International Food and Agribusiness Management Review
Volume 21 Issue 3, 2018; DOI: 10.22434/IFAMR2017.0045

Received: 17 May 2017 / Accepted: 7 September 2017

Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry

RESEARCH ARTICLE

Andrew Geil[a], Glen Sagers[b], Aslihan D. Spaulding[c], and James R. Wolf[ⓘ][d]

[a]*Senior Security Analyst, Compeer Financial, 2000 Jacobssen Drive, Normal, IL 61761,USA*

[b]*Assistant Director and Professor of Security, and* [d]*Professor of Information Systems,*
School of Information Technology, Illinois State University, P.O. Box 5150, Normal, IL 61790-5150, USA

[c]*Professor of Agribusiness, Department of Agriculture, Illinois State University,*
P.O. Box 5020, Normal, IL 61790-5020, USA

Abstract

The goal of this study was to survey farmers and agribusiness owners about their perceptions of cyber security, and how age, gender, and education might affect those perceptions. Using the Health Belief Model as a framework, the survey measured the constructs of perceived susceptibility, severity, benefits, barriers, self-efficacy and cues to action. In addition to the framework, levels of previous cyber-crime victimization and technology implementation were measured. The results of this survey demonstrated that perceived susceptibility to cyber-attacks and the perceived benefits of protective technology are related to an individual's choice to implement cyber security technology. Over half of the respondents had been victims of a computer security incident, demonstrating that even individuals working in agriculture can be impacted by computer crime incidents. This project deepens the understanding of how individuals react to known threats, and what motivates them to adopt protection technologies.

Keywords: cyber security, health belief model, agribusinesses threat perceptions, computer self-efficacy
JEL code: Q16, O33, D83, I12

[ⓘ]Corresponding author: jrwolf@ilstu.edu

1. Introduction

The last place the average American might expect to observe advanced computer technology being used is in the tilled farm fields, but nothing could be further from the truth. According to the 2013 USDA Farm Computer Usage and Ownership report, 67% of farms in the United States have access to the Internet. Farmers and other agricultural operators are applying technology more than they ever have before (USDA, 2013).

While technological advances have created new opportunities, enhanced productivity, and promoted connectivity, they have also introduced new threats. Cyber threats currently pose some of the greatest threats to the United States economy. It is important to recognize that protecting the information technology assets of the agriculture industry is just as important as protecting those of our nation's banks, hospitals, and retail industries.

Numerous incidents of cyber-attacks against individual and organizations occur on a daily basis. The U.S. Secretary of Defense Leon Panetta noted during a speech, 'We are literally the target of thousands of cyber-attacks every day – every day!' (Orr, 2013). Panda Security Labs (2013) revealed that nearly a third of all computers scanned around the world are infected with some kind of malware. Trojans were the most prevalent malware, followed by worms, viruses, and spyware. Some of the highest malware infection rates were found in China (59.36%), Turkey (46.58%), and Peru (42.55%). The United States was found to have a moderate infection rate (30.58%). As many anti-virus scanners have low detection rates, it is possible that actual infection rates are even higher.

As agriculture grows more connected to the global Internet, it has become a target of malicious actors. According to the Verizon (2013) Data Breach Investigation Report, most of the known cyber-attacks against businesses occurred against organizations with less than one hundred employees. Of the 621 documented breaches listed in the report, eleven of them occurred against agricultural organizations (Verizon, 2013). It is imperative for agricultural organizations, businesses, and individuals working in the field to be aware of the potential threats against them.

Farmers, agribusiness owners, and other individuals employed or associated with agriculture provide a unique sampling population. The line between business and personal use of a computer may be blurred. Like other small business industries, the home office may also serve as the office for the farm. The same computer used for personal matters, social networking, and gaming, might also be used to do farm taxes, log onto the local farm's co-op website, or complete USDA eForms.

Using the Health Belief Model (HBM), this study examined the views and perceptions of cyber security by individuals employed in the agriculture industry. Examining the self-efficacy of individuals involved in agriculture suggests the need for cyber security education. Agribusiness owners and farm operators do not need to be certified or educated to the same degree as information technology experts, no more than a nurse or doctor in a hospital needs to be. However, individuals and small business owners operating in a globally connected environment need to be aware of the cyber threats and risks that their operations face.

2. Literature review

As technology continues to evolve at a rapid pace, farmers and agribusinesses face constant adoption choices. It is important to examine the types of technology in use and their implementation in the industry beyond the personal computer.

2.1. Health care models

In many ways, choosing to use computer security technology parallels the choice to obtain a vaccine to guard against a disease. The individual must weigh the value of the protective measure against costs, barriers, and benefits. Specific to the computer security, the individual's self-efficacy also must be weighed in the choice. Fear appeal models, which examine both the threat and self-efficacy, are more appropriate for examining computer security technology adoption. Two different models, the Protection Motivation Theory (PMT) and HBM, are discussed below. Each of these, although utilized mainly in the health care field, can be applied to the information security research.

■ *Protection Motivation Theory*

Rogers (1975) proposed the PMT to explain the processes involved with coping with a threat. The PMT explains adaptive and maladaptive coping with a health threat as a result of threat appraisal. It was later revised in 1985 to allow the theory to encompass persuasive communication, focusing on the cognitive processes that facilitate behavior change (Rogers, 1985).

Rogers stated four components of a fear appeal to which an audience would respond. Perceived susceptibility is the individual's estimation of the probability with which they will contract a disease. Perceived severity is the individual's estimation of the effect that the disease would have on them if they were to contract it. Response efficacy is the degree to which an individual believes a preventive method or treatment will avert the threat. Self-efficacy, which was added by Maddux and Rogers (1983), is the individual's belief in his/her own ability to complete the treatment successfully.

The PMT has been widely used to explain the factors that influence and predict health behaviors, including adherence to prescribed medical treatments (Flynn *et al.*, 1995; Searle *et al.,* 2000), genetic testing (Helmes, 2002), skin cancer and tanning (Jones and Leary, 1994; McClendon and Prentice-Dunn, 2001), alcohol consumption (Murgraff *et al.,* 1999), and smoking (MacDonell *et al.*, 2013).

