Association for Information Systems

AIS Electronic Library (AISeL)

AMCIS 2020 Proceedings

Meta-Research in Information Systems

Aug 10th, 12:00 AM

Themes in Information Security Research in the Information Systems Discipline: A Topic Modeling Approach

Stephanie Totty
University of Memphis, satotty@memphis.edu

He Li
Clemson University, hli10@memphis.edu

Brian Janz
University of Memphis, bdjanz@memphis.edu

Chen Zhang
University of Memphis, czhang12@memphis.edu

Totty, Stephanie; Li, He; Janz, Brian; and Zhang, Chen, "Themes in Information Security Research in the Information Systems Discipline: A Topic Modeling Approach" (2020). *AMCIS 2020 Proceedings*. 7.
https://aisel.aisnet.org/amcis2020/meta_research_is/meta_research_is/7

Themes in Information Security Research in the Information Systems Discipline: A Topic Modeling Approach

Completed Research

Stephanie Totty
University of Memphis
satotty@memphis.edu

He Li
Clemson University
hl3@clemson.edu

Brian Janz
University of Memphis
bdjanz@memphis.edu

Chen Zhang
University of Memphis
czhang12@memphis.edu

Abstract

Information security continues to grow in importance in all aspects of society, and therefore evolves as a prevalent research area. The Information Systems (IS) discipline offers a unique perspective from which to move this stream of literature forward. Using a semi-automated thematic analysis approach based on the topic modeling technique, we review a broad range of information security literature to investigate how we might theorize about information security on a grander scale. Five themes resulted from our analysis: Software Security Decisions, Firm Security Strategy, Susceptibility, Information Security Policy Compliance, and Other Developing Themes. Implications of our findings and future research directions are discussed.

Keywords

information security, literature review, topic modeling, thematic analysis.

Introduction

Organizations are undergoing digital transformation by increasingly adopting and infusing information technologies into their business processes, triggering the unintended consequence of information security concerns (Kappelman et al. 2019; Luftman et al. 2015). Information security refers to the "confidentiality, integrity and accessibility of digital information assets (data, information, knowledge, documents) and relevant IT assets (hardware, software, networks)" (McLaughlin and Gogan 2018, p. 239). Notably, non-digital information is excluded from the definition because Information Systems (IS) researchers often focus on information secured by IT artifacts. Information security incidents have a high price tag for organizations—e.g., the average cost of a data breach could be as high as $3.86 million, according to the Ponemon Institute (2018). Security incidents also negatively influence organizations' market value (Goldstein et al. 2011), cause business discontinuity, and hurt organizational reputation. Hence, information security has garnered great interest from researchers, practitioners, and policy makers.

The IS discipline, emphasizing IT artifacts, has unique advantages in advancing our understanding of information security and has contributed in this research area since the early 1990s. Over the past 30 years, IS research on information security has evolved from early-stage, practical research focusing on the individual level to more theory-driven research, also addressing organizational-level phenomena. Contextually, prior information security research has not only expanded our understanding in various settings such as individual use of personal computers (e.g., Liang and Xue 2010) and organizations in different industry sectors (e.g., Sen and Borle 2015) but also started to use the contextualization approach and offered context-sensitive theories (e.g., Aurigemma and Mattson 2019). In addition, existing information security research is gradually paying attention to the time dimension in theory building and accordingly is helping to explain how the effectiveness of information security management changes over time (e.g., Angst et al. 2017). Prior studies have also adopted a diverse range of methodologies such as field surveys, experiments, econometrics, qualitative research, and Review and Theory Development (RTD).

Despite the aforementioned aspects, we believe that a comprehensive review examining different streams of information security literature can help provide a holistic view of the phenomenon and foresee a sustainable trajectory of future research advancing our knowledge. The objective of this paper is to build upon prior information security research in the IS field to (1) clarify major research themes and their inter-connections, (2) assess the current status of the literature, and (3) envision breakthrough directions for future research. We identify themes and trends by developing a semi-automated approach leveraging the advantages of both topic modeling and content analysis techniques.

