Winter 12-13-2018

SNS Use, Risk, and Executive Behavior

Andrew Green
Kennesaw State University

James Parrish
University of North Texas Health Sciences Center

James Smith
Augusta University

jason B. Thatcher
University of Alabama

SNS Use, Risk, and Executive Behavior

Andrew Green[1]
Michael J. Coles College of Business, Kennesaw State University
Kennesaw, Georgia, USA

James Parrish
College of Business, University of North Texas
Denton, Texas, USA

James N. Smith
School of Computer and Cyber Sciences, Augusta University
Augusta, Georgia, USA

Jason B. Thatcher
Culverhouse College of Business, the University of Alabama
Tuscaloosa, Alabama, USA

ABSTRACT

Organizations can suffer attacks designed to take advantage of employee vulnerabilities. Successful attacks cause firms to suffer financial damage ranging from minor information breaches to severe financial losses. Cybercriminals focus on organization executives, because the power and influence they wield affords access to more sensitive data and financial resources. The purpose of this research in progress submission is to identify the types of executive behaviors that information security professionals believe introduce risk to an organization, as well as to explore the degree of risk organizations face as a result of these behaviors.

Keywords: Information Security; Executive behavior; Organizational risk; Cybersecurity; SNS usage

MOTIVATION

Cybercriminals direct social engineering (SE) attacks at organizational employees as a means to secure access to sensitive data (Conteh and Royer 2016; Gardner and Thomas 2014; Greitzer et al. 2014; Wilcox et al. 2014). For example, cybercriminals use pretexting, a form of

[1] Corresponding author. agreen57@kennesaw.edu

SE, to create scenarios that convince victims to perform a desired action (Brody et al. 2012; Greitzer et al. 2014; Luo et al. 2011). Examples of successful pretexting attacks include the theft of employee W2 data, or loss of hard dollars (Honan 2015; Rivera 2018). Pretexting can be embedded in many vectors of attack, including phishing (Conteh and Royer 2016; Symantec 2015; Verizon Enterprises 2016), spear phishing (He 2012; Heartfield and Loukas 2015; Laszka et al. 2015; Teplinsky 2013), vishing via telephone, voice over IP (VoIP), or short message service (SMS) messages (Gardner and Thomas 2014; Shahriar et al. 2015). Such breaches put organizations at risk in three primary areas: monetary losses, corporate liability, and credibility (Cavusoglu et al. 2004).

Constantiou and Kalinikos (2015) observed that data gathered from social network sites (SNS) could be used to design SE attacks. SNS users share personal information for various reasons, such as developing or maintaining personal relationships or general knowledge acquisition (Krasnova et al. 2017; Wakefield and Wakefield 2016), as well as perceived benefits to job performance (Ali-Hassan et al. 2015). Such data, collected from employees' personal social media presence, such as community-based platforms (Facebook, Twitter, and LinkedIn), discussion boards, blogs, wikis, and the like (Greitzer et al. 2014; He 2012; Kim 2012), help cybercriminals to design authentic pretexting scenarios.

Consider Business Email Compromise (BEC) attacks, which focus on compromising or spoofing the email accounts of organization executives (Federal Bureau of Investigation 2017; Honan 2015; Korolov 2015). This form of pretexting is often referred to as an email account compromise (EAC) attack, and are a component of the overall BEC attack chain (Federal Bureau of Investigation 2017). Organization executives are frequent targets of EACs because of their access to sensitive data, as well as their ability to command actions from subordinates (Bullée et

al. 2017; Federal Bureau of Investigation 2017; Sharp 2017; Trustwave 2017). With an EAC attack, the cybercriminals can use social media data to hijack or spoof executives' accounts and convince employees to initiate an electronic funds transfer (EFT) or wire transfer to a bank account that they control, primarily located in China and Hong Kong (Burch et al. 2015; Federal Bureau of Investigation 2017; Kemp 2016).

