ICEBESS 2021
International Conference of Ethics on Business, Economics, and Social Science

in conjunction with
2021 ACOMC
Annual Conference of Management Challenges

GLOBAL JOURNAL OF ADVANCED RESEARCH
(Scholarly Peer Review Publishing System)
ISSN: 2394-5788

DO RESEARCHERS ANSWER THE INDUSTRY'S NEEDS? A REVIEW OF INFORMATION SECURITY FRAUD STUDIES

Afrida Putritama
Universitas Negeri Yogyakarta,
Sleman, DI Yogyakarta
Indonesia
aputritama@uny.ac.id

Diana Rahmawati
Universitas Negeri Yogyakarta,
Sleman, DI Yogyakarta
Indonesia
rahmawati_diana@uny.ac.id

Ratna Yudhiyati
Universitas Negeri Yogyakarta,
Sleman, DI Yogyakarta
Indonesia
ratna.yudhiyati@uny.ac.id

ABSTRACT

The rising chance for fraud in the digital environment encourages researchers to study information systen security. The growing number of studies discussing fraud in the digital environment and information system threat inspire the need for studies that integrate various study results in the form of a literature review.

Previous literature reviews have not provided a summary or analysis of what information technology fraud that attracted academics' attention the most. In addition, previous literature reviews have not specifically summarized security measures to prevent and detect information technology crimes suggested by previous studies. This study aims to identify the topics raised by previous research on information technology fraud with a focus on two main issues, namely various fraud techniques found in the digital environment and security measures to overcome fraud in the digital environment. This study also identified and explained research gap related to these two topics.

This study found that the most commonly discussed technique of information system fraud in scientific articles is data security threat, which was then followed by brute force attacks, while deceptive activity was the least discussed topic. The security measure to overcome digital environmental fraud that is most discussed by previous research is preventive measures, which are then followed by detection and response.

Keywords: Fraud, information system risks, threat, security measures, cybercrime, literature review

1. INTRODUCTION

Currently, information technology has become an integral part of the success of a business. Businesses that want to win against competitors should utilize information technology as demanded by their respective industry. However, the use of information technology can create new risks for businesses that adopt it. These businesses may situations or threats that they have never experienced before they adopted information technology. Each business may face different situation and IT-adoption challenges based on their respective situations [1].

The increasing use of information technology and how businesses integrate it to their existing operations allow certain parties to steal resources or information by exploiting the digital environment. This act is referred to as information technology fraud, or often also called cybercrime, cyberthreat, and other similar terms.

Fraud in the digital environment is a threat that grows along with the widespread use of information technology by businesses. In 2015, theft of personal data via the internet reached 191 million data, which is the highest number of data thefts ever recorded [2]. The theft of payment card data that utilize formjacking grows in 2018 where Symantec recorded 3.7 million formjacking attempts [3]. Formjacking is a technique that use malicious JavaScript code injected in web pages or eCommerce sites to steal credit card data or other payment information. The growth of eCommerce will provide greater number of targets for these cyber criminals in the years to come.

The increasing number of information technology threat encourages researchers to conduct study related to system and information technology security. There are studies that focuses on identifying the various types and modes of fraud in the digital environment and how to overcome them [4]. Other studies discussed the factors that increase a business' probability in becoming a victim of fraud in the digital environment, while some studies assessed business' readiness and capability in fighting against information technology fraud [5], [6]. There are other studies that focuses on fraud prevention, detection, and investigation [7], [8]. The increasing number of studies and topics related to fraud in the digital environment encourage the need for studies that integrate various research results and previous studies. One way that can be done to integrate the results of research and previous studies is a literature review.

The literature review method has been applied several times to the topic of systems and information technology [9], [10]. These studies classified and analyzed previous information and technology research and studies from the point of view of the information systems framework. They provide information that most of the research in the field of information technology security focuses on governance, human resources, and data confidentiality.

However, previous literature reviews have not provided a summary or specific analysis of what types of information technology fraud that's has attracted the attention of academics so far. Identifying and classifying fraud techniques which has been the focus of previous research is useful to determine whether academics accommodate the needs of the industry and address real-world situation or not. The survey results found the fraud techniques used by cyber criminals often changed significantly as years passed [2], [3]. A literature review of IT fraud studies allows us to assess whether the trends of certain research topics follow rising popularity of IT fraud techniques used by cyber criminals. Thus, researchers and industry practitioners can identify and address existing gaps between literature and industry needs regarding IT fraud studies.

In addition, previous literature reviews have not specifically summarized IT fraud preventive and detective methods that have been suggested by previous studies. To date, research in the field of information security has not succeeded in agreeing on the best prevention and detection measures in dealing with fraud in the digital environment. Each study states that the solutions they offer tend to be relevant only to the groups that make up their research population. A literature review that focuses on grouping prevention and detection measures can identify research gaps and explain why it is difficult for researchers to be able to formulate prevention and detection measures that are relevant for all groups.

This study reviews previous studies on IT fraud by focusing on two main issues, namely various techniques of fraud in the digital environment and steps to prevent or detect these techniques. This study also explains research gap related to these two topics that may help future researchers to identify potential future research topics related to fraud in the digital environment

2. RESEARCH METHOD

2.1 Literature Review Approach

This literature review uses a narrative and a descriptive review approach. The literature review method is appropriate for research that aims to draw conclusions from previous research or find certain patterns in previous studies that have different results[11]. This study aims to identify and analyze fraud techniques found in the digital business environment addressed in previous studies. Thus, the literature review method is considered appropriate in this study.

The narrative review approach uses verbal descriptions to describe previous studies, focusing on specific topics such as the theory used in the studies, research methods, or research results. Narrative review does not have a standard method in its implementation, but narrative reviews are often carried out by grouping previous research into certain classifications determined by the researcher [11]. The narrative review approach is considered appropriate for this study because it aims to classify previous studies based on IT fraud techniques that are addressed or relevant in the studies. The descriptive review approach classifies previous studies into groups, calculate the frequency of each group, summaries, and analyze the pattern to derive findings [11]. This study implemented the descriptive review approach by calculating the number of studies classified into each group to find patterns that may indicate the trends of certain topics so they can be compared to industry's needs.

2.2 Articles Selection

The main objects of this literature review were articles published in peer-reviewed journals. However, this study also included articles published as conference proceedings, if the articles are identified in the article selection process. This literature review selected articles by applying four stages, namely journal-based search, database-based search, keyword selection, and backward/forward search[9].

2.2.1 Journal Selection

This research selected reputable journals in the field of systems and information technology as a starting point for articles search. Journals should be published in English. This list of reputable journals was compiled by combining lists used by previous studies [9], [10]. The following is a list of journals that have been determined by the researcher as a starting point.

- MIS Quarterly
- Information System Research (ISR)
- Journal of Management Information System (JMIS)
- Journal of the Association for Information Systems (JAIS)
- European Journal of Information System
- Information & Management
- Communications of the Association for Information Systems (CAIS)
- Information System Journal (ISJ)

2.2.2 Database Selection

This study uses the ScienceDirect and Web of Science databases as the main databases for article searches. The database was chosen because journals that have been determined as the initial basis for searching for articles have been indexed by the two databases. This research also used Google Scholar to help identify if researchers missed identifying any relevant articles using these two main databases.

2.2.3 Keywords

This study selected articles that contain one or more keyword in their title or abstract. The keywords used in the search were;
"Information security", OR "computer security", OR "network security", OR "cybercrime", OR "online security", AND
"risk", OR "threat", OR "fraud", OR "breach", OR "theft", OR "deception"

After deciding the main journals, database, and keywords that will be basis of articles search, researchers conducted the following steps. The researchers search for articles by using predetermined keywords on the related journal web page's search feature. This study reviewed articles published in 2010-2020. Then, the researchers searched for articles in ScienceDirect web database and the Web of Science using predetermined search keywords. The search period was also 2010-2020. The researcher then conducted an article search using Google Scholar web database. The Google Scholar search results that enter the list or articles to be reviewed were only articles that had not been identified in the previous steps and published in well-reputed peer-reviewed journal or conference proceedings.

2.3 Literature Review Process

There is no standard method for conducting a literature review. In this study, researchers performed the following steps.

First, this study groups articles into categories and then calculates the frequency of each category to identify specific trends or patterns [11]. The categories were based on the different types of the research objectives [12], [13], types of information system security threats [14], security measures against fraud [15], research design [13] (Spender et al., 2017), and data collection techniques [12]. Two researchers classified each article in the list of reviewed articles individually based on a pre-arranged guideline. The results were compared and discussed between the two researchers to reach a unified result.

Table 1. Article Grouping Category

Category	Item	Reference
Nature of the theoretical aim of the paper	1) exploratory, 2) development, 3) testing, 4) review, 5) methodological 5) > 1 theoretical aim	[12] [13]
Information system security threats	1) Data security, 2) data privacy, 3) information overload, 4) data credibility, 5) transaction risk, 6) brute force attack, 7) illegal transaction, 8) deceptive activity 9) >1 security threats	[14]
Security measures against	1) preventive, 2) detective, 3) response	[15]

fraud	4) > 1 security measure 5) N/A	
Research design	1) Qualitative, 2) Quantitative, 3) both	[13]
Method of data collection	1) Interview, 2) observation, 3) archival, 4) participant observation, 5) others, 6) > 1 methods	[12]

Second, this study utilized a structured thematic analytical method by performing cluster analysis using NVIVO, based on word similarly. This method aimed to identify themes or topics that are often discussed in articles and journals, without any researchers' bias.

3. RESULTS AND DICUSSIONS

3.1 An Overview of Information Security Studies' Research Method

The article selection process as described in the Methods section identified 79 articles published in 2010 – 2020 that fulfill the predetermined criteria. These articles were grouped according to categories mentioned in Table 1.

First step is classifying research aims of these articles. This study found that most studies in this field are still aimed at testing an existing theory or model, reaching 46 percent. However, the proportion of research that aims to develop a research model or new idea is also quite large, reaching 30 percent. At this stage of analysis, the researcher combines two previously separate categorical items, namely developmental and methodological because in the process of categorizing the researcher found that these two objectives resulted in similar ideas or findings in the field of information security.

Table 2. Classifying Articles based on Research Aim

Research/Paper aim	**Number of Articles**	**Percentage**
Exploratory	1	1%
Development or methodological	24	30%
Review	8	10%
Testing	36	46%
> 1 theoretical aim	8	10%
Others	2	3%
Total	79	

Tabel 2 shows that there were eight articles identified as having more than one research aims. These articles aim to build a new technique or model on information systems (development). However, they do not stop at developing the model, they also immediately test the effectiveness of the model by using actual data (testing). Thus, it can be concluded that scientific articles in the field of information security generally aim to test an existing model or theory or building a new model or technique in the field of information system security.

This finding was in line with the result of grouping articles based on its research design. Table 3 shows that most studies in the field of information security and fraud use quantitative methods. