Advances in Business Research
2012, Vol. 3, No. 1, 107-112

Computer Security Threats: Small Business Professionals' Confidence in Their Knowledge of Common Computer Threats

Thomas Hayes, University of Arkansas - Fort Smith
Margaret Tanner, University of Arkansas - Fort Smith
George Schmidt, University of Arkansas - Fort Smith

This paper investigates the possible existence of overconfidence by small business professionals in their knowledge of different types of computer security threats. Specifically, this article focuses on the ability of small business owners and managers to understand and identify four main types: viruses, Trojans, spyware, and phishing attacks. Contrary to our expectations, subjects did not exhibit overconfidence in their knowledge of computer security threats. Implications for education and practice are discussed.

Computer usage in everyday life and in business is on the rise. E-mail, the Internet, and numerous other computer programs allow small businesses to focus on the conduct of their business, rather than on recordkeeping and communication processes. With the increased usage of computer technology, however, comes the increased exposure to data security threats. Indeed, cybercrime is on the rise, and company losses are mounting. In their 2012 Data Breach Investigations Report (DBIR), Verizon reports 855 incidents of cyber-attacks, involving 174 million compromised records. Further, the report states that 98% of these attacks came from an outside agent (i.e., as opposed to an employee), and 69% incorporated some form of malware (e.g., viruses).

Further exacerbating the problem is the proliferation of new strains of malware every year. Panda Labs, a computer security vendor, reported that more than 25 million new strains of malware were created in 2009 (Skinner, 2010). With such malware, cybercriminals can steal vital company information. For example, hackers can plant malicious software on business computers to capture online banking credentials such as logins and passwords (Gorman & Perez, 2009).

Small businesses are particularly susceptible to cybercrime attacks because they frequently lack sophisticated security capabilities and the financial resources to safeguard their computer systems. Cybercriminals are getting smarter, and small businesses are not always equipped to thwart attacks. Compounding this problem is the misperception by business owners of the likelihood of an attack. In a recent survey, Deloitte and Touche, LLP, found that only 41% of roughly 1400 respondents believed that a cyber-attack was highly likely, while 38 % believed that attacks were unlikely or extremely unlikely (Investment Weekly News, 2010).

Given that cyber-attacks are more organized than ever and are increasingly prevalent, it is important to gauge the knowledge of small business professionals to prevent and detect such attacks. Results from an earlier study suggest that students are overconfident in their knowledge of various malware (e.g., viruses) and the potential damage from such malware (Schmidt, Hayes, & Tanner, 2007). We wish to extend that research by testing the knowledge and confidence levels of small business professionals regarding various forms of malware, including viruses, Trojans, spyware, and phishing attacks.

Specifically, the purpose of this study is to examine whether or not small business professionals are overconfident with respect to their knowledge of various computer security threats (e.g., viruses). If these individuals are overconfident and/or uninformed with respect to the aforementioned knowledge, they are less likely to be prepared to face such threats in their own businesses. Further, their overconfidence may exacerbate customers' misconceptions regarding the business' preparedness to fight privacy theft and other forms of cyber-attacks.

Malware

Remarkable advances in computer technology have occurred over the past two decades, influencing virtually every aspect of our lives. Computer technology has especially affected many facets of business. For example, e-mail has replaced the office memo as a means of communication in the workplace. As such, computer proficiency is fundamental to success in today's businesses. This proficiency should also include a working knowledge of malware. Several types of malware are considered in the current study, namely, viruses, Trojans, spyware, and phishing attacks.

Computer viruses are programs that attach themselves to other computer programs, generally without the user's knowledge. Specifically, Crume (2000) defines viruses using the following two criteria:

- the computer virus executes itself when the host program is run, and
- the computer virus replicates by attaching a copy of itself to other programs when it is executed

Of course, the key issue with viruses is the damage, sometimes irreparable, they can cause to a business' computer systems.

