model in Organizations. *Computers in Human Behavior, 57,* 442-451.

Sandeep, M. S., & Ravishankar, M. N. (2018). Sociocultural Transitions and Developmental Impacts in the Digital Economy of Impact Sourcing. *Information Systems Journal, 28*(3), 563-586.

Sarkar, A., Pick, J., & Rosales, J. (2016). Multivariate and Geospatial Analysis of Technology Utilization in US Counties. Paper presented at the Twenty-second Americas Conference on Information Systems, San Diego, CA.

Sipple, J., Francis, J., & Fiduccia, P. C. (2019). Exploring the gradient: The economic benefits of ‘nearby’schools on rural communities. *Journal of Rural Studies*, 68, 251-263.

Slavova, M., & Karanasios, S. (2018). When Institutional Logics Meet Information and Communication Technologies: Examining Hybrid Information Practices in Ghana's Agriculture. *Journal of the Assocation for Information Systems, 19*(9), 775-812.

Stenberg, P., Morehart, M., Vogel, S., Cromartie, J., Breneman, V., & Brown, D. (2009). *Broadband Internet's Value for Rural America*. Washington, DC: United States Department of Agriculture.

Taylor, S., & Todd, P. (1995a). Decomposition and Cross-over Effects in the Theory of Planned Behavior: A Study of Consumer Adoption Intentions. *International Journal of Research in Marketing, 12*(2), 137-155.

Taylor, S., & Todd, P. (1995b). Understanding Information Technology Usage - a Test of Competing Models. *Information Systems Research, 6*(2), 144-176.

Thompson, R., Higgins, C., & Howell, J. (1991). Personal Computing: Toward a Conceptual Model of Utilization. *MIS Quarterly, 15*(1), 125-143.

Triandis, H. (1984). Toward a Psychological Theory of Economic Growth. *International Journal of Psychology, 19*(1-4), 79-95.

Tsai, H. S., Shillair, R., & Cotten, S. (2017). Social Support and "Playing Around": An Examination of How Older Adults Acquire Digital Literacy with Tablet Computers. *Journal of Applied Gerontology, 36*(1), 29-55.

Van der Stede, W. (2014). A Manipulationist View of Causality in Cross-Sectional Survey Research. *Accounting, Organizations and Society, 39*(7), 567-574.

Van Niekerk, J. F., & Von Solms, R. (2010). Information Security Culture: A Management Perspective. *Computers & Security, 29,* 476-486.

Venkatesh, V., Brown, S., Maruping, L., & Bala, H. (2008). Predicting Different Conceptualizations of System Use: The Competing Roles of Behavioral Intention, Facilitating Conditions, and Behavioral Expectation. *MIS Quarterly, 32*(3), 483-502.

Vuorinen, J., & Tetri, P. (2012). The Order Machine - the Ontology of Information Security. *Journal of the Assocation for Information Systems, 13*(9), 695-713.

Whitacre, B., Strover, S., & Gallardo, R. (2015). How Much Does Broadband Infrastructure Matter? Decomposing the Metro-Non-Metro Adoption Gap with the Help of the National Broadband Map. *Government Information Quarterly, 32*(3), 261-269.

Author Biographies

Kent Marett is an Associate Professor of Business Information Systems and Robert Keil Fellow at Mississippi State University. He received his PhD in Management Information Systems from Florida State University. His research interests involve information security, deceptive communication, and business computing in geographically rural areas. His work has been published in *MIS Quarterly*, the *Journal of the Association for Information Systems*, *Information Systems Research*, and the *Journal of Management Information Systems*, among other top journals.

Shan Xiao is an Assistant Professor of Management Information Systems in the School of Business Administration at Gonzaga University. Her research interest concentrates on individuals' decisions on cybersecurity behaviors, such as persuasive communication, information security compliance, and data privacy issues. She has published in peer-reviewed scientific journals and conferences, such as *The Data Base for Advances in Information Systems*, *AIS Transactions on Replication Research*, and *Americas Conference on Information Systems*. She has also served as a reviewer for several journals and conferences. In addition, she had six years of field experience in information systems at Hewlett Packard and was Project Management Professional (PMP) certified since 2012.

This page intentionally left blank.