The PMT has been applied to several research projects on computer security technology, and it has been used in several studies on users' intentions to adopt security software to protect against the threat of spyware (Chenoweth *et al.,* 2009; Johnston and Warkentin, 2010). Vance *et al.* (2012) used the PMT as a framework to study habitual information systems security compliance within a Finnish municipal organization. Within the field of academia, the PMT has been applied to study the adoption of anti-plagiarism software (Lee, 2011).

■ *Health Belief Model*

The HBM was originally created to predict the behaviors of individuals related to their personal health activities. Created by Rosenstock (1966), the HBM argues that the belief in a threat, combined with the belief in the effectiveness of a protective behavior, predicts the likelihood of adopting that behavior. Originally, the HBM was developed in response to the failure of a tuberculosis health screening program. The researchers wanted to understand the factors that influence individuals' choices to reject the screening. Further studies using the HBM model have attempted to explain the rejection of vaccines, elective surgery, and other medical treatments. In summary, the HBM proposes that individuals will accept a medical treatment if they believe they are susceptible to a disease, believe that the treatment will effectively prevent the threat, and that barriers to successfully completing the treatment are minimal.

The perceived susceptibility construct examines the individuals' beliefs that a threat can affect them. In a health care context, this might be the individuals' belief that they will contract a disease or virus. In the context of computer security, perceived susceptibility refers to the likelihood of individuals to believe that their computers can become infected with a computer virus or be 'hacked.' Several factors might affect a respondent's level, such as previous incidents of victimization, knowledge of other individuals' victimization, or previous education on the subject.

In addition to the likelihood of an incident being perceived as important, the degree of influence is also critically important. Perceived severity examines individuals' beliefs that event would have an effect on them. In a security context, this would refer to a perceived effect of a cyber-attack on an individual or his/her business. If the perceived effect of an event is believed to be low, it is likely that an individual would take few, if any steps to prevent it from occurring.

The perceived benefits construct examines the role of the individual's perception of the usefulness or utilitarian value of a new behavior or technology in decreasing the risk of an event. In health care, individuals are more likely to adopt a behavior (e.g. take a vaccine) if they believe that it will lessen the likelihood of them contracting the disease. In the context of security behavior, individuals would be more likely to install anti-virus, patch software, or take cyber-security training if they believe those measures would better protect them from cyber-attacks.

The perceived barriers construct examines the individual's perception of the obstacles or obstructions preventing the adoption of a new behavior. Out of the original four HBM constructs, the perceived barriers may be the greatest factor in determining behavior change (Janz and Becker, 1984). Technology is a rapidly changing field, and individuals and organizations may not have the time, effort, or financial resources to invest in continually evolving security.

The HBM was modified in 1988 to include the self-efficacy construct (Rosenstock *et al.,* 1988). Self-efficacy was defined by Bandura (1977) as the 'personal judgments of one's capabilities to organize and execute courses of action to attain designated goals'. Zimmerman (2000: 83) noted: 'self-efficacy measures focus on performance capabilities rather than on personal qualities, such as one's physical or psychological characteristics. The respondents judge their capabilities to fulfill given task demands, such as solving fraction problems in arithmetic, not who they are personally or how they feel about themselves in general'. In essence, self-efficacy examines the individuals' beliefs that they are able to make a decision regarding certain events or topics.

The cues-to-action construct assumes that previous events, interactions with other people, and other activities influence people's behavior and motivate them to change their behavior. In health care, examples would include illness of family members, media reporting, signs of a disease outbreak, or advice from health care practitioners. Applied to the world of cyber security, examples of cues might include malware infection, media reporting of significant cyber-attacks, knowledge of attacks against one's own industry, security notification pop-ups in a browser (Whalen and Inkpen, 2005), or even friends and colleagues having experienced a recent cyber-security incident.

Socio-demographic variables, including age, income, gender, race, and others, affect the core constructs of the HBM. Other variables, such as knowledge of the threat, prior threat interaction, and education levels, for instance, could influence the individuals' responses to a potential threat.

The HBM has some limitations that could limit its utility in information systems research (or health research, for that matter). A core assumption of the HBM is that all individuals have the same of access to equal information about the disease. In reality, individual education and experiences can have profound effects on an individual's understanding of a disease.

The HBM does not consider environmental or economic factors that prohibit or promote the recommended action. For example, although an individual might feel that he/she is highly susceptible to a disease, that vaccine is highly effective, and that he/she would obtain the vaccine if he/she saw peers contracting the disease, the cost of vaccine might prevent him/her from obtaining the vaccine. Social pressure might also affect the adoption of a behavior; an individual might avoid exercising in the gym because he/she is shy or nervous around other people. In the context of information systems research, although an individual might believe they are highly vulnerable to computer security threats, they may not be able to purchase protective technology due to high cost.

Finally, the HBM does not consider individuals' behaviors that occur for reasons unrelated to protection. For example, an individual might wear a seat belt while operating a car only to comply with the state law rather than out of concern for their health and well-being. Other activities might occur for aesthetic reasons, such as exercising for appearance or social interaction rather than health reasons.

■ *Health Belief Model based information security research*

Two previous studies have utilized the HBM to examine individuals' adoption of security technology. The first was completed by Ng, Kankanhalli, and Xu (2009). In their study, the authors believed that most models used to study technology adoption focused primarily on the tangible benefits. Consequently, the authors opted to use the HBM to examine the adoption of technology to prevent a negative outcome rather than attain a tangible positive benefit. The sample in their study comprised two classes of IT students from a university and employees of three IT-related firms. Their study focused on email safety and organizational security awareness.

The study revealed that perceived susceptibility, perceived benefits, and self-efficacy significantly affected email security related behavior. From a theoretical standpoint, this study demonstrated the success in using a health based model to explain computer security behavior. Practically, the study demonstrated that if a person's perceived susceptibility is higher, he/she is more likely to engage in good computer security behavior. Ng *et al.* (2009: 823) noted, 'the importance of perceived severity (as a moderator), perceived susceptibility and perceived benefits instructs us on how to design the content for organizational security awareness messages'. The authors also noted that future research should focus on individuals who utilize IT resources but do not use them as the core of their business.