While some viruses do minimal damage (e.g., taking up disk space), others can cause significant damage. Boot sector viruses, for example, can quickly spread, and ultimately will prevent a computer's operating system from working correctly (Maximum Security, 2001). Some viruses, such as the CIH virus, are especially dangerous because they can wipe out the BIOS on a user's system, rendering the computer useless (Crume, 2000).

Trojans are similar to viruses, containing code that can create significant damage. However, they cannot spread on their own or replicate themselves (Crume, 2000). Rather, Trojans often spread under the guise of something harmless, such as an e-mail attachment, hence their name.

In recent years, Trojans have been used effectively by cybercriminals to steal confidential information (e.g., bank account numbers). Clampi, Zeus and URLZone are just a few of the more sophisticated Trojans that install themselves on Windows computers and hijack username and password information for use in remote thefts (Vamosi, 2010). Banking information is consistently targeted by these Trojans. For example, Citibank's systems were hacked, resulting in a loss of personally identifiable information (PII) (McGrane & Smith, 2011). Specifically, Citibank reported that data for 1% of their cardholders was accessed through this breach. Some of the information that may have been compromised includes customers' names, account numbers, contact details and email addresses.

Similar to Trojans, spyware programs have the ability to collect personal information and even monitor web pages accessed by the user without their knowledge (Walters & Matulich 2011; Carvey, 2005). Users inadvertently load these programs on their computer when they install free downloadable software (e.g., shareware) (Mensch & Wilkie, 2011; Kucera, Plaisent, Bernard, & Maguiraga, 2005). While spyware programs may not result in data or hardware loss like viruses or Trojans, they can still be problematic for users, especially small business users. Because of their ability to gather potentially confidential information (e.g., Social Security Numbers), spyware programs can be very costly to these businesses in terms of customer litigation, damaged reputation, etc.

Finally, phishing attacks, although not considered malware per se, also pose serious threats to computer security. In a phishing attack, the cybercriminal usually sends the victim a fraudulent email in order to trick the victim into sharing sensitive information or installing malware on their computer (Hong, 2012). Again, the obvious danger is that once the victim shares sensitive information such as bank account numbers, losses can be severe, particularly for small businesses. Not only do businesses face direct losses (e.g., theft) from such an attack, but companies may face indirect losses (e.g., loss of reputation) as well.

Overconfidence

Overconfidence in one's abilities is a common phenomenon; it can be found in a wide range of settings, from capital markets (e.g., Chen, Kim, Nofsinger, & Rui 2007; Ko & Huang, 2007) to the classroom (e.g., Clayson, 2005). Indeed, the research suggests that overconfidence is a strong human tendency that persists even in light of proven faulty judgments. For example, Arkes, Dawes, & Christiansen (1986) found that individuals rely on their own judgments, even when those judgments proved inaccurate.

Research also finds that entrepreneurs tend to exhibit overconfidence in their decision to start a business (Koellinger, Minniti, & Schade, 2007). In addition, Brixy, Sternberg, & Stüber (2013), suggest that overconfidence among entrepreneurs contributes to their reluctance to utilize publicly available assistance for their businesses. Overconfidence among business people is very concerning, particularly given that overconfidence may attribute to high failure rates among new business owners (Koellinger et al., 2007).

In the present study, we look at overconfidence by business people in their knowledge of various malware, including viruses, Trojans, spyware and phishing attacks. If business people are overconfident in their knowledge of malware attacks, they may underestimate the likelihood of losses due to such attacks or they may fail to take appropriate steps to protect business assets and data. As cybercrime statistics soar, this overconfidence, if it exists, could lead to greater losses. Thus, it is important to understand whether or not business people are overconfident in their knowledge of such threats. Hence, we test the following proposition: Business people will be overconfident in their knowledge of computer security threats, specifically, viruses, Trojans, spyware, and phishing attacks.