Addressing risks organizations face from executive social media use has been lightly explored in the information security literature. Research has touched on the impact of executive behavior impact on financial reporting risks, project management risks, (Davidson et al. 2015; Liu and Wang 2016), information leakage about the organization itself (Molok et al. 2013), and damage to organizations and their customers (Cain 2011). Additionally, while existing literature has explored steps organizations can take to minimize the potential damage from social engineering attacks in general (Rocha Flores and Ekstedt 2016; Vaast and Kaganer 2013), to understand the legalities surrounding organizational policies regarding employees use of their personal social media channels in non-work related situations (Sánchez Abril et al. 2012), and examined organizational issues associated with surveillance of personal SNS (Uldam 2016), scant literature sheds light on the financial risks executives social media use.

Research objective

While an extensive literature examines individual drivers of SNS use (boyd and Ellison 2007), scant research examines how the SNS use of executives create risks for their employing organization in ways that SNS use by regular rank-and-file employees do not. For example, executives disclosing their location in a SNS post may pose a financial risk to an organization, as it may offer insight into strategic maneuvers by firm leadership. To explore executive behaviors, we propose asking information security professionals how executives SNS use pose

risks, particularly financial risks, to an organization. An associated goal of this research study is to explore the degree to which these behaviors pose additional forms of risk to an organization. Hence, we investigate: What executive SNS behaviors pose financial risks to an organization?

LITERATURE REVIEW

Information Security definition

The term information security, while frequently used, lacks a seminal definition or explanation. Existing literature observed the term is a concept that lacks a clear-cut definition (Anderson 2003; Torres et al. 2006). Dlamini et al. (2009) found that the concept of information security predates the invention of the computer. Interestingly, there are numerous articles (Crossler et al. 2013; Johnston et al. 2015; Lowry et al. 2015; Rocha Flores and Ekstedt 2016) which use the term information security without ever supplying a definition, thus leaving it to the reader to interpret its meaning through their own personal lenses and experiences.

Further complicating the issue of defining information security is the increasing use of the terms cybersecurity or cyber security. These terms may be viewed by some as having the same meaning, thus making their usage interchangeable (Agresti 2010; von Solms and van Niekerk 2013). von Solms and van Niekerk (2013) explored the differences between the terms information security and cyber security/cybersecurity, concluded there is a difference between the terms, and argued they should not be used interchangeably. This study will use the Torres et al. (2006, p. 532) definition of information security as "…a well-informed sense of assurance that information risks and technical, formal and informal controls are in dynamic balance".

Organization executives

Existing literature has explored organization executives through multiple lenses. As early as Hambrick (1981), literature explored the impact that executives had on the success of their

organization. The seminal work of Hambrick and Mason (1984), which offered the Upper Echelons perspective model, served as a foundation for exploring the various ways in which organizational outcomes can be anticipated. According to Hambrick and Mason (1984), organizational outcomes should be viewed as reflections of top managers and their values. Hambrick and Mason (1984) also argued that the behavior and characteristics of executives mattered as it related to organizational outcomes. Hambrick and Mason (1984) theorized that top managers made strategic choices that would impact the performance of the organization. According to Hambrick and Mason (1984), the success or failure of these choices could be partially predicted based on observable criteria such as age, functional tracks, prior career experiences, education level, socioeconomic background, financial position, and group characteristics.

Building on Hambrick and Mason (1984), Hambrick et al. (2005) argued that senior executives are of specific interest because they serve as an interface between the organization and its environment, and wield sufficient power to impact the organization. According to Hambrick et al. (2005), executive level work is qualitatively different than work found at other levels of the organization. Hambrick et al. (2005) also found that executive leadership behaviors could impact both the vitality and performance of their organization, and thus warranted further examination.