Claar (2011) completed the second information security study utilizing the HBM. As part of his doctoral dissertation, Claar explored the security habits of home computer users using the HBM as a model, noting 'striking similarities in the beliefs and perceptions in protecting one's health and in protecting one's computer from infection and attack.'

Claar's (2011) population of interest included all home computer users who were responsible for their home computer security. Snowball sampling was used to recruit the participants for this study. The first group of respondents was a group of undergraduate students at a university. In addition, several Google news groups were chosen randomly to advertise the survey and recruit respondents. Because snowball sampling was implemented, it was unknown how many potential respondents who received the invitation to take the survey declined to take it. Ultimately, the project recruited 186 responses for the analysis.

The results of Claar's study revealed that the perceptions of vulnerability to an attack and prior experience with security incidents were the most significant contributors to the use of computer security (Claar, 2011). Perceived barriers to the implementation of computer security technology and self-efficacy were also found to influence computer security usage. In essence, a high perceived vulnerability to cyber-attack, the belief that security technology was not obstructive, and the individuals' self-confidence to implement computer security technology were significant factors in this study.

Both Ng and Claar's studies used respondents who likely had received some level of IT-related security awareness training before participating in the research. For future research, Claar sought to have his research applied to non-technology savvy individuals (2011). Thus, this model framework for cyber security will be implemented for the first time in an industry that does not focus on IT, let alone IT security.

While both the PMT and the HBM offer frameworks for studying security technology adoption, the HBM appears to be more appropriate. The PMT focuses more on the behavioral response based on fear appeals, whereas the HBM is concerned with behavioral abilities. This study concentrated on the current perceptions and deployment of security technology, rather than fear appeals that might motivate the respondents to implement the protective technology. Using the HBM will better allow us to determine the behavioral activities, which affect the perceptions or use of protective computer technology.

2.2. Hypotheses

The purpose of the project was to examine the implementation of cyber security and perceptions of threats, vulnerabilities, and self-efficacy among farmers, agribusinesses owners, agricultural industry employees, and other individuals involved in agriculture. The results provided descriptive information about the use of technology, previous computer crime victimization, credit and debit card use, and interest in cyber security education.

The survey instrument was developed based on the tool created by Claar (2011). Copyright permission to use a modified version of the instrument for the use in this project was obtained from the original author (C. Claar, personal communication, November 14, 2013). Although the original instrument questions targeted the generic individual, some items were modified to make them relevant to the individual farmer or agribusiness owner.

Perceived susceptibility refers to the individuals' beliefs that they are vulnerable to a computer security incident. When individuals believe that their computer is likely to be a victim of a computer security incident, they are more likely to implement a security technology to prevent it. As such, the following hypothesis was established:

H_1: perceived susceptibility to computer security incidents is positively related to computer security usage.

The perceived severity construct is the individual's belief that if a computer security incident were to occur, the event would have a negative effect on his/her lifestyle and financial health, would disrupt business activity, and the like. If a user believes that the loss of computing functionality due computer security incident is high, he/she would be more likely to implement technology to protect his/her computer. As such, the following hypothesis was established:

H_2: perceived severity of computer security incidents is positively related to computer security usage.

In the HBM, perceived benefits referred to an individual's perceptions of the effectiveness of an action (like a receiving a vaccine) to reduce the probability of contracting a disease. Similar to computer security technology, anti-virus, anti-spyware, and other network protection technologies can reduce the risk of a computer becoming infected with malware. When an individual believes those technologies are beneficial to his/her computer's health, he/she would be more likely to implement them. The following hypothesis follows:

H_3: perceived benefits of security technology are positively related to computer security usage.

Although an individual might feel an action is beneficial at reducing a threat, certain mitigating activities might be unpleasant, too costly, or inconvenient to implement. Computer security software often inconveniences the users, causes difficulty in completing tasks, and obstructs productivity while trying to secure a system. If an individual feels that a protective technology is too obstructive for productivity, they are less likely to implement it. The following hypothesis follows:

H_4: perceived barriers to implementing computer security technology are negatively related to computer security usage.

Self-efficacy refers to the individual's belief in his/her ability to perform an action. Individuals with greater confidence in their ability to perform an action are more likely to initiate and engage in that action. Information security self-efficacy refers to the individual's ability to select, install, configure, and operate security technology, such as anti-virus, anti-spyware, and network firewalls on his/her computer. As such, the following hypothesis follows:

H_5: information security self-efficacy is positively related to computer security usage.

A cue to action refers to the knowledge of another individual, or information obtained from a reliable source, about the spread of computer viruses, computer vulnerabilities, or suspicious activity by the user's computer. For example, an individual might be more likely to install anti-virus software if he/she sees news reports about a computer virus spreading across the internet, just like individuals might also be more likely to engage in a preventive activity if their peers, neighbors, or other affiliates are affected by a disease. As such, the following hypothesis follows:

H_6: cues to action are positively related to computer security usage.

With the ability to compare demographics of the respondents, three further hypotheses related to the age, gender, and education of the respondents will be tested against each of the primary hypotheses. Previous information systems research has demonstrated that age, gender, and other demographic moderators can have an effect on technology adoption (Liang and Xue, 2009). Thus, the moderating effects of age, gender, and education will be examined as follows:

H_{7a}: age significantly moderates the relationship between Perceived Susceptibility and computer security usage.
H_{7b}: age significantly moderates the relationship between Perceived Severity and computer security usage.
H_{7c}: age significantly moderates the relationship between Perceived Benefits and computer security usage.
H_{7d}: age significantly moderates the relationship between Perceived Barriers and computer security usage.
H_{7e}: age significantly moderates the relationship between Information Security Self-efficacy and computer security usage.

H_{8a}: gender significantly moderates the relationship between Perceived Susceptibility and computer security usage.
H_{8b}: gender significantly moderates the relationship between Perceived Severity and computer security usage.
H_{8c}: gender significantly moderates the relationship between Perceived Benefits and computer security usage.
H_{8d}: gender significantly moderates the relationship between Perceived Barriers and computer security usage.
H_{8e}: gender significantly moderates the relationship between Information Security Self-efficacy and computer security usage.