Although this is not the first RTD effort concerning information security, this review is different in important ways in terms of the scope and analytical approaches. First, most previous reviews focus on a specific set of information security problems. For example, Cram et al. (2019) and Cram et al. (2017) focused on information security policies, a sub-stream of information security research. In a similar vein, Backhouse and Dhillon (1996) and Siponen (2005) examined security approaches taken by practitioners. Other reviews mapped articles to the philosophical research paradigms employed (e.g., Dhillon and Backhouse 2001) or derived practical guidelines through mapping research to existing frameworks. For example, McLaughlin and Gogan (2018) mapped articles to a framework based on ISO/IEC 27035. In addition, unlike prior information security reviews, we analyze linkages between previously segmented sub-streams, which generates insights into future research. Furthermore, quite different from prior research using thematic analysis (e.g., McIntyre and Srinivasan 2017), the newly-proposed approach provides a more objective, scientific way of determining the themes (Debortoli et al. 2016; Yu et al. 2011). This approach has the potential to overcome some critical disadvantages of content analysis or self-categorization. We also have detailed stepwise recommendations of thematic analysis using our proposed semi-automated approach.

Methodology

Literature Search

We conducted a keyword search using "security" on the article's title, abstract, author keywords, and Web of Science's Keywords Plus® using Web of Science. This keyword is similar to McLaughlin and Gogan's (2018) keyword. Like them, we believe our approach revealed most information security studies in the journals searched. We restrict the journal samples to Association of Information Systems (AIS) Senior Scholar's Basket of Eight because our objective is to analyze how the IS community has contributed to information security research and "major contributions are likely to be in the leading journals" (Webster and Watson 2002, p. xvi). The Basket of Eight journals are internationally recognized as top tier IS publication outlets. Our initial search resulted in 305 references. References without abstracts were editorials, introductions to special sections and a book review, so we excluded those observations, leaving 298 references.

A Semi-Automated Thematic Analysis Approach Using Topic Modeling

To derive an automatic categorization of the literature, we perform topic modeling on the abstracts. The topic modeling approach uses terms and the distances among them as criteria to cluster articles into a smaller number of groups, which could be a useful source for further categorization. In line with prior literature (e.g., Mortenson and Vidgen 2016), we chose to mine the abstracts because article titles and author-provided keywords often are limited to a low, specified number of characters or words and full papers would add a great deal of noise to the data.

We used text parsing to break the text into tokens, remove punctuation, reduce the words to their stems/roots, categorize the terms into parts of speech, and remove "stop words" like articles and prepositions. We ignored all parts of speech except for nouns. We enabled spell checking to reduce this potential source of noise. Finally, the text topics emerged from the terms collected by the text parsing and text filter steps. Different topics are created from different combinations of terms. This was accomplished through Singular Value Decomposition (SVD) which is essentially a grouping function that creates smaller and denser data matrices from large sparse data matrices by replacing terms with concepts or topics. Given that it is unlikely that these topics are orthogonal, we allowed the possibility of correlated topics.

Although topic modeling can automatically categorize articles based on keywords, the number of topics identified leaves a key decision for researchers (Mortenson and Vidgen 2016). There is no single straightforward way to determine the "best" number of topics using mathematical analysis (Mortenson and Vidgen 2016). To overcome this issue, we ran analyses specifying the algorithm to create three to ten topics, respectively because an RTD paper rarely determines less than three or more than ten themes.

Two authors of this paper then independently read the results from using a different number of topics. The authors discussed which result was best based on the criteria of how the terms in each topic are different from those in other topics. We agreed that eight topics was the best result for our next step of the analysis, which transforms topics to themes. Table 1 presents the eight topics along with the top five terms in each.

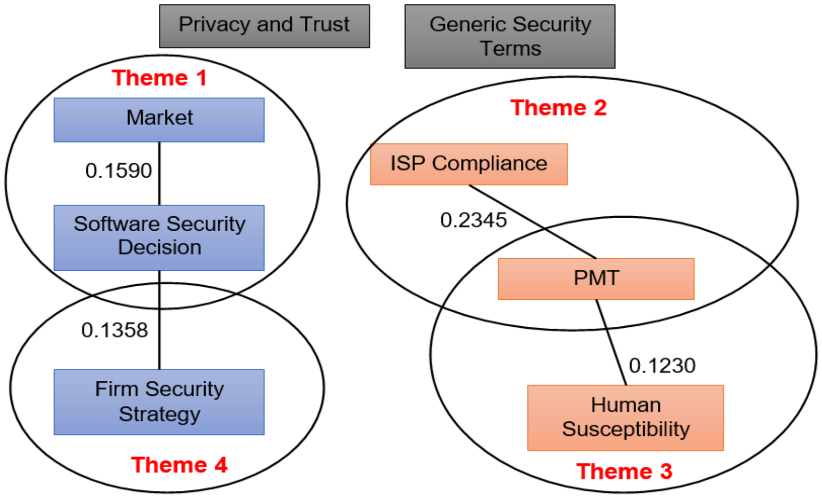
Topic	**Top 5 Defining Terms**
Information Systems Policy Compliance	compliance, employee, ISP, policy, noncompliance
Software Security Decisions	software, vendor, software vendor, vulnerability, network
Protection Motivation Theory	behavior, threat, user, fear, PMT
Firm Security Strategy	investment, firm, risk, security investment, breach
Human Susceptibility	detection, user, deception, website, warning
Market	market, exchange, service, contract, transaction
Privacy and Trust	privacy, consumer, trust, data, service
Generic Security	ISS, process, system, organization, business

Table 1. Topics Emerging from Text Mining

While eight topics produced the best result, some results did not fit the scope of this review based on our definition of information security. For example, although privacy and trust are related to information security, they are very different and not within our scope. In addition, there is room to further maximize the categorization by merging some topics. For instance, prior information security literature has conducted extensive work using Protection Motivation Theory (PMT) to tackle security issues—primarily individuals' secure behavior or Information Security Policy (ISP) compliance—thereby creating opportunities to divide this group of literature into other related topics. Furthermore, some contextual terms related to the domain of our review are likely to be categorized into separate topics. In our case, the terms listed in the topic of General Security are very generic and often used in almost all information security articles, which could be categorized into other topics based on the focus of the studies. Last, because the area is evolving, there will be some contemporary research topics appearing over time. However, these developing studies with new contexts or research foci are not using common keywords with previous well-defined groups of studies. Solely depending on the topic modeling approach may overlook these developing themes.

In this research, we propose a useful technique to assist us with further coding the themes. In the topic modeling analysis, a matrix of probabilities of each article being categorized into each topic is produced. We performed a correlation analysis on this probability matrix. We argue that if two themes have high positive correlations, they are more likely to share similar attributes and could be further abstracted as one theme. In contrast, with high but negative correlations, articles categorized into one topic will not be categorized into the other one, suggesting the distinct nature of these topics.

Figure 1 depicts our analytical process of abstracting topics into themes based on the correlation matrix. In this visualization, we use lines to connect topics that have positive and statistically significant (at $p < 0.05$ level) correlation. Negative statistically significant relationships are not displayed. We found that Privacy and Trust and Generic Security Terms are not significantly correlated with any other topic, confirming our initial analysis. Hence, we drop these two topics. In addition, Software Security Decisions and Firm Security Strategy topics have positive significant correlation. However, because they focus on different aspects, i.e., software vendor versus firm strategy, we keep these two topics but know that these two topics will have greater intersections. Market and Software Security Decisions are also positively correlated. Examining the keywords in these two topics, we notice that some articles in the Market topic may be associated with financial securities and some articles are related to software security market competition. We thus merge the related software security market competition to the Software Security Decision category and drop financial securities literature from the sample. Furthermore, PMT is positively associated with both the ISP Compliance and Human Susceptibility topics, but the correlation between ISP Compliance and Human Susceptibility is negative and significant. This demonstrates that ISP Compliance and Human Susceptibility are two separate themes, and PMT articles can be merged with either ISP Compliance or Human Susceptibility depending on the context of the study. As shown in Figure 1, we have four remaining themes.



Note: Lines connecting boxes demonstrate positive and significant correlations. The numbers depicted on the lines are the positive correlations.

Figure 1. Methodology of Deriving Themes

Based on the defined themes, we remove unrelated articles and re-categorize articles in the removed topics based on the matrix of binary categorization of articles into topics. Note that one article may be assigned to multiple topics. Table 2 describes the process in detail.