Organization executives are of special interest to adversaries, because of the level of access and oversight they have. Krombholz et al. (2015) outlined whaling attacks, a type of phishing attack, which specifically targets organization executives. Adversaries can use whaling attacks to achieve different goals. For example, Hong (2012) described whaling attacks targeting chief operating officers (CEOs) with fake subpoenas as email attachments, which had malware

installed. In 2016, a finance executive at Mattel was the victim of a whaling attack, resulting in a $3 million EFT that was recovered before it could be collected by the adversaries (Associated Press 2016).

Organizational information disclosure

A review of existing literature regarding organizational information disclosure revealed the presence of multiple themes in the space. Conger et al. (2013) explored the challenges organizations face in protecting corporate data. Among their findings in this area, Conger et al. (2013) noted that data collection and sharing among organizations, combined with the growing number of ways that customer data can be collected, pose a significant challenge to organizations in their efforts to protect data collected. Hsu et al. (2015) studied the effectiveness of extra-role behaviors exhibited by organization workers as they relate to information security policy effectiveness. Defined as employee behaviors which extend beyond those described in organization security policies, Hsu et al. (2015) found that when combined with in-role behaviors, extra-role behaviors have a positive impact on organizational security policy effectiveness. Lowry and Moody (2015) proposed a new model which examined employee motivations, in an attempt to determine employee intent to comply with new organization security policies. This model, which combined control theory with reactance theory, found that organizational controls were a positive predictor of an employee's intent to comply with new security policy, while perceived threats to personal freedom resulted in employee reactance to new security policy. Lowry et al. (2015) explored ways in which organizations could leverage fairness theory and reactive theory to increase the likelihood that employees would adhere to organization security policies. Among their findings, Lowry et al. (2015) discovered that employees were more likely to adhere to organization security policies if an atmosphere of

organization trust existed. Lowry et al. (2015) found that one method to increase the level of organization trust was through the implementation of explanation adequacy, in which employees were informed as to the underlying reason for the existence of, and the importance of, organization security policy. Lee et al. (2016) examined the impact of mandatory standards on the effectiveness of organizational information security. Among their findings, Lee et al. (2016) reported that implementation of a higher security standard does not necessarily lead to an increase in security for an organization.

Existing literature has also explored the marketplace consequences organizations can face after suffering a data breach. Wang et al. (2013) examined the impact organizations may face when publicly disclosing a data breach event. Wang et al. (2013) found no significant difference in marketplace reaction when an organization disclosed a data breach in financial reporting documents, but that the marketplace did respond differently when a breach was announced outside the release of financial reporting documents.

METHOD

Grounded theory methods were first proposed by Glaser and Strauss (1967). Grounded theory methods can be applied to both qualitative and quantitative research data (Charmaz 1995). Grounded theory emphasizes theory development, and allows researchers to aim at various levels of theory when conducting research (Denzin and Lincoln 1994). Use of grounded theory methods allows the researcher to discover concepts which are grounded in collected data, as well as determining their underlying sources (Corbin and Strauss 1990). Glaser and Strauss (1967) argued that grounded theory methods could be used to develop new theory by focusing on the differences between daily realities of behaviors, and how those behaviors are interpreted by those who engage in those behaviors (Suddaby 2006). Because there is little understanding of the

degree of financial risk posed to an organization by way of executive behaviors and SNS usage, use of grounded theory methods will provide an avenue to determining the answer to the research question for the proposed study.

The proposed study of financial risks associated with executive use of SNS will be a two-phase, mixed methods study. Data will need to be collected about the specific behaviors that executives can engage in via SNS usage, which may result in financial risks to an organization. Once this data is collected and analyzed, the behaviors will then be grouped into constructs for the purpose of collecting further data about the degree to which these behaviors may pose a financial risk to an organization. The figure below illustrates the proposed structure of the study to be performed.