H_{9a}: education significantly moderates the relationship between Perceived Susceptibility and computer security usage.
H_{9b}: education significantly moderates the relationship between Perceived Severity and computer security usage.
H_{9c}: education significantly moderates the relationship between Perceived Benefits and computer security usage.
H_{9d}: education significantly moderates the relationship between Perceived Barriers and computer security usage.
H_{9e}: education significantly moderates the relationship between Information Security Self-efficacy and computer security usage. The hypotheses are shown in Figure 1.

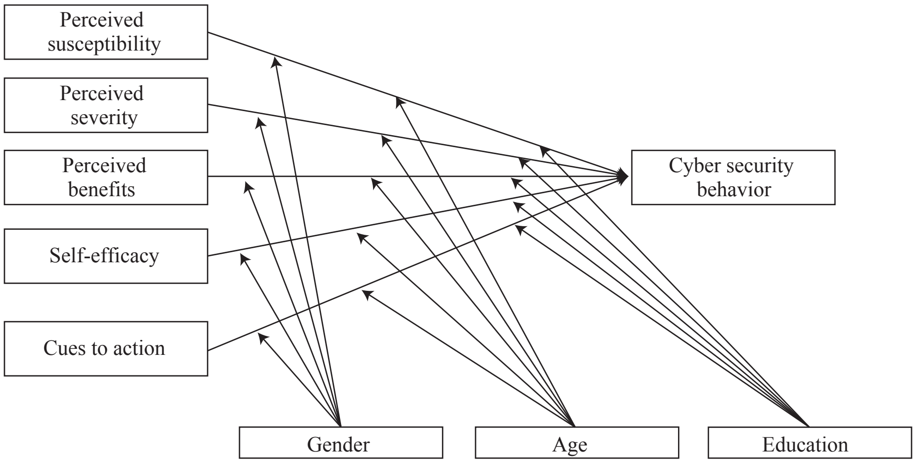

Figure 1. Health Belief Model based survey model.

3. Material and methods

The study population comprised farmers, producers, agribusiness owners, or other individuals who have participated in a USDA Farm Service Agency (FSA) program in three selected Illinois counties. Any farm operator, owner, or agribusiness owner in those counties who had participated in an FSA program and registered in the FSA database had a chance of being selected for this survey. Utilizing the Freedom of Information Act, a list of all participants in the three selected counties was obtained. The three counties were selected for their number one rankings for each of the top three agricultural commodities in Illinois: cash crops, cattle, and hogs. The statistics and rankings were obtained from the National Agricultural Statistical Service (USDA, 2007).

3.1. Data

The sample from each county was drawn by random sampling. Because the population roster provided by the FSA contained many individuals in the agriculture industry in a specific county, a true representative sample could not be drawn.

Overall, 1,800 respondents, 600 from each county, were randomly selected. The sample was then split into two groups, ‘A’ and ‘B’, with 300 participants from each county in each group. The first group received the paper copy of the survey to complete, with the option to complete the survey online. The second group received an invitation letter to complete the survey online.

McLean County is ranked first in the state for the value of sales in grains, oilseeds, dry beans, and peas. Although McLean ranks number two in the state in total acreage for these crops, it ranks number one in the total cash sales from them (U.S. Department of Agriculture). Of the 1,513 respondents in the 2007 Agricultural Census, 812 of them identified their primary occupation as ‘farming’ while the remaining 701 selected ‘other.’ The average net cash income of an agriculture operation was $117,050. Twin cities of Bloomington-Normal and Illinois State University are also located in McLean County. This geographically largest county in the state has a population in excess of 153,000, most residing within the boundaries of the Bloomington-Normal metropolitan areas.

Jo Daviess County is located in northwestern Illinois and boasts the highest inventory of cattle in the state. It borders the states of Iowa and Wisconsin, both of which are considered major agricultural producers themselves. The county had 1,016 farms, as of 2007, averaging 267 acres[1]. Overall, 443 out of 1,016 Census respondents identified their primary income as 'farming.' The average net cash income of an agriculture operation in Jo Daviess County was $44,710.

De Kalb County in north central Illinois ranks number one in hog inventory. The total head count of hogs and pigs, according to the Census, was 225,397. As of 2007, the county had 930 farms, averaging 440 acres (U.S. Department of Agriculture). The average net cash income for an agriculture operation in De Kalb County was $84,017.

These three counties represent three of the top agriculture industries in Illinois. Jo Daviess has the highest head count of ducks within the state while McLean County ranks seventh in the state in sheep and lamb count. Additionally, many silos, co-ops, grain storage sites, and other agribusinesses can be found throughout each of these counties.

3.2. Survey instrument

The paper survey was mailed via the U.S. Postal system directly to each farm operator or owner, using his/her address registered with the FSA. The consent from the respondents was obtained utilizing an informational cover letter. The cover letter explained the purpose of the survey and provided contact information for the project. Implied consent was obtained from the respondents completing and returning the survey. This survey was not anonymous but confidentially was guaranteed to respondents in the cover letter. The survey included a pre-paid return postage envelope to encourage the return of the surveys to the researcher.

The respondents receiving the invitation to participate online were provided a similar cover letter, with instructions on how to access the website. The online survey matched the paper survey, allowing equal comparison between answers provided. The online site allowed respondents to complete the same survey using radio buttons and drop boxes. A link on the index page of the site provided a connection to the survey website hosted at SurveyShare.com.

The online survey required respondents to provide their survey identification number before being permitted to proceed. The survey identification number was included in the invitation. A review of all submissions to the online site revealed no attempts by intruders or cyber vandals to modify the survey results. A review of IP access logs to the website revealed no traffic above the response rates of the survey.

The first section of the survey instrument requested basic demographic information from the respondent. Demographic variables include age, gender, length of time in agriculture, role of the respondents, income levels, and the types of agriculture in which they were involved.

The respondents were provided a series of security scenarios representing the current threats that internet users face (Table 1). The original scenarios in Claar's instrument were derived from research by Boss (2007), who formulated them using the 2001 U.S. Department of Justice National Crime Victimization Survey. Each item 'assesses the degree to which individuals feel that is likely they will experience the scenario, and assesses the impact to them were it to happen' (Boss, 2007: 75).

Based on the scenarios provided, the respondents were asked to respond to each of the first three constructs (perceived susceptibility, perceived severity, and perceived benefits) relative to each scenario. Perceived susceptibility was measured on a five point Likert scale ranging from 'very likely' to 'very unlikely'. Perceived severity was measured on a five point Likert scale ranging from 'no effect' to 'major effect'. Perceived benefits were measured on a five point Likert scale ranging from 'poor' to 'excellent'.

[1] 1 acre = 0.40 ha.

Table 1. Security scenarios.

Scenario
My computer system becoming corrupted by a virus.
My computer being taken over by a hacker.
My files becoming corrupted by a computer virus.
My personal identity being stolen (credit cards, social security number, etc.).
My agribusiness or farm identity being stolen (loan fraud, etc.).
Not being able to access the Internet due to a computer virus.
My computer becoming infected with a virus by visiting a website.

‘Perceived Barriers’ refer to the cost and difficulty in implementing computer security technology. The construct consisted of four questions measured on a Likert scale ranging from ‘highly agree’ to ‘highly disagree’ (BAR1, ‘the expense of computer security technology (anti-virus, firewalls, etc.) is a concern for me.’; BAR2, ‘the use of computer security software (anti-virus, firewalls, etc.) would make day-to-day tasks more difficult’; BAR3, ‘implementing and using computer security technology is time consuming’; BAR4, ‘implementing security technology on the computers I use would require an investment of effort other than time.’).

Information ‘Self-Efficacy’ refers to the individual’s belief that he/she can successfully implement security technology to protect his/her computer. The construct comprises four questions measured on a Likert scale ranging from ‘highly agree’ to ‘highly disagree’ (SEF1, ‘I can determine the appropriate computer security technology for my computer’; SEF2, ‘I can correctly install and manage computer security technology for my computer’; SEF3, ‘I know how to find information on how to respond to a computer security problem’; SEF4, ‘if my computer were to become infected by a virus, I would know how to fix it’).

The ‘Cues to Action’ construct refers to the previous experiences, triggers, or events that prompt a user to implement computer security technology. The construct comprises four questions measured on a Likert scale ranging from ‘highly agree’ to ‘highly disagree’ (CUE1, ‘if another agribusiness or farmer were to tell me of a recent experience with a computer virus, I would be more conscious of my computer’s chance of being attacked’; CUE2, ‘if my computer were to start behaving strangely, I would be concerned if I had been the victim of a computer virus’; CUE3, ‘if I saw a news report or read a newspaper or magazine about new computer security vulnerability, I would be more concerned about my computer’s chances of being attacked’; CUE4, ‘if I received an email from the maker of my computer’s operating system about new security vulnerability, I would be more concerned about my computer’s chances of being attacked’).

‘Computer Security Usage’ was the dependent variable in this research. Each respondent was asked about his/her use of after-market anti-virus, anti-spyware, and network firewall protection. If an individual has purchased after-market software, he/she might be concerned about computer security to the point they have made an investment in it. The measure of computer security usage consists of three questions measured on a binary scale, with ‘yes’ response being worth 1 point, ‘no’ and ‘don’t know’ being worth 0 points. If a user has implemented all three technologies, he/she received a ‘high’ rating; two technologies were listed ‘medium’; one technology was ‘low’; and no technology received a score of ‘none.’ This created a scale against which independent variables could be compared. Two questions were designed to elicit information about previous computer security incidents that had affected the respondent. The respondents could respond yes, no, or that they didn’t know. Those who did respond yes were asked to provide information on how long ago the incident had occurred.

3.3 Data analysis

136 mail surveys were returned, and thirty-two were completed electronically, for a total of 168 responses. After removing unusable responses from the total due to missing data, blank returns, and other incomplete surveys, 138 surveys were deemed valid. This resulted in a valid response rate of 8.1% (Table 2). The largest number of returns was from DeKalb County (N=54), followed by McLean County (N=45) and Jo Daviess County (n=39).

The first mailing of surveys and invitation letters was sent on January 9th, 2014. After four weeks, a total of one hundred and two mailed surveys were returned. The website received 30 responses.

Table 2. Demographic data.

Variable	Frequency (n)	Percentage
Gender		
Male	118	85.5
Female	20	14.5
Age		
18-20	2	1.4
21-30	5	3.6
31-40	18	13.0
41-50	39	28.3
51-60	41	29.7
61-70	19	15.9
71-80	11	8.0
Education		
Completed high school	26	18.8
Some college	28	20.3
Completed two-year degree	10	7.2
Completed four-year degree	42	30.4
Some graduate work	11	8.0
Graduate degree	15	10.9
Doctoral degree	3	2.2
Professional degree	3	2.2
Role in agriculture		
Farm operator	98	71.0
Farm employee	1	0.7
Landlord (non-farming)	30	21.7
Agribusiness – owner	7	5.1
Agribusiness – employee	2	1.4
Gross income		
Less than $50,000	43	31.2
$50,001 to $100,000	22	15.9
$100,001 to $250,000	21	15.2
$250,001 to $500,000	19	13.8
$500,001 to $750,000	11	8.0
More than $750,000	22	15.9

■ *Sample characteristics*

Half of the respondents reported that they had been previously affected by a computer security incident (Table 3). Of those who had been affected, almost half of the incidents had occurred within the past year (46.4%), or the respondent could not remember when the incident occurred (39.1%). There was a significant effect by previous computer incident victimization on computer security usage (F=4.437, *P*=0.014).

■ *Construct reliability analysis*

Cronbach's alpha is a measure of internal consistency to how closely related a set of items are as a group. A high value is considered above 0.9, while in most social science research, above 0.7 is considered acceptable. A reliability analysis for all of the model constructs was completed, revealing the Cronbach's alpha level was above 0.7 (Table 4). The scale of reliability did not improve with the removal of any of the construct variables.

■ *Independent variables*

The items for each of the constructs were combined into a single factor score by means of aggregation. The range of the data covered the entire range of possibilities, with the exception of Cues to Action. The highest aggregated response for Cues to Action was 4.5. The skewedness for these constructs ranged from -0.705 to 0.049, indicating an acceptable distribution of values. The kurtosis of the values ranged from -0.668 to 2.840. The Cues to Action variable was the only construct outside of the acceptable range of ±2. Because the exceptionally high value is positive, this demonstrates that the distribution of values were located in the tail of distribution, rather than around the mean.