Step	**Articles Remaining**
1. Remove articles that are only assigned in Privacy and Trust topic	270
2. Remove articles that are only assigned in Market topic because they are more likely to focus on financial securities	249
3. For articles that are only assigned in Generic Security Terms topic, 3.1 if the maximum probability is below 0.1, remove	222
3.2 if the maximum probability is greater than 0.1, assign them into the topic that has highest probability (5 papers were assigned to Firm Security Strategy, 8 papers were assigned to ISP Compliance, and 1 paper was assigned to Software Security Decisions)	222
4. For articles that are not assigned in PMT topic, assign them into the topic that has highest probability (3 papers were assigned to Firm Security Strategy, 9 papers were assigned to ISP Compliance, 11 articles were assigned to Human Susceptibility, and 1 paper was assigned to Software Security Decisions)	222
5. For articles that are not in any four of the remaining topics, manually examine the title and abstracts. Identify relevant papers (4) and remove others.	176

Table 2. Article Re-Categorization Process

After recategorization, we have a list of revised themes and articles in each theme. Figure 2 shows the finalized themes along with the number of articles in each theme. We see that some articles are categorized into more than one theme. We also include a new theme labeled Other Developing Themes. In this theme, we observe that some more recent studies (from Table 2, Step 5) start to look at the societal impacts of information security as well as the behaviors of online hacker communities.

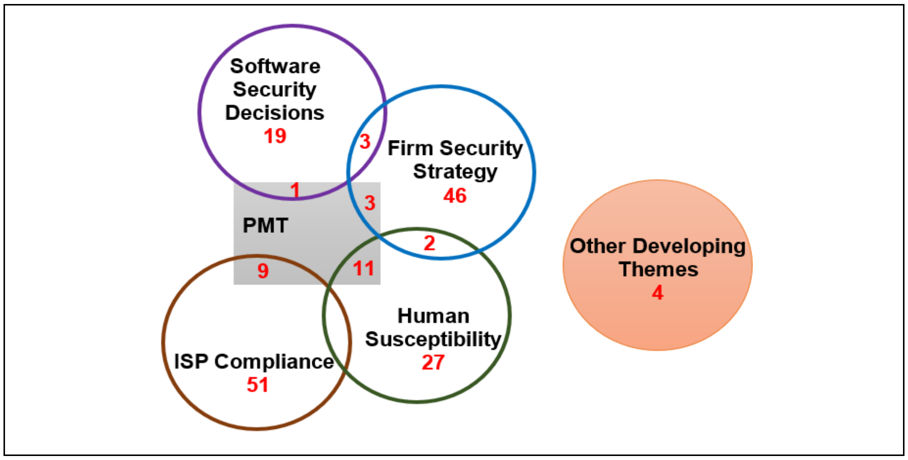


Figure 2. Themes of Information Security Research

Themes in Information Security Research

ISP Compliance

The emergence of ISP Compliance as a topic is not surprising given that researchers have also recognized and conducted reviews to synthesize this stream of research (e.g., Cram et al. 2019; Cram et al. 2017). ISP compliance research tends to be behavior oriented, focusing on the antecedents and consequences of ISP compliance and moderators of those relationships. This theme of literature has adopted multiple theoretical lenses, including PMT and deterrence theory. Research on fear appeals in the ISP compliance behavior context also fall in this theme. Perceived threat in PMT is considered a fear appeal, which has shown a significant impact on an individual's intention to adhere to recommended secure behavior and is influenced to varying degrees by several factors (Johnston and Warkentin 2010). Security Education, Training, and Awareness (SETA) is a strategy used to motivate individuals to perform secure behaviors. SETA has been found to influence many PMT-based components (Posey et al. 2015).

Software Security Decisions

Software Security Decisions encompass several types of decisions related to keeping software secure. First, software vulnerabilities are investigated in this theme. Hackers attempt to exploit vulnerabilities, and different types of attacks have been modeled, along with their resulting network effects (Dey et al. 2012). Software diversification, where software code is altered to limit a hacker's ability to exploit a system's vulnerabilities, has been shown to be effective at mitigating the risk of network failure under certain conditions (Chen et al. 2011). Second, firms' patch releases are a response to software vulnerabilities. Factors affecting patch release behavior include the type and extent of the impact, software type, legislative pressures (Temizkan et al. 2012), vulnerability disclosures, and vendor type (open or closed source) (Arora et al. 2010). Patch decisions also include whether to support unlicensed users (August and Tunca 2008) and whether to stop support of older software (Ghoshal et al. 2017). Third, research investigates contextual factors that affect software security decisions. Models indicate whether and how SaaS versions should be offered by vendors (August et al. 2014). SaaS products have been treated as a contextual difference to its on-premise software counterparts (Choudhary and Zhang 2015).

Firm Security Strategy

The Firm Security Strategy theme includes information security investment and other prevention against information security incidents, e.g., security breaches.

Information security investments are an important area for businesses because departments are always vying for a larger portion of the organization's budget. Much research has studied the optimal security investment (e.g., Herath and Herath 2008) and conditions under which information security investment is more effective at preventing incidents. For example, proactive security investments have been found to be more effective at preventing security incidents than reactive investments (Kwon and Johnson 2014).

The availability of security breach data following the implementation of U.S. national and state laws around 2005 is one of the reasons research in this area has exploded. Further, the rise in information security breaches and the resulting tangible and intangible damages provide motivation for studying the antecedents and outcomes of security breaches. Regarding antecedents, prior research has investigated the external and internal factors that impact firms' security performance and risk of an information security breach. Externally, state security breach disclosure laws significantly influence the risk of a data breach in financial, educational, and medical industries (Sen and Borle 2015). Internally, while some studies found a correlation between IT security investment and risk of a data breach (e.g., Sen and Borle 2015), several studies emphasize that deeper integration of security practices into IT-related processes beyond mere security investments in organizations helps reduce breaches (e.g., Angst et al. 2017; Kwon and Johnson 2013). Furthermore, how firms disclose security risk factors to external stakeholders may impact future security breaches. More specifically, firms disclosing risk-mitigating information in their annual reports are less likely to encounter security incidents in the future (Wang et al. 2013).

Additionally, decisions regarding the deployment of security technologies by the firm fall into this theme. For example, the configuration of an intrusion detection system (IDS) determines whether the firm realizes value from the IDS (Cavusoglu et al. 2005). Further, findings suggest that an IDS and firewall must be configured properly to avoid a negative impact on the firm (Cavusoglu et al. 2009).

Human Susceptibility

The Human Susceptibility theme that emerged from topic modeling includes several aspects of human behavior that make humans the target of security attacks. This includes theories and studies investigating why humans are susceptible as well as studies that outlined solutions to minimize this susceptibility, often in the form of design science articles.

Hackers rely on people's lack of ability to detect deception. Several conditions have been found to increase a person's susceptibility. Fear or anticipation of losing something valuable has been shown to increase a person's susceptibility to phishing (Goel et al. 2017). PMT proposes that perceived threat and coping response influence behavioral intention and actual behavior. Several articles in this theme made use of PMT to explain motivations (Boss et al. 2015). For example, the technology threat avoidance theory extends PMT to the information security context (Liang and Xue 2009).

Using rhetoric to describe informal sanction severity and certainty is one strategy that has been found to enhance the effectiveness of fear appeals (Johnston et al. 2015). However, other research has shown that focusing on the responses to threats is a better strategy than focusing on the threat (Warkentin et al. 2016). In addition, when people rely more on software tools, they are more likely to be deceived by fake websites (Zahedi et al. 2015). Finally, several papers offer design approaches as potential solutions to help people detect phishing web sites (e.g., Abbasi et al. 2015; Abbasi et al. 2010).

Other behaviors that make people susceptible include habitually reacting (e.g., automatically responding instead of reading and comprehending) to security warnings (Vance et al. 2018). For example, a polymorphic design—a regularly updated appearance—for security warnings has shown success in reducing the impact of habituation on reactions to security warnings (Anderson et al. 2016).

Current Limitations and Future Research Guidelines

We analyze each theme of information security research and the correlations between different themes to offer recommendations for future research.

First, among the four major themes, we observe that the ISP Compliance and Human Susceptibility themes focus on the individual level while Software Security Decisions and Firm Security Strategy studies are often conducted at the organizational level. The correlations of papers categorized in these two major camps are negative and statistically significant. We suggest that future research may consider undertaking multi-level studies to incorporate insights from both sides of these IS security research perspectives (Rousseau 2011; Rousseau et al. 2008). Because security research has clear effects on multiple levels of the organization and because decisions made at one level effect other levels, it is important to combine these perspectives. For example, organizational-level strategic emphasis of firm IT security management can utilize individual-level behavioral wisdom as a theoretical foundation. In addition, we would recommend an alignment between an organization's business, the IT organization, and the IS security department to tackle information security problems better. Alignment will help because these problems tend to involve the strategic fit of business, IT, and information security, and it will do so on multiple dimensions including people, technology, and process.

Second, our thematic analysis renders some interesting observations: 1) Several studies have utilized PMT as a theoretical lens, especially the individual-level information security behavior research; 2) Most software security decision studies rely on decision theory or game-theoretic models (which are based on strong assumptions of rationality); and 3) Firm security strategy studies primarily adopt organizational IT strategy theoretical lenses such as institutional theory, resource-based view, and organizational learning theory. Overall, there is a lack of coherent theory building that is specific to information security, less a few exceptions, (e.g., Liang and Xue 2009). Given that information security has its own unique attributes such as high uncertainty and value at risk, we suggest that in the future researchers consider developing information security-specific theories to advance our theoretical understanding of the phenomenon. Contextualization or grounded theory approaches could prove to be promising. Future studies may also consider adopting the metaphors of insurance or gambling and use storytelling approaches to generate fresh insights and theoretical perspectives.

Third, the methodologies used in prior individual-level security behavioral studies are primarily survey-based with cross-sectional data. Longitudinal analysis is not commonly performed to produce more insightful and robust results. Software Security Decisions literature focuses on developing customized game-theoretical models, which is based on strong assumptions of firms' and decision makers' rationality. Firm security strategy studies have conducted longitudinal, secondary data analyses, but heavily relied on the reported data breaches. However, not all security breaches are reported, and this measure omits many details such as the security attack attempts. Mix-method studies are rare in the information security research, and we encourage researchers to consider these methods in future research.

Fourth, the time dimension—an important construct to theory building—has not, to this point, adequately been considered. This might be because most studies have utilized cross-sectional survey data. We suggest future research consider incorporating the time dimension in information security theory building. The time dimension could be central to theory building as "the present needs to be understood in the context of the past; but the past is not fixed but may be recast as new narratives emerge over time; and these narratives cast a long shadow into the future" (Cram 2011, pp. 637-638). As information systems researchers, we "could benefit from more explicitly considering measure of time" in our research (Saunders and Kim 2007, p. iv).

Finally, as demonstrated in the thematic analysis, we observe two promising and emerging research opportunities. The first is to understand hacker communities and how hackers behave, which could offer great theoretical foundations for information security research as hackers and firms are co-evolving in the security space. The second is the broader societal impacts of information security. As digitalization and information security garner greater interest from both academics and practitioners, we need to think about the positive and negative consequences of frequently reported data breaches and other types of security failures and concerns. A better understanding of how information security introduces new societal problems or how our growing attention to information security issues contributes to the mitigation of certain societal challenges would produce great contributions.

While our review offers valuable insight, our study has limitations.[1] First, we limited our journals to the AIS Basket of Eight. While we are likely to see the major contributions using this constraint, surveying a broader body of literature would allow us to have a more complete sense of the current literature. Further, adding additional sources, like conference proceedings, may allow us to better identify up and coming research areas that have not made it to publication in top journals, yet. Second, additional articles may have been

[1] We thank an anonymous reviewer for the suggestion.

included when using more or different keywords. While we carefully selected our search term, it is possible that some security articles were excluded because of our choice.

Discussion and Conclusion

This paper provides a review of information security research in top IS journals and attempts to provide a more integrated appreciation of the research through the development and application of an innovative, semi-automated text-mining approach. Equipped with this approach, we examine articles from top IS journals and determine the themes emerging from the literature. We analyze and discuss the themes that emerged and accordingly proposed suggestions for future research.

The major contributions are two-fold. First, unlike previous review articles, we do not limit our focus to specific aspects of security research (e.g., information security policy compliance or PMT) or take on a specific perspective (e.g., practitioners). As such, this allows us to thoughtfully consider all of the security literature to expand our perspective and take steps toward integrating the disparate security-related research streams.

Furthermore, this is one of the first literature reviews to make use of text mining to analyze previous literature. This novel approach to literature review provides some additional objectivity to the review by allowing themes to emerge from the data instead of imposing themes on the data. While some of the topics that emerged in our analysis align with themes of or within prior reviews (i.e., ISP compliance), other topics emerged that have not emerged in previous literature reviews (i.e., software security decisions, firm security strategy, human susceptibility). While there are advantages to adding more objectivity using this approach, there are also limitations. For example, topic modeling using SVD is limited in that there is no objective way to determine the optimal number of topics. Our suggested semi-automated approach based on topic modeling results, probability matrix, correlation analysis, and content analysis offers a methodological contribution to the thematic analysis and RTD methods. This semi-automated approach provides qualitative and RTD researchers a promising way to save time and produce more reliable results.