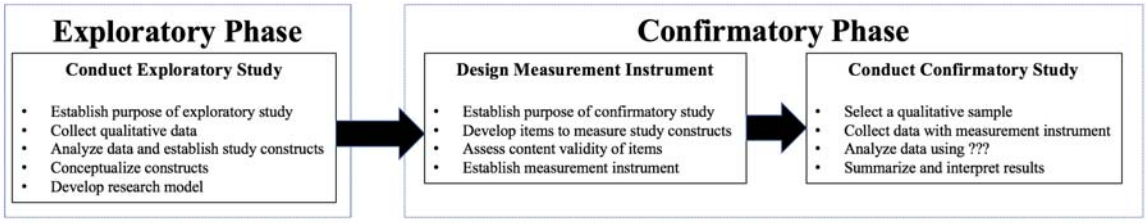

Figure 1. Proposed study structure

This study will advance current research by gaining a deeper understanding of how executive behaviors on SNS impact risk to the organization. This deeper understanding will come about as a result of collecting examples of senior executive behaviors from information security professionals, which they believe pose risk to an organization. These behaviors will then be grouped into constructs, which will then be rated by information security professionals in terms of degree of risk to an organization.

REFERENCES

Agresti, W. W. 2010. "The Four Forces Shaping Cybersecurity," in: *IEEE Computer Magazine*. pp. 101-104.

Ali-Hassan, H., Nevo, D., and Wade, M. 2015. "Linking Dimensions of Social Media Use to Job Performance: The Role of Social Capital," *The Journal of Strategic Information Systems* (24:2), pp. 65-89.

Anderson, J. M. 2003. "Why We Need a New Definition of Information Security," *Computers & Security* (22:4), pp. 308-313.

Associated Press. 2016. "Mattel Vs. Chinese Cyberthieves: It's No Game."

boyd, d. m., and Ellison, N. B. 2007. "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* (13:1), pp. 210-230.

Brody, R. G., Brizzee, W. B., and Cano, L. 2012. "Flying under the Radar: Social Engineering," *International Journal of Accounting & Information Management* (20:4), pp. 335-347.

Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., and Hartel, P. 2017. "On the Anatomy of Social Engineering Attacks—a Literature-Based Dissection of Successful Attacks," *Journal of Investigative Psychology and Offender Profiling*), pp. 1-26.

Burch, G., Taylor, A., and Yeung, C. 2015. "Wire Transfer Email Fraud and What to Do About It," *Intellectual Property & Technology Law Journal* (27:1), pp. 13-15.

Cain, J. 2011. "Social Media in Health Care: The Case for Organizational Policy and Employee Education," *American Journal of Health-System Pharmacy* (68:11), pp. 1036-1040.

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. 2004. "Economics of Itsecurity Management: Four Improvements to Current Security Practices," *Communications of the Association for Information Systems* (14), pp. 65-75.

Charmaz, K. 1995. "Grounded Theory," in *Rethinking Methods in Psychology*, J.A. Smith, R. Harre and L. Van Langenhove (eds.). London, United Kingdom: Sage Publishing.

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

Constantiou, I. D., and Kalinikos, J. 2015. "New Games, New Rules: Big Data and the Changing Context of Strategy," *Journal of Information Technology* (30:1), pp. 44-57.

Conteh, N. Y., and Royer, M. D. 2016. "The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor," *International Journal of Computer* (20:1), pp. 1-12.

Corbin, J. M., and Strauss, A. 1990. "Grounded Theory Research: Procedures, Canons, and Evaluative Criteria," *Qualitative Sociology* (13:1), pp. 3-21.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32), pp. 90-101.

Davidson, R., Dey, A., and Smith, A. 2015. "Executives' "Off-the-Job" Behavior, Corporate Culture, and Financial Reporting Risk," *Journal of Financial Economics* (117:1), pp. 5-28.

Denzin, N. K., and Lincoln, Y. S. 1994. *Handbook of Qualitative Research*. Thousand Oaks: Sage Publications.

Dlamini, M. T., Eloff, J. H. P., and Eloff, M. M. 2009. "Information Security: The Moving Target," *Computers & Security* (28:3), pp. 189-198.

Federal Bureau of Investigation. 2017. "Business E-Mail Compromise; E-Mail Account Compromise; the 5 Billion Dollar Scam." from https://www.ic3.gov/media/2017/170504.aspx

Gardner, B., and Thomas, V. 2014. *Building an Information Security Awareness Program: Defending against Social Engineering and Technical Threats*. Elsevier.

Glaser, B. G., and Strauss, A. L. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. New Brunswick, New Jersey: AldineTransaction.

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., and Cowley, J. 2014. "Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits," *2014 IEEE Security and Privacy Workshops*, pp. 236-250.

Hambrick, D. C. 1981. "Strategic Awareness within Top Management Teams," *Strategic Management Journal* (2:3), pp. 263-279.

Hambrick, D. C., Finkelstein, S., and Mooney, A. C. 2005. "Executive Job Demands: New Insights for Explaining Strategis Decisions and Leader Behaviors," *Academy of Management Review* (30:3), pp. 472-491.

Hambrick, D. C., and Mason, P. A. 1984. "Upper Echelons: The Organization as a Reflection of Its Top Managers," *Academy of Management Review* (9:2), pp. 193-206.

He, W. 2012. "A Review of Social Media Security Risks and Mitigation Techniques," *Journal of Systems and Information Technology* (14:2), pp. 171-180.

Heartfield, R., and Loukas, G. 2015. "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks," *ACM Computing Survey* (48:3), pp. 1-39.

Honan, B. 2015. "Ubiquiti Networks Victim of $39 Million Social Engineering Attack." from http://www.csoonline.com/article/2961066/supply-chain-security/ubiquiti-networks-victim-of-39-million-social-engineering-attack.html

Hong, J. 2012. "The State of Phishing Attacks," *Communications of the ACM* (55:1), pp. 74-81.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., and Lowry, P. B. 2015. "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness," *Information Systems Research* (26:2), pp. 282-300.

Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.

Kemp, T. 2016. "Social Engineering Fraud: A Case Study," *Risk Management* (63:6), pp. 8-9.

Kim, H. J. 2012. "Online Social Media Networking and Assessing Its Security Risks," *International Journal of Security and Its Applications* (6:3), pp. 11-18.

Korolov, M. 2015. "Omaha's Scoular Co. Loses $17 Million after Spearphishing Attack." from http://www.csoonline.com/article/2884339/malware-cybercrime/omahas-scoular-co-loses-17-million-after-spearphishing-attack.html

Krasnova, H., Veltri, N. F., Eling, N., and Buxmann, P. 2017. "Why Men and Women Continue to Use Social Networking Sites: The Role of Gender Differences," *The Journal of Strategic Information Systems* (26:4), pp. 261-284.

Krombholz, K., Hobel, H., Huber, M., and Weippl, E. 2015. "Advanced Social Engineering Attacks," *Journal of Information Security and Applications* (22), pp. 113-122.

Laszka, A., Lou, J., and Vorobeychik, Y. 2015. "Multi-Defender Strategic Filtering against Spear-Phishing Attacks," *Twenty-Ninth AAAI Conference on Artificial Intelligence*, Austin, TX, pp. 537-543.

Lee, C. H., Geng, X., and Raghunathan, S. 2016. "Mandatory Standards and Organizational Information Security," *Information Systems Research* (27:1), pp. 70-86.

Liu, S., and Wang, L. 2016. "Influence of Managerial Control on Performance in Medical Information System Projects: The Moderating Role of Organizational Environment and Team Risks," *International Journal of Project Management* (34:1), pp. 102-116.

Lowry, P. B., and Moody, G. D. 2015. "Proposing the Control-Reactance Compliance Model (Crcm) to Explain Opposing Motivations to Comply with Organisational Information Security Policies," *Information Systems Journal* (25:5), pp. 433-463.

Lowry, P. B., Posey, C., Bennett, R. J., and Roberts, T. L. 2015. "Leveraging Fairness and Reactance Theories to Deter Reactive Computer Abuse Following Enhanced Organisational Information Security Policies: An Empirical Study of the Influence of Counterfactual Reasoning and Organisational Trust," *Information Systems Journal* (25:3), pp. 193-273.

Luo, X., Brody, R., Seazzu, A., and Burd, S. 2011. "Social Engineering: The Neglected Human Factor for Information Security Management," *Information Resources Management Journal* (24:3), pp. 1-8.

Molok, N. N. A., Chang, S., and Ahmad, A. 2013. "Disclosure of Organizational Information on Social Media: Perspectives from Security Managers," *Pacific Asia Conference on Information Systems*, Jeju Island, Korea, pp. 1-12.

Rivera, R. 2018. "Person Pretending to Be Ceo Steals Info from Charleston Co. Aviation Authority." from http://www.live5news.com/story/37681721/person-pretending-to-be-ceo-steals-info-from-charleston-co-aviation-authority

Rocha Flores, W., and Ekstedt, M. 2016. "Shaping Intention to Resist Social Engineering through Transformational Leadership, Information Security Culture and Awareness," *Computers & Security* (59), pp. 26-44.

Sánchez Abril, P., Levin, A., and Del Riego, A. 2012. "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee," *American Business Law Journal* (49:1), pp. 63-124.

Shahriar, H., Klintic, T., and Clincy, V. 2015. "Mobile Phishing Attacks and Mitigation Techniques," *Journal of Information Security* (6:3), pp. 206-212.

Sharp, A. 2017. "Fbi Warns of Surge in Wire-Transfer Fraud Via Spoofed Emails." from http://www.reuters.com/article/us-cyber-fraud-email-idUSKBN1811QH

Suddaby, R. 2006. "From the Editors: What Grounded Theory Is Not," *Academy of Management Journal* (49), pp. 633-642.

Symantec. 2015. "Internet Security Threat Report."

Teplinsky, M. J. 2013. "Fiddling on the Roof: Recent Developments in Cybersecurity," *American University Business Law Review* (2:2), pp. 225-322.

Torres, J. M., Sarriegi, J. M., Santos, J., and Serrano, N. 2006. "Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness," in: *2006 International Conference on on Information Security*. Samos Island, Greece: Springer Publishing, pp. 530-545.

Trustwave. 2017. "2017 Trustwave Global Security Report."

Uldam, J. 2016. "Corporate Management of Visibility and the Fantasy of the Post-Political: Social Media and Surveillance," *New Media & Society* (18:2), pp. 201-219.

Vaast, E., and Kaganer, E. 2013. "Social Media Affordances and Governance in the Workplace: An Examination of Organizational Policies," *Journal of Computer-Mediated Communication* (19:1), pp. 78-101.

Verizon Enterprises. 2016. "2016 Data Breach Investigations Report."

von Solms, R., and van Niekerk, J. 2013. "From Information Security to Cyber Security," *Computers & Security* (38), pp. 97-102.

Wakefield, R., and Wakefield, K. 2016. "Social Media Network Behavior: A Study of User Passion and Affect," *The Journal of Strategic Information Systems* (25:2), pp. 140-156.

Wang, T., Kannan, K. N., and Ulmer, J. R. 2013. "The Association between the Disclosure and the Realization of Information Security Risk Factors," *Information Systems Research* (24:2), pp. 201-218.

Wilcox, H., Bhattacharya, M., and Islam, R. 2014. "Social Engineering through Social Media: An Investigation on Enterprise Security," *International Conference on Applications and Techniques in Information Security,* L. Batten, G. Li, W. Niu and M. Warren (eds.), Melbourne, Australia: Springer, pp. 243-255.