Human kidnapping for Ransom the Probability for Cyber Kidnapping

Dr. Okey Igbonagwam, The Donald R. Tapia School of Business, Saint Leo University, Virginia Beach, VA, USA

Dr. Kingsley Nwosu, The Donald R. Tapia School of Business, Saint Leo University, Newport News, VA, USA

ABSTRACT

There are evidences suggesting technological era has benefitted mankind in so many ways, while at the same time introduced technology based criminal activities such as hacking. Computing hacking attacks impact could have on an organization, including damage to systems that require human intervention to repair or replace, disruption of business operations, and delays in transactions and cash flow. Many enterprises, modern threats catastrophically destroyed their businesses. For example, DigNotar was compromised in 2011by fraudulent Certificate Authority (CA), which generated hundreds of seemingly valid certificates for dozens of popular domains. This attack led to DigNotar to file bankrupt, example cyber-attacks are no longer a joke. Cybercrime is now a common vocabulary, just as Hackers are synonymous with nefarious attacks. Miller suggests these hackers are evolving from "whiz kids" seeking notorieties into bona fide cybercriminal, often motivated by significant financial gains. They are even in some cases sponsored by nation-states, criminal organizations, and radical political groups.

Introduction

Judging how an information system (IS) has influenced individuals, there must be strategies and programs to effectively secure their computer assets, while preventing IS compromise (Im and Baskerville 2005).

On organizational levels, prior research has concluded that the largest security threat facing organizations is the inappropriate or insecure behavior of its own IS users (Keller et al. 2005; Ramim and Levy 2006; Whitman 2003). The causes of these behaviors are not fully understood, and research is required to identify the factors responsible for the inappropriate security behavior of IS users (Teer et al. 2007). Cronan and Douglas (2006) argued the need for a better understanding of the precedents of inappropriate security behavior.

Is ransomware the next cybercrime wave? Miller suggests today's cyber threats are sophisticated and pervasive. Many enterprises and information are being targeted, equally evidence these threats are not limited to business entities but also individuals. This study will investigate this phenomena and the probability of individual single strike.

Arora (2012) defines ransomware as "a kind of malware that first installs itself on a victim's system through downloads or malicious links, then proceeds to encrypt important files that can be only decoded on payment by a private key provided by the attacker." Weisbaum (2013) describes ransomware as a diabolic nasty malware that can lock up all the users' personal files including backup files in some cases with state-of-the-art encryption. The attacker(s) have the only decryption key and demand payment such as $300 or two Bitcoins to decry the files. Even with threat of this nefarious cyber-attack, the publicly awareness appears limited. The Webster dictionary, for example is yet to update in its vocabularies. However, it is important to elevate ransomware to higher public awareness, especially as cybercrimes continue to envelop into newer dimensions. Abrams (2013) describes CryptoLocker, a ransomware program released in September 2013 targeted all versions of Windows including Windows XP, Windows Vista, Windows 7, and Windows 8. It encrypted certain files using a mixture of RSA & AES encryption. After, it displays a CryptoLocker payment program prompting the users to send a ransom of either $100 or $300 in order to decrypt their files. Abrams states, "this screen will also display a timer stating that you have 96 hours, or 4 days, to pay the ransom or it will delete your encryption key and you will not have any way to decrypt your files. This ransom must be paid using MoneyPak vouchers or Bitcoins. Once you send the payment and it is verified, the program will decrypt the files that it encrypted."

This study investigated Computer self-efficacy (CSE) relating to ransomware. CSE is defined as individuals' judgment of their ability to use a computer in the achievement of a job task (Compeau and

Higgins 1995), has been used to explain the behavior of IS users (Compeau and Higgins 1995; Kuo and Hsu 2001; Marakas et al. 1998). Research has shown that CSE exerts a significant influence on an individual's decision to use computers to achieve various tasks (Compeau and Higgins; Kuo and Hsu 2001; Marakas et al.). One problem with using CSE, however, is its generalizability, that is "the extent to which self-efficacy perceptions are restricted to particular situations" (Compeau and Higgins 1995, p. 192). As such, Compeau and Higgins argued the need for further examination of CSE and its associations with specific domains of interest or tasks relating to computers. InfoSec represents one such computer-related task that can be performed by a group of non-specialist IS users (Aytes and Connolly 2004). Marakas et al. (2007) argued that even vigorously validated measures of CSE, when applied to unrelated studies, will have limited generalizability.

As such, researchers have been advised to develop new measures, or to significantly revise and revalidate existing measures to align measures of CSE with the specific task being investigated (Bandura 2001). This research built on seminal work of Compeau and Higgins (1995) by addressing the need for the development of newly specialized CSE measures, examining the inappropriate

Theoretical Background

The theory of self-efficacy theory (SCT) (Bandura 1977) advocates the belief one has in his or her capability to perform a specific task. The theory is that environmental influences such as social pressures, cognitive and other personal factors such as personality and demographic characteristics, and behavior are reciprocally determined (Compeau and Higgins 1995).

The SCT advances output expectations and self-efficacy as the cognitive forces that influence behavior (Bandura 1977; Compeau and Higgins 1995). Accordingly, individuals will undertake behaviors they see as having favorable outcomes (Compeau and Higgins 1995). Thus, before actually performing a behavior, individuals often evaluate their ability to perform such behavior. Self-efficacy expectations deal with beliefs about one's ability to perform a particular task (Bandura 1986). As such, it relates to judgments of what individuals can do with the skills they possess and is not focused on the actual skill itself.

Computer Self-efficacy

Derived from the broader self-efficacy construct, CSE is concerned with self-efficacy in relation to computer use and was defined by Compeau and Higgins (1995) as “an individual’s perception of his or her ability to use a computer in the accomplishment of a job task” (p. 193). Using an empirical study of the perception of 2000 randomly selected knowledge workers, Compeau and Higgins examined how computer use was mediated by encouragement of others, duration of use and use by others, organizational support and training, outcome expectations, affect, and anxiety. Compeau and Higgins concluded that IS users with higher CSE had higher usage of computers, enjoyed using them more, and possessed less computer related anxiety.

These claims were further validated in a later study of 394 subjects (Compeau et al. 1999). For their seminal study, Compeau and Higgins (1995) developed the instrument of CSE consisting of 10 items in ascending order of difficulty; respondents were asked to state whether or not they could complete the job using a software package. If respondents could complete the task, they would then indicate their confidence in their ability using a 10-point Likert scale. The Compeau and Higgins measure has been applied in various technological contexts, and has been identified as having high reliability and validity (Levy and Green 2009). The original seminal CSE instrument was central to this research study as it was used as the foundation for the development of a new Computer Security Self-Efficacy (CSSE) instrument and construct

Computer Self-Efficacy and Information System Security

There has been limited research that advances CSE as a variable in the study of InfoSec related behaviors. Crossler and Belanger (2006) examined the impact of CSE on the usage of InfoSec tools, based on the level of instruction received by individuals. They concluded that an individual’s level of CSE directly impacted his or her use of security tools. Phelps (2005) examined the effect of CSE on the effectiveness of InfoSec in relation to a library IS and concluded that participants with higher self-efficacy were more effective at implementing system security. Other researchers, such as Chai et al. (2006), as well as Lee, LaRose, and Rifton (2008) also identified a positive relationship between self-efficacy and information security behavior, however, they failed to develop and validate a robust specialized instrument to measure CSE in the context of InfoSec.

In reviewing measures utilized in prior studies measuring InfoSec related self-efficacy, multiple instruments were identified. Chai et al. (2006) utilized a four-item measure, adapted from the work of Bandura et al. (1996), and originally developed to measure academic self-efficacy. The adapted measure consisted of four items, and utilized a five-point response format. Chai et al., however, argued the need for future studies incorporating additional factors and a larger, more diverse population.

In another study, Lee et al. (2008) developed a five-item measure that evaluated individuals' confidence to run an anti-virus program, install personal firewalls, update virus definitions, update patches, and screen e-mail on a seven-point scale. Lee et al. conceded that the model needed additional refinement and validation. Further, Phelps (2005) developed a measure for self-efficacy in the context of InfoSec comprising 20 questions and a responses scale of 0 to 100. Phelps recommended that further research should be conducted aimed at enhancing the instrument to ensure construct validity, and to further examine factors that influence InfoSec.

This study attempted to fulfill that need through the development and validation of the CSSE measurement instrument related to a single ransomware occurrence on an individual computer user.

Research Questions

There have been no significant empirical studies on this subject. This study attempts to answer below questions and observe how it could contribute to better understanding of this type of cybercrime.

1. How much do you know about ransomware?
2. What is the probability of individual ransomware attack?
3. Does the law enforcement agencies equipped to deal with cybercrimes like ransomware?