REFERENCES

Abbasi, A., Zahedi, F., Zeng, D., Chen, Y., Chen, H. C., and Nunamaker, J. F. 2015. "Enhancing Predictive Analytics for Anti-Phishing by Exploiting Website Genre Information," Journal of Management Information Systems (31:4), pp. 109-157.

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., and Nunamaker, J. F. 2010. "Detecting Fake Websites: The Contribution of Statistical Learning Theory," MIS Quarterly (34:3), pp. 435-461.

Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., and Jenkins, J. L. 2016. "How Users Perceive and Respond to Security Messages: A NeuroIS Research Agenda and Empirical Study," European Journal of Information Systems (25:4), pp. 364-390.

Angst, C. M., Block, E. S., D'Arcy, J., and Kelley, K. 2017. "When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches," MIS Quarterly (41:3), pp. 893-916.

Arora, A., Krishnan, R., Telang, R., and Yang, Y. B. 2010. "An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure," Information Systems Research (21:1), pp. 115-132.

August, T., Niculescu, M. F., and Shin, H. 2014. "Cloud Implications on Software Network Structure and Security Risks," Information Systems Research (25:3), pp. 489-510.

August, T., and Tunca, T. I. 2008. "Let the Pirates Patch? An Economic Analysis of Software Security Patch Restrictions," Information Systems Research (19:1), pp. 48-70.

Aurigemma, S., and Mattson, T. 2019. "Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research," Journal of the Association for Information Systems (20:12), pp. 1700-1742.

Backhouse, J., and Dhillon, G. 1996. "Structures of Responsibility and Security of Information Systems," European Journal of Information Systems (5:1), pp. 2-9.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," MIS Quarterly (39:4), pp. 837-864.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2005. "The Value of Intrusion Detection Systems in Information Technology Security Architecture," Information Systems Research (16:1), pp. 28-46.

Cavusoglu, H., Raghunathan, S., and Cavusoglu, H. 2009. "Configuration of and Interaction between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems," Information Systems Research (20:2), pp. 198-217.

Chen, P. Y., Kataria, G., and Krishnan, R. 2011. "Correlated Failures, Diversification, and Information Security Risk Management," MIS Quarterly (35:2), pp. 397-422.

Choudhary, V., and Zhang, Z. 2015. "Patching the Cloud: The Impact of SaaS on Patching Strategy and the Timing of Software Release," Information Systems Research (26:4), pp. 845-858.

Cram, L. 2011. "The Importance of the Temporal Dimension: New Modes of Governance as a Tool of Government," Journal of European Public Policy (18:5), pp. 636-653.

Cram, W. A., D'Arcy, J., and Proudfoot, J. G. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance," MIS Quarterly (43:2), pp. 525-554.

Cram, W. A., Proudfoot, J. G., and D'Arcy, J. 2017. "Organizational Information Security Policies: A Review and Research Framework," European Journal of Information Systems (26:6), pp. 605-641.

Debortoli, S., Müller, O., Junglas, I., and vom Brocke, J. 2016. "Text Mining for Information Systems Researchers: An Annotated Topic Modeling Tutorial," Communications of the Association for Information Systems (39:1), p. 7.

Dey, D., Lahiri, A., and Zhang, G. Y. 2012. "Hacker Behavior, Network Effects, and the Security Software Market," Journal of Management Information Systems (29:2), pp. 77-108.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives," Information Systems Journal (11:2), pp. 127-153.

Ghoshal, A., Lahiri, A., and Dey, D. 2017. "Drawing a Line in the Sand: Commitment Problem in Ending Software Support," MIS Quarterly (41:4), pp. 1227-1247.

Goel, S., Williams, K., and Dincelli, E. 2017. "Got Phished? Internet Security and Human Vulnerability," Journal of the Association for Information Systems (18:1), pp. 22-44.

Goldstein, J., Chernobai, A., and Benaroch, M. 2011. "An Event Study Analysis of the Economic Impact of IT Operational Risk and Its Subcategories," Journal of the Association for Information Systems (12:9), pp. 606-631.