Methodology

Small business professionals from the Fort Smith, Arkansas region participated in the study, which was conducted in two parts. First, the forty-eight participants completed a survey that asked them to report how confident

they were in their knowledge of various computer security threats. Using a 5-point Likert scale, participants indicated the level of agreement with several statements that assessed confidence in their knowledge of viruses, Trojans, spyware, and phishing attacks. The survey also asked participants about their level of computer usage as well as measures they've taken to address computer security threats in their businesses.

In the second part of the study, these same business professionals took a test to assess their actual knowledge of the aforementioned security threats. The test consisted of several multiple-choice questions related to viruses, Trojan horse programs, spyware and phishing attacks. The purpose of the test was to determine if these individuals could correctly recognize the malware types and identify the potential damages caused by each.

For example, each subject indicated their agreement with three statements that assessed the level of confidence in their knowledge of viruses (e.g., "I am confident in my understanding of computer viruses."). Based on their responses, we created a summated score (VIRUS_CONF), which we could then compare with their score on the portion of the test that assessed knowledge of viruses (VIRUS_SCORE). Various demographic variables were also gathered to more fully understand the environment within which these business professionals operate. The results of both instruments are compiled and discussed in the next section of the paper.

Results

As mentioned previously, forty-eight small business professionals participated in the study. Of those participants, twenty-eight (58%) were male. Thirty-six (75%) participants were also regular users of e-mail and the Internet, reporting that they used both more than twice a day, on average. Moreover, an overwhelming majority of subjects reported using software to mitigate computer security threats, including anti-virus software (94%), firewalls (83%), and spyware removal software (73%). These results suggest that subjects are at least aware of computer security threats and rely on software solutions to minimize them.

To test our proposition regarding whether small business professionals were overconfident in their knowledge of computer security threats, we examined the relationship between their test score in each of the aforementioned areas with their confidence scores. For example, we tested whether a subject's virus test score is a function of their confidence score as stated in the following equation: VIRUS_SCORE = F(VIRUS_CONF).

Table 1 reports the regression results from our study. The average test score in each area was low (e.g., a 34.7% average test score on the virus portion of the test).

Table 1: Panel A: Regression Results

	Average Confidence	Average Test Score	Adjusted R^2	F	t
VIRUS_SCORE=f(VIRUS_CONF)	2.60	34.7%	13.6%	8.391*	2.897***
TROJAN_SCORE=f(TROJAN_CONF)	2.34	20.1%	27.9%	19.204*	4.382***
SPY_SCORE = f(SPY_CONF)	2.83	29.9%	28.6%	19.811*	4.451***
PHISH_SCORE = f(PHISH_CONF)	2.38	46.5%	32.8%	23.942*	4.893***

Panel B: Confidence Item Analysis

	Average Knowledge (Self) (2 questions)	Average Security Measure (1 question)	T
Viruses	2.51	2.77	2.047**
Trojans	2.19	2.65	2.072**
Spyware	2.81	2.88	.36
Phishing	2.28	2.56	1.93*

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

The results, however, do show a significant correlation between subjects' confidence scores and their respective test scores for each security threat tested. In other words, subjects that were more confident in their knowledge of viruses scored better on those test questions, and vice versa. The same was true for the other security threats. If subjects were overconfident in their knowledge of malware, we would not expect to see a significant positive relationship between the two variables. Therefore, subjects in this study do not appear to exhibit overconfidence. This result is contrary to our expectations, since we expected small business professionals to be overconfident in their knowledge of computer security threats similar to the students in Schmidt et al. (2007).

Discussion and Implications

As the above results suggest and contrary to our expectations, small business professionals do not exhibit overconfidence with respect to their knowledge of several computer threats, namely, viruses, Trojans, spyware, and

phishing attacks. Moreover, these results run contrary to prior research that finds individuals tend to be overconfident in many contexts. A possible explanation for these results is that small business professionals have more at stake, since these types of security issues can threaten their very livelihood. This explanation is just one possible scenario and seems reasonable, since one would expect a small business owner to be conservative with respect to business practices that affect their profitability and success.