4. What is the probability of law enforcement agencies dedicating a ransomware?

Research Methodology

Through a review of existing literature, an initial list of CSSE items was developed. The initial list of items was developed based on a review of existing literature (Bandura 1977; Compeau and Higgins 1995; Compeau et al. 1999; Crossler and Bellanger 2006; Gist and Mitchell 1989; Hill et al. 1987; Marakas et al. 1998; Torkzadeh et al. 2006). There were 32 initial CSSE items identified from the literature review.

Qualitative Phase

The 20 CSSE items obtained from the literature review were used to develop a preliminary CSSE survey instrument. The instrument asked respondents to assess their current capabilities related to dedicating a cyber-attack like ransomware by responding to a series of multiple choice questions. The instrument utilized a 7-point Likert scale allowing responses on a confidence scale of 1 to 7, with 1 indicated the lowest confidence and 7 the highest confidence that the individual could be impact by ransomware given various scenarios. Participants in the main survey were asked to respond to the question: *"I believe I have the ability to dictate a ransomware attack…"* given various scenarios.
Expert Panel: The preliminary survey instrument was put through a qualitative review by an experts' panel of three IS faculty members and three IS professionals who evaluated the instrument, the clarity of the items, and the precision of the instruments. Feedback from the expert panel was used to adjust the instrument resulting in a finalized survey instrument containing 20 items (Appendix A). The results of the expert panel were appropriate in making a determination of the instrument's validity and addressed the second research question for this study.

Probability of Zero Leakers, PZL Main Study

Subsequently, this study uses a subjective probability which reflects judgment of individual Balakrishnan, N., et, al. (2013). This study applies Probability of Zero Leakers (PZL) as an effective approach to matric ransomware occurrences. The PZL is a scenario-level metric suitable for use in multiple-threat raids defined as the probability that all threats of concern in a scenario will be successfully eliminated by the BMDS (Wilkening 1999). As such, PZL is often used interchangeably with the Navy's Probability of Raid Annihilation (PRA) which was originally defined as the probability that a "single ship will be able to defend itself against multiple anti-ship cruise missile threats (a raid)" (Blake, Little and Morse 2003) and later adopted for use in Ballistic Missile Defense (BMD). PZL is a particularly good metric to use when the possibility of even a single leaker would be so devastating that it warrants ignoring all other possible outcomes, such as the possibility of one or more leakers.

In this study, PZL has the advantage of being very simple to calculate if a mechanism is already in place to determine the probability ransomware occurrence (PRO) for each attack. As shown in the equation below, PZL is equal to the product of the PRO values associated with each of the N attacks.

$$P_{ZL} = \prod_{i=1}^{N} (P_{RO,i})$$

One key observation which follows from this simple equation is that the ransomware occurrences against other cyber-attacks, in terms of P_{ZL}, will always be lower (and in many cases, it will be much lower) than the P_{RO} occurring more than once against each individual computer. Because every cyber-attack may be less than one P_{RO} occurrence, multiplying many P_{RO} values together returns a lower P_{ZL}. For example, if the P_{RO} between every cyber launch and every target computer equals .93, and we may face an attack of three, then expanding the P_{ZL} equation we have:

P_{ZL} = P_{RO} (Zero Occurrence) * P_{RO} (One Occurrence) * P_{RO} (Two Occurrences)

= (0.93) * (0.93) * (0.93)

= 0.8

Given occurrence of two, a P_{RO} of 0.93 translates into a P_{ZL} of 0.8. In other words, a P_{RO} of 0.93 against each occurrence would translate into only an 80% chance of successfully damage to individual computers. A .93 P_{RO} therefore does not translate into a 0.93 probability of successfully damage to individual computers.

Conclusions

The examples from the preceding sections have shown how misunderstanding the applicability of a metric to the type of scenario one is trying to study can drastically skew the results obtained.

It was shown that single-threat-scenario metrics such as probability ransomware occurrence (Pro) may still be harmful to a single computer user, even at the level when considering multiple cyber-threat scenarios. Because Pro and other cyber-attack only provide information about harmfulness even a single threat, attempting to use one of these metrics for multiple-threat scenarios can result in greatly underestimating the damage of cyber-attack like the ransomware.

Probability of Zero Leakers, P_{ZL}, was then presented as a viable option for use in multiple-threat scenarios, and its limited ability to fully characterize the performance of a BMDS against a multiple-threat raid was explained. Using P_{ZL} exclusively can result in ambiguity in the output data in the best case, and in the worst case can result in trends that are opposite of the real capability of the system.