Herath, H. S. B., and Herath, T. C. 2008. "Investments in Information Security: A Real Options Perspective with Bayesian Postaudit," Journal of Management Information Systems (25:3), pp. 337-375.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," MIS Quarterly (34:3), pp. 549-566.

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.

Kappelman, L., Torres, R., McLean, E., Maurer, C., Johnson, V., and Kim, K. 2019. "The 2018 SIM IT Issues and Trends Study," MIS Quarterly Executive (18:1), pp. 51-84.

Kwon, J., and Johnson, M. E. 2013. "Health-Care Security Strategies for Data Protection and Regulatory Compliance," Journal of Management Information Systems (30:2), pp. 41-66.

Kwon, J., and Johnson, M. E. 2014. "Proactive Versus Reactive Security Investments in the Healthcare Sector," MIS Quarterly (38:2), pp. 451-472.

Liang, H. G., and Xue, Y. J. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," MIS Quarterly (33:1), pp. 71-90.

Liang, H. G., and Xue, Y. J. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," Journal of the Association for Information Systems (11:7), pp. 394-413.

Luftman, J., Derksen, B., Dwivedi, R., Santana, M., Zadeh, H. S., and Rigoni, E. 2015. "Influential IT Management Trends: An International Study," Journal of Information Technology (30:3), pp. 293-305.

McIntyre, D. P., and Srinivasan, A. 2017. "Networks, Platforms, and Strategy: Emerging Views and Next Steps," Strategic Management Journal (38:1), pp. 141-160.

McLaughlin, M.-D., and Gogan, J. 2018. "Challenges and Best Practices in Information Security Management," MIS Quarterly Executive (17:3), pp. 237-262.

Mortenson, M. J., and Vidgen, R. 2016. "A Computational Literature Review of the Technology Acceptance Model," International Journal of Information Management (36:6, Part B), pp. 1248-1259.

Ponemon Institute. 2018. "Ponemon Institute's 2018 Cost of a Data Breach Study: Global Overview." from https://www.ibm.com/security/data-breach

Posey, C., Roberts, T. L., and Lowry, P. B. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," Journal of Management Information Systems (32:4), pp. 179-214.

Rousseau, D. M. 2011. "Reinforcing the Micro/Macro Bridge: Organizational Thinking and Pluralistic Vehicles," Journal of Management (37:2), pp. 429-442.

Rousseau, D. M., Manning, J., and Denyer, D. 2008. "Evidence in Management and Organizational Science: Assembling the Field's Full Weight of Scientific Knowledge through Syntheses," Academy of Management Annals (2:1), pp. 475-515.

Saunders, C., and Kim, J. 2007. "Editor's Comments: Perspectives on Time," MIS Quarterly (31:4), pp. iii-xi.

Sen, R., and Borle, S. 2015. "Estimating the Contextual Risk of Data Breach: An Empirical Approach," Journal of Management Information Systems (32:2), pp. 314-341.

Siponen, M. T. 2005. "An Analysis of the Traditional Is Security Approaches: Implications for Research and Practice," European Journal of Information Systems (14:3), pp. 303-315.

Temizkan, O., Kumar, R. L., Park, S., and Subramaniam, C. 2012. "Patch Release Behaviors of Software Vendors in Response to Vulnerabilities: An Empirical Analysis," Journal of Management Information Systems (28:4), pp. 305-337.

Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., and Kirwan, C. B. 2018. "Tuning out Security Warnings: A Longitudinal Examination of Habituation through fMRI, Eye Tracking, and Field Experiments," MIS Quarterly (42:2), pp. 355-380.

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.

Warkentin, M., Walden, E., Johnston, A. C., and Straub, D. W. 2016. "Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination," Journal of the Association for Information Systems (17:3), pp. 194-215.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," MIS Quarterly (26:2), pp. xiii-xxiii.

Yu, C. H., Jannasch-Pennell, A., and DiGangi, S. 2011. "Compatibility between Text Mining and Qualitative Research in the Perspectives of Grounded Theory, Content Analysis, and Reliability," Qualitative Report (16:3), pp. 730-744.

Zahedi, F. M., Abbasi, A., and Chen, Y. 2015. "Fake-Website Detection Tools: Identifying Elements That Promote Individuals' Use and Enhance Their Performance," Journal of the Association for Information Systems (16:6), pp. 448-484.