Table 3. Previous computer security incidents.

	Frequency	Percentage
Previously affected by a computer security incident		
Yes	69	50.4
No	58	42.3
Don't know	11	7.2
If yes, how long ago?[1]		
Year	32	46.4
Month	7	10.1
Week	3	4.3
Don't remember	27	39.1

[1] n=69.

Table 4. Cronbach's alpha scores.

Construct	Cronbach's alpha	n of items
Perceived susceptibility	0.940	7
Perceived severity	0.933	7
Perceived benefits	0.951	7
Perceived barriers	0.794	4
Information self-efficacy	0.869	4
Cues to action	0.786	4

■ *Dependent variables*

Computer security usage was the dependent variable for this study. Respondents were asked to provide information on their use of anti-virus, anti-spyware, and firewall technology for their computers. A majority of the respondents used anti-virus, while rates of anti-spyware and firewall usage were much less (Table 5).

The dependent variable was determined by assigning each respondent a score reflective of their overall implementation of security technology. The range of scores was from none to high, with a standard deviation of 0.880, a skewedness of 0.117, and a kurtosis of -0.659. Only 12.3% of the respondents indicated they do not use computer security technology.

4. Results

To test the hypotheses established for this study, ordinal logit (PLUM) regression was conducted using SPSS (SPSS version 22.0, IBM Corporation, Armonk, NY, USA) (Table 6). This allowed the ordinal dependent variable, computer security usage, to be regressed on the independent variables of perceived susceptibility, severity, benefits, barriers, self-efficacy, and cues to action (Model 1). A second step was taken to regress the main modifying variables (age, gender, education), and the two way interactions between those moderating variables of susceptibility, severity, benefits, barriers, self-efficacy, and cues to action against the dependent variable (Model 2).

For Model 1, the research model has a Chi-Square factor of 13.555 and a significance of 0.038. The significance level below 0.05 demonstrates the model is significant with the predictors. When the moderating variables are introduced in Model 2, the model fitting information changed to a Chi-Square of 40.338 and a significance level of 0.048, thus indicating the model was still significant.

In Model 1 regression, the main effects of susceptibility, severity, benefits, barriers, self-efficacy, and cues to action, were tested (H_1-H_6). H_1, which predicted that perceived susceptibility to computer security incidents would be positively related to computer security usage was supported (μ=0.367, *P*=0.033). H_2, which predicted perceived severity of computer security incidents would be positively related to computer security usage, was not supported (μ=-0.050, *P*=0.770, n.s.). H_3, which predicted the perceived benefits of computer security technology was positively related to computer security usage, was supported (μ=0.577, *P*=0.008). H_4, which predicted the perceived barriers of implementing computer security technology would be negatively related to computer security usage was not supported (μ=-0.305, *P*=0.176, n.s.). H_5, which

Table 5. Dependent variable responses.

Variable	Yes	No/don't know
Anti-virus	112	26
Anti-spyware	55	83
Firewall	20	118

Table 6. Regression information.[1]

	-2 log likelihood	Chi-square	df	Sig.
Model 1	333.736	13.355	6	0.038*
Model 2	306.753	40.338	27	0.048*

[1] Model 1 = regression of ordinal dependent variable on the independent variables of perceived susceptibility, severity, benefits, barriers, self-efficacy, and cues to action; Model 2 = regression of the main modifying variables and the two way interactions between moderating variables against the dependent variable; df = degrees of freedom; * = values differ significantly at the 0.05 level.

predicted information security self-efficacy would be positively related to computer security usage, was not supported (μ=0.241, *P*=0.169, n.s.). H_6, which predicted cues to action would be positively related to computer security usage, was not supported (μ=0.075, *P*=0.786, n.s.).

In Model 2, the main effects of susceptibility, severity, benefits, barriers, self-efficacy, and cues to action, were tested, along with the modifying factors age and education, along with the interactions between those factors and the main factors. Due to the low number of female respondents, an accurate test of the modifying effect could not be completed.

Hypotheses $H_{7a\text{-}f}$, which predicted that age would have a significant moderating effect with susceptibility, severity, benefits, barriers, self-efficacy, and cues to action, only H_{7a} was supported (H_{7a}: μ=0.034, *P*=0.040; H_{7b}: μ=0.017, *P*=0.365, n.s.; H_{7c}: μ=-0.009, *P*=0.661, n.s.; H_{7d}: μ=0.003, *P*=0.908, n.s.; H_{7e}: μ=-0.017, *P*=0.291, n.s.; H_{7f}: μ=0.024, *P*=0.359, n.s.). The main effect of age on computer security usage was also not significant (μ=-0.199, *P*=0.181).

Hypotheses $H_{9a\text{-}f}$, which predicted that education would have a significant moderating effect with susceptibility, severity, benefits, barriers, self-efficacy, and cues to action were not supported (H_{9a}: μ=-0.214, *P*=0.065, n.s.; H_{9b}: μ=-0.030, *P*=0.773, n.s.; H_{9c}: μ=-0.113, *P*=0.399, n.s.; H_{9d}: μ=0.200, *P*=0.147, n.s.; H_{9e}: μ=-0.105, *P*=0.324, n.s.; H_{9f}: μ=-0.245, *P*=0.191, n.s.). The main effect of education on computer security usage was also not significant (μ=1.852, *P*=0.053, n.s.).

Although not part of the original proposed model, two other major factors were also tested for their overall effect as modifying variables on the dependent variable. The effect of gross income was found to be not-significant (μ=0.103, *P*=0.213). Total farm size (acres) was also determined to be not-significant (μ=0.041, *P*=0.232).

Several other significance tests were run to determine if there were correlations or differences amongst groups within the respondent pool. There was a significant correlation between the level of computer security usage and age, but the association was weak (X^2=0.288, *P*=0.048) (Table 7). Levels of computer security usage did not differ for respondents with farms above the mean farm size (938), compared to those below it (F=0.688, *P*=0.408). The role of the respondent did not have a significant effect on computer security usage. (F=1.402, *P*=0.238).

5. Discussion

Using the HBM, the project was able to evaluate the cyber security perceptions of individuals involved in agriculture. From descriptive measures, the means of perceived severity indicate that there is a moderate to high level of concern that a computer security incident would impact the individual. The benefits of computer security technology were viewed as moderately high, indicating that anti-virus and other technologies are viewed as having some value in protecting computers. Perceived barriers and perceived susceptibility were rated at moderate levels, demonstrating the implementation of computer security technology was not viewed as overly obstructive, but nor did the respondents consider themselves as overly susceptible to a cyber-attack. Finally, self-efficacy averaged below the median score, indicative that respondents might not feel comfortable with selecting, configuring, and managing computer security technology.

The model revealed perceived susceptibility and perceived benefits are significant factors for members of the agricultural community when it comes to implementing computer security technology. Only perceived susceptibility was a modifying factor on age. Surprisingly, education as a modifying variable had no effect on the choice to implement protective measures.

Neither the size of the farm, nor the role of the respondent, appears to have an effect on the adoption of computer security technology. Significant differences in computer security usage were observed between

Table 7. Regression parameters.[1]

	Est. (μ)	**Std. error**	**Wald**	**df**	**Sig.**	**Interval**	
						Lower bound	**Upper bound**
Model 1							
Susceptibility	0.367	0.172	4.544	1	0.033*	-0.705	-0.030
Severity	-0.050	0.172	0.085	1	0.770	-0.388	0.288
Benefits	0.577	0.216	7.147	1	0.008*	0.154	1.000
Barriers	-0.305	0.225	1.831	1	0.176	-0.746	0.137
Self-efficacy	0.241	0.175	1.896	1	0.169	-0.102	0.584
Cue to action	0.075	0.277	0.073	1	0.786	-0.467	0.617
Model 2							
Susceptibility	-0.083	1.278	0.004	1	0.948	2.423	2.423
Severity	-0.794	1.408	0.318	1	0.573	1.966	1.966
Benefits	2.168	1.515	2.047	1	0.152	5.138	5.138
Barriers	-2.196	1.670	1.729	1	0.189	1.077	1.077
Self-efficacy	2.022	1.263	2.560	1	0.110	4.498	4.498
Cue to Action	0.372	1.965	0.036	1	0.850	4.223	4.223
Age	-0.199	0.149	1.788	1	0.181	0.093	0.093
Education	1.852	0.958	3.739	1	0.053	3.729	3.729
Total farm size (acres)	0.041	0.000	2.947	1	0.232	-3.207	1.214
Gross income	0.103	-0.128	1.552	1	0.213	-0.330	0.074
Susceptibility * Age	0.034	0.017	4.212	1	0.040*	0.066	0.066
Severity * Age	0.017	0.018	0.822	1	0.365	0.052	0.052
Benefits * Age	-0.009	0.020	0.192	1	0.661	0.030	0.030
Barriers * Age	0.003	0.023	0.013	1	0.908	0.047	0.047
Self-efficacy * Age	-0.017	0.016	1.115	1	0.291	0.015	0.015
Cue to Action * Age	0.024	0.026	0.841	1	0.359	0.075	0.075
Susceptibility * Education	-0.214	0.116	3.402	1	0.065	0.013	0.013
Severity * Education	-0.030	0.105	0.083	1	0.773	0.175	0.175
Benefits * Education	-0.113	0.134	0.712	1	0.399	0.149	0.149
Barriers * Education	0.200	0.138	2.102	1	0.147	0.470	0.470
Self-efficacy * Education	-0.105	0.106	0.972	1	0.324	0.104	0.104
Cue to action * Education	-0.245	0.187	1.709	1	0.191	0.122	0.122

[1] * = *P*<0.05; 1 acre = 0.40 ha.

those previously affected by a computer security incident compared those who had not. Individuals who had been previously impacted by an incident were more likely to have higher levels of computer security. This possibly indicates that many security installations are done for reactive purposes after an incident, rather than before it occurs.

This study was among the first to use the HBM to study computer security implementations. Ng (2009) reported similar results amongst perceived susceptibility and perceived benefits. Claar (2011) found that perceived susceptibility and previous experience with a computer security incident affected the use of computer security technology. These studies shared a common theme that the perception of the threat and the benefits of protective technology are the most significant factors contributing to computer security implementation. Similar to both of the previous studies, this study found that cues to action variable was not a significant factor in computer usage.

In the context of computer security, this study has deepened the understanding of human behavior in the face of threats. The dynamics of the agricultural population allows researchers to examine the implementation of computer security in an area where personal and business activities may be closely intertwined. Other similar studies have focused either on the individual computer user in the home environment or on employees in an organizational setting but not on both concurrently.

5.1. Limitations and future work

As with any study, this research had some limitations. The high non-response rate of the survey population may be due to many unknown factors. It will never be known how many of the respondents chose not to respond precisely because they do not have computer technology implemented. Other respondents may not have wished to disclose sensitive information about their security implementation.

The online nature of the study likely limited the number of respondents. Some respondents might not have been able to complete the study due to a lack of internet access, while others may not have felt comfortable completing a survey about computer security online. Other researchers have noted that e-mail solicitation of respondents is a very poor method of recruiting participants in security studies (Claar, 2011). Perhaps the best way to engage participants continues to be through physically mailed surveys or direct interaction.

Another limitation of this study is the self-reported nature of the dependent variable. The self-report bias might have motivated the respondents to report a higher level of usage than would be determined through direct observation, which would have affected the results. This project also made the assumption that the respondent understood the differences between anti-virus, anti-spyware, and firewall technologies.

Finally, the list of participants was obtained from a Federal agency. The frequency with which the FSA program updates, audits, or purges its participant list is unknown. The high rate of returned surveys due to incorrect mailing addresses indicates that the list is poorly maintained, or at the very least, not updated.

Using the HBM for information security research is a relatively new method of researching technology related behavior. While other studies have focused on traditionally IT-savvy populations, future research could be applied to industries not typically considered IT-centric. Even with agriculture, certain segments of the industry, i.e. aviation, marketing, and others, regularly use technology; thus, they could be studied more extensively. Beyond the scope of security technology, further research on the factors that affect technology adoption in agriculture should continue to be conducted to deepen the understanding of consumer behavior.

The dependent variable in this study was the use of anti-virus, anti-spyware, and firewall technology implementation. Future research could further expand upon security behavior, such as browsing suspicious websites, opening unsolicited email attachments, file sharing, and online piracy activity, to determine risky behavior. Investigating the level of engagement of these activities by respondents might further explain the constructs like perceived susceptibility and self-efficacy.

5.2. Practical implications

The low rates of self-efficacy amongst the respondents indicate there are gaps in security knowledge in the agricultural community. Half of the respondents reported they had been affected by a computer security incident. Over half the respondents in this study indicated the desire to participate in some form of cyber security training. One respondent noted the need for a computer security standardized practices, which could be made to parallel other industries.

The practical conclusion to be drawn is that there exists a need for computer security education within the industry. An opportunity exists for leading organizations in the industry, such as Farm Bureaus, Associations, or the FSA to offer an awareness level education programs, or liaison with organizations which do. Security awareness programs should train users on the purpose, function and basic methodology of computer security.

5.3 Conclusions

American agriculture faces risks on a regular basis. While traditional threats of weather and market instability continue to exist, the cyber-attack threats are now imminent. The very technology that helps connects farmers and others in agriculture to the world risks opening the door to new threats. The threat of disruption to personal or business functions as the result of a cyber-attack is high. Information security for a farm or agribusiness should not be neglected, and technology alone cannot provide sufficient protection.

Agriculture is one of the core pillars of the American economy. Protecting those involved in agriculture from cyber-attack is critical to ensuring the continuity of business activities, personal livelihood, and the American way of life. Technology can greatly enhance productivity, but only if that technology is safe, secure, and protected. As a nation, we have a vested interest in protecting our nation's farmers from risk in the fields or online.

References

Bandura, A. 1977. Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review* 84 (2): 191-215.

Boss, S. 2007. Control, perceived risk and information security precautions: external and internal motivations for security behavior. PhD dissertation, University of Pittsburgh, Pittsburgh, PA, USA.

Chenoweth, T., R. Minch and T. Gattiker. 2009. Application of protection motivation theory to adoption of protective technologies. In: *Proceedings of the 42nd Hawaii international conference on system sciences*. IEEE Computer Society, Washington, DC, USA.

Claar, C.L. 2011. The adoption of computer security: an analysis of home personal computer user behavior using the health belief model. PhD dissertation, Utah State University, Logan, UT, USA.

Flynn, M.F., R.D. Lyman and S. Prentice-Dunn. 1995. Protection motivation theory and adherence to medical treatment regimens for muscular dystrophy. *Journal of Social and Clinical Psychology* 14(1): 61-75.

Helmes, A.W. 2002. Application of the protection motivation theory to genetic testing for breast cancer risk. *Preventive Medicine* 35(5): 453-462.

Janz, N.K. and M.H. Becker. 1984. The health belief model: a decade later. *Health Education Quarterly* 11(1): 1-47.

Johnston, A.C. and M. Warkentin. 2010. Fear appeals and information security behaviors: an empirical study. *MIS Quarterly* 34(3): 549-66.

Jones, J.L. and M.R. Leary. 1994. Effects of appearance-based admonitions against sun exposure on tanning intentions in young adults. *Health Psychology* 13(1): 86-90.

Lee, Y. 2011. Understanding anti-plagiarism software adoption: an extended protection motivation theory perspective. *Decision Support Systems* 50(2): 361-69.

Liang, H., and Y. Xue. 2009. Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly* 33(1): 71-90.

MacDonell, K., X. Chen, Y. Yan, F. Li, J. Gong, H. Sun, L. Xioaming and B. Stanton. 2013. A protection motivation theory-based scale for tobacco research among Chinese youth. *Journal of Addiction Research and Therapy* 4: 154-170.

Maddux, J. E. and R.W. Rogers. 1983. Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change. *Journal of experimental social psychology* 19(5): 469-479.

McClendon, B.T. and S. Prentice-Dunn. 2001. Reducing skin cancer risk: an intervention based on protection motivation theory. *Journal of Health Psychology* 6(3): 321-328.

Murgraff, V., D. White and K. Phillips. 1999. An application of protection motivation theory to riskier single-occasion drinking. *Psychology and Health* 14(2): 339-350.

Ng, B.Y., A. Kankanhalli and Y.C. Xu. 2009. Studying users' computer security behavior: a health belief perspective. *Decision Support Systems* 46(4): 815-825.

Orr, B. 2013. Pentagon expands cyber defense amid daily attacks. *CBS News*. Available at: http://tinyurl.com/yb4vvnnk.

Panda Security Labs. 2013. Annual Report PandaLabs. Available at: http://tinyurl.com/ycd5vh6j.

Rogers, R.W. 1975. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology* 91: 93-114.

Rogers, R.W. 1985. Attitude change and information integration in fear appeals. *Psychological Reports* 56(1): 179-182.

Rosenstock, I.M. 1966. Why people use health services. *The Milbank Memorial Fund Quarterly* 44(3): 94-124.

Rosenstock, I.M., V.J. Strecher and M.H. Becker. 1988. Social learning theory and the health belief model. *Health Education and Behavior* 15(2): 175-183.

Searle, A., K. Vedhara, P. Norman, A. Frost and R. Harrad. 2000. Compliance with eye patching in children and its psychosocial effects: a qualitative application of protection motivation theory. *Psychology, Health and Medicine* 5(1): 43-54.

United States Department of Agriculture. 2007. Census publications. Available at: http://tinyurl.com/y8t3pam6.

United States Department of Agriculture National Agricultural Statistics Service. 2013. Farm computer usage and ownership. Available at: http://tinyurl.com/y9pmfee4.

United States Department of Justice. 2002. Bureau of justice statistic national crime victimization survey. Available at: http://tinyurl.com/ydy8c52u.

Vance, A., M. Siponen and S. Pahnila. 2012. Motivating IS security compliance: insights from habit and protection motivation theory. *Information and Management* 49(3-4): 190-198.

Verizon. 2013. 2013 Data breach investigations report. Available at: http://tinyurl.com/crnzu89.

Whalen, T. and K.M. Inkpen. 2005. Gathering evidence: use of visual security cues in web browsers. Available at: http://tinyurl.com/y6uprdbv.

Zimmerman, B.J. 2000. Self-efficacy: an essential motive to learn. *Contemporary Educational Psychology* 25(1): 82-91.