Summary of Key Research Findings

Four main factors of CSSE were identified; Performance Accomplishments and Technical Support, Goal Commitment and Resource Availability, Experience Level, and Individual Characteristics. The Cronbach's Alpha of the four factors was very high, indicating high reliability for all four factors. The Performance Accomplishments and Technical Support factor was found to explain the largest variance in the data collected, just under 29%. This factor included the CSE characteristics of performance accomplishment and situational support found in literature (Bandura 1977; 1986). Bandura (1977) identified performance accomplishment as the most crucial source of self-efficacy beliefs. Thus, one conclusion drawn from this study is that prior success using encryption, and access to readily available support should likely result in high CSSE and users who are more likely to avoid ransomware.

Goal Commitment and Resource Availability, the second significant factor, represented a combination of the existing goal commitment, time, and persuasion characteristics identified in prior literature (Compeau and Higgins 1995; Marakas et al. 1998). These characteristics from literature were supplemented with the newly identified characteristic of resource availability.

Resource availability was identified in the qualitative phase as an item that individuals considered important when assessing their ability to dictate a ransomware. This factor explained over 20% of the variance in the collected data.

The third factor identified was Experience Level, and consisted of the characteristics of

skill level identified in prior literature (Bandura 1977; Marakas et al. 1998). The conclusion, therefore, is that an individual's experience level will impact their CSSE level. The experience level factor explained just over 10% of the variance in the data collected.

The final factor, Individual Characteristics, represented a collaboration of two characteristics identified in prior literature, namely age and gender (Bandura, 1986; Marakas et al., 1998). Of interest is the fact that age appears to impact CSSE, irrespective of whether the respondent is younger or older. This factor, although important, explained only 9% of the variance in the data, the least of all the factors identified.

Implications

This study has several implications for the field of IS. First, this study contributes to the body of knowledge regarding the use of cyber-attack like ransomware. Prior seminal research, such as Compeau and Higgins (1995), Kuo and Hsu (2001), as well as Marakas et al. (1998) have confirmed the effectiveness of CSE in influencing an individual's decision to use computers to achieve various tasks. By extending CSE research into the area of ransomware cyber-attack, this study has provided new information that may contribute to a better understanding of the precedents of inappropriate InfoSec behavior of IS users. Consequently, we hope that this work will provide fertile ground for future research aimed at understanding the precedents of industrial and governmental entities specifically, and InfoSec behavior more generally.

This study is also significant as it holds implications for the InfoSec industry. Prior research has argued for a better understanding of the precedents of inappropriate user security behavior as this can aid in the development of strategies to influence these behaviors. Understanding what IS users consider important in their ability to dictate a ransomware should assist computer security professionals' work to increase security defense mechanisms and potentially other InfoSec mechanisms. Thus, this study may have implications for the development of strategies to promote positive InfoSec behaviors.

Business Applicability

This study findings would necessitate security awareness consultancy not just for individual computer users but also corporate and governmental entities. Because Cyber-attacks like the ransomware is dangerous to all computer users; thus, the commitment to protecting computing assets are also not locally confined, cyber-attacks are global issues. As such, other factors like culture impact any common solutions for a global issue. So, an innovative security awareness approach must provide a level plain field for this global issue. Web based initiative is proposed with database as a clearing house to enhance cyber related security defense to provide computer users with timely necessary information. Furthermore, cyber-attack like ransomware is a form of kidnapping of computer assets for ransoms. In human kidnapping scenario, there are negotiators to facilitate the release of kidnapped persons. We believe that there might be a need for such in the cyber-attack like ransomware scenario, because some computer information assets might also be a life and death consequences, and negotiation must be necessary.

Because when users fail to respond to these demands, these assets could be totally be destroyed. So, security assurance becomes even more significant when our customers are faced with a data breach like the one recently announced by Target with unauthorized access to customer information in Target stores between Nov. 27 and Dec. 15, 2013.

Finally, future research should attempt to evaluate the predictive nature of CSSE in the context of other valid IS constructs, using other populations like government and corporate entities to enhance generalizability.

References

Abrams, L. (2013). CryptoLocker Ransomeware Information Guide and FAQ: Bleeping Computer LLC.

Arora, K. (2013). Cyber Threat: Now, 'ransomware' plays havoc with data [Software]: The Economic Times (Online) [New Delhi] 25 Oct 2013.

Balakrishnan, N., Render, B., and Stair, R. M. (2013). Managerial Decision Modeling with SpreadSheets: Prentice Hall, Upper Saddle River. NJ.

Ball, R.E. (2003). *The Fundamentals of Aircraft Combat Survivability Analysis and Design.* AIAA.

Bandura, A. (1977). “Self-efficacy: Towards a Unifying Theory of Behavioral Change,” *Psychological Review*, (84:2), February, pp. 191-215.

Ben-Asher, J.Z. (2004). "Systems Engineering Aspects in Theatre Missile Defense-Design Principles and a Case Study." *Systems Engineering* 7, no. 2: 186-194.

Blake, Donna W., Carolyn Little, and Judy Morse (2003). "03-SIW-057 The Navy’s Probability of Raid Annihilation Assessment Process.

Brown, Gerald, Matthew Carlyle, Douglas Diehl, Jeffrey Kline, and Kevin Wood. (2005). "A Two-Sided Optimization for Theater Ballistic Missile Defense." *Operations Research* 53, no. 5 (September-October): 745-763.

Compeau, D. R., and Higgins, C. A. (1995). “Computer Self-efficacy: Development of a Measure and Initial Test. *MIS Quarterly*, (19:2), pp. 189-211.

Cronan, T.P. and Douglas, D.E. (2006) Toward a comprehensive ethical behaviour model for information technology, *Journal of Organisational and End User Computing*, 18(1), i-xi.

Davis, Paul K., Russell D. Shaver, and Justin Beck. (2008). *Portfolio-Analysis Methods for Assessing Capability Options.* Santa Monica, CA: RAND Corporation.

Erbschloe, M. (2003). Guide to Disaster Recovery. Course Technology Cengage Learning: Mason, Ohio.

Garrett, Robert K., Jr., Steve Anderson, Neil T. Baron, and James D., Jr. Moreland. (2011). "Managing the Interstitials, a System of Systems Framework Suited for the Ballistic Missile Defense System." *Systems Engineering* (Wiley Periodicals) 14, no. 1: 87-109.

Im, G. P., and Baskerville, R. L. 2005. “Information System Threat Categories: The Enduring Problem of Human Error,” *The DATA BASE for Advances in Information Systems*, (36:4), pp. 68–79.

Keller, S., Powell, A., Horstman, B., Predmore, C., and Crawford, M. (2005). “Information Security Threats and Practices in Small Businesses,” *Information Systems Management*, (22:2), pp. 7-19.

Kuo, F., and Hsu, M. (2001). “Development and Validation of Ethical Computer Self-efficacy: The Case of Softlifting,” *Journal of Business Ethics*, (32:4), pp. 299-315.

Lee, Y., and Larsen, K. (2009). "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems* (18:2), pp. 177-187.

Miller, L. C. (2012). Modern Malware for Dummies. John Wiley & Sons, Inc: Hoboken, NJ.

Malimage, K., and Warkentin, M. "Influence of Perceived Value of Data on Anti-Virus Software Usage: An Empirical Study of Protection Motivation," Paper presented at the Dewald Roode Workshop on Information Systems Security Research, Blacksburg, VA, 2011.

Marakas, G., Johnson, R., and Clay, F. (2007). “The Evolving Nature of the Computer Selfefficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time,” *Journal for the Association of Information Systems,* (8:1), pp. 16-46.

Ramim, M., and Levy, Y. (2006). “Securing E-learning Systems: A Case of Insider Cyber Attacks and Novice IT Management in a Small University,” *Journal of Cases on Information Technology,* (8:4), pp. 24-34.

Teer, F. P., Kruck, S. E., and Kruck, G. P. (2007). “Empirical Study of Students’ Computer Security Practices / Perceptions,” *The Journal of Computer Information Systems*, (47:3), pp. 105-110.

Under Secretary of Defense for Acquisition, Technology & Logistics. "Report to Congress on the Assessment of the Ground-Based Midcourse Defense Element of the Ballistic Missile Defense System." Washington, D.C., 2010.

Weisbaum, H. (2013). CryptoLocker crooks launch new 'customer service' website for victims, NBC News contributor Nov., 14, 2013.

Whitman, M. (2003). “Enemy at the Gate: Threats to Information Security,” *Communications of the ACM,* (46:8), pp. 91-95.

Wilkening, D.A. (1999). "A Simple Model for Calculating Ballistic Missile Defense Effectiveness." *Science & Global Security* 8:2: 183-215.