It should be noted that the confidence scores were relatively low. For example, subjects' average level of confidence about viruses was 2.6, where a 1 indicates low confidence and a 5 indicates high confidence. Participants, on average, were not comfortable with any of these malware issues. Another possibility for the lack of overconfidence is that confidence or knowledge of computer malware threats is not an easy thing to measure. In this study, we asked three questions related to confidence about the various malware threats. Two of the questions asked about the participants own knowledge or confidence in the phenomenon. The third question asked participants to record their level of agreement with the phrase "My computer system is safe from (viruses, Trojans, spyware, phishing attacks)." The average ratings of these questions are provided in Panel B of Table 1. From that data you can see that the average ratings in the security of their business systems (e.g., "My computer system is safe from viruses.") were significantly higher for three of the four types of malware threats utilized in this study. We also retested the original hypothesis using subjects' answers to this one question (e.g., "My computer system is safe from viruses.") to see if the results were different. We found that the confidence in the computer system itself was still positively related to the test scores, but the relationships were not as strong. As before, there does not appear to be evidence of overconfidence.

It is important to note that the test scores in each area were very low, indicating that subjects, on average, were unable to correctly recognize the malware types and the threats they pose. Subjects' average test scores for each security threat were below 50% and well below a "passing grade." This result would suggest that while subjects did not necessarily exhibit overconfidence, their deficiency with respect to computer security threats might still put their businesses at risk.

Finally, we should mention that larger companies typically have the resources to help safeguard their computer systems. Smaller businesses lack these resources, instead relying upon employees' knowledge and readily available tools such as antivirus software. These solutions may not be sufficient, however. Employees may not have the requisite knowledge of various computer security threats. Moreover, the business' software tools may not be regularly updated or are otherwise ineffective at detecting security threats. In either case, there is the potential that companies can face significant losses from security breaches.

Limitations and Future Research

While care was taken to address all methodological issues, there are a couple limitations that warrant discussion. First, it is important to note that the results may not be generalizable due to the limitations inherent in a convenience sample. Subjects for the study came from the Fort Smith region, thus the sample may not be representative of all small business professionals. To further validate the results, future research should replicate this study using small business professionals across a more diverse range of demographics, including different regions of the country, different industries, small towns versus large metropolitan areas, etc.

Second, the results of the study run counter to our expectations about overconfidence. Specifically, we expected subjects to exhibit overconfidence in their knowledge of computer security threats, and this was not the case. While we offer a plausible explanation for this result, future research should investigate the reasons that small business professionals do not exhibit the same overconfidence found in other settings.

Finally, it worth mentioning that while subjects did not exhibit overconfidence, their knowledge of computer security threats is still very lacking. As noted in the previous section, subjects' average scores were below 50% across all four security threats. Kruger & Dunning (1999) argue that this poor performance may be overcome by improving the skill level of participants. Thus, in future research, this proposition can be tested by conducting pre- and post-tests of subjects' knowledge of computer security issues. The answer to this question could have important implications for the content used in training programs.

Despite these limitations, the present study does contribute to our understanding of small business professionals' knowledge of computer security issues. Specifically, it tells us that small business professionals may not exhibit overconfidence in their knowledge of said security issues. The results also remind us, however, that these individuals may still be ill-prepared to protect their business assets from computer security threats. Currently, there is no one piece of software that can detect or prevent all cyber-attacks. Accordingly, data and system security will continue to be a concern. Business owners should consider taking additional precautions to safeguard their systems. For example, hiring individuals or firms to conduct security reviews would be a wise practice. Companies of all

sizes must learn to take the necessary steps to safeguard their assets and their computer data in order to thwart computer hackers.

REFERENCES

Arkes, H., Dawes, R., & Christensen, C. 1986. Factors influencing the use of a decision rule in a probabilistic task. **Organizational Behavior and. Human Decision Processes**, 37(1), 93-110.

Brixy, U., Sternberg, R., & Stüber, H. 2013. Why some nascent entrepreneurs do not seek professional assistance. **Applied Economic Letters**, 20(2), 157-161.

Carvey, H. 2005. **Windows forensics and incident recovery**. Boston, MA: Addison-Wesley.

Chen, G., Kim, K., Nofsinger, J., & Rui, O. 2007. Trading performance, disposition effect, overconfidence, representativeness bias, and experience of emerging market investors. **Journal of Behavioral Decision Making**, 20(4), 425-451.

Clayson, D. 2005. Performance overconfidence: Metacognitive effects or misplaced student expectations? **Journal of Marketing Education**, 27(2), 122-129.

Crume, J. 2000. **Inside internet security**. London: Addison-Wesley.

Data Breach Investigations Report. 2012. Verizon Corporation.

Deloitte poll: Respondents lack confidence in ability of private enterprises to reduce the occurrence of cyber crime. (2010, September 25). **Investment Weekly News**, p. 193

Gorman, S., & Perez, E. (2009, November 11). Hackers indicted in widespread. ATM heist. **Wall Street Journal**, p. A.10.

Hong, J. 2012. The state of phishing attacks. Association for Computing Machinery. **Communications of the ACM**, 55(1), 74.

Kruger, J. & D. Dunning. (1999). Unskillled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. **Journal of Personality and Social Psychology**, 77, 1121-1134.

Ko, K., & Huang, Z. 2007. Arrogance can be a virtue: Overconfidence, information acquisition, and market efficiency. **Journal of Financial Economics**, 84, 529-560.

Koellinger, P., Minniti, M., & Schade, C. 2007. I think I can, I think I can: Overconfidence and entrepreneurial behavior. **Journal of Economic Psychology**, 28(4), 502-527.

Kucera, K., Plaisent, M., Bernard, P., & Maguiraga, L. 2005. An empirical investigation of the prevalence of spyware in internet shareware and freeware distributions. **Journal of Enterprise Information Management**, 18(6), 697-708.

Maximum security. 2001. Indianapolis, IN: Sams Publishing.

McGrane, V., & Smith, R. (2011, June 9). Hacking at Citi is latest data scare. **Wall Street Journal**, p. C.1.

Mensch, S., & Wilkie, L. 2011. Information security activities of college students: An exploratory study. **Academy of Information and Management Sciences Journal**, 14(2), 91-116.

Schmidt, G., Tanner, M., & Hayes, T. 2007. Computer security threats: Student confidence in their knowledge of common threats. **Journal of Business and Leadership: Research, Practice, and Teaching**, 3(1), 211-215.

Skinner, C. 2010. 25 million new malware strains found in 2009. **PC World**, 28(3), 44.

Vamosi, R. 2010. New banking Trojan horses gain polish. **PC World**, 28(1), 41.

Walters, M., & Matulich, E. 2011. Assessing password threats: Implications for formulating university password policies. **Journal of Technology Research**, 2: 1-9.

Thomas Hayes is an associate professor of accounting at the University of Arkansas - Fort Smith. He received his Ph.D. in accounting from University of North Texas. His current research interests include auditing, information systems, and accounting pedagogy. He has published in Academy of Information and Management Sciences Journal, International Journal of Business, Accounting, and Finance, International Journal of Education Research, and others.

Margaret Tanner is an associate professor of accounting and Head of the Department of Accounting, Economics and Finance at University of Arkansas - Fort Smith. She received her Ph.D. in accounting from University of North Texas. Her current research interests include pedagogical issues, financial reporting, and curriculum development and assessment. She has published in International Journal for Educational Integrity, International Journal of Education Research, Journal of Business and Leadership, and others.

George Schmidt is an associate professor of accounting at University of Arkansas - Fort Smith. He received his Ph.D. in accounting from University of North Texas. His current research interests include financial accounting and information systems. He has published in International Journal of Business, Accounting, and Finance, Journal of Business and Leadership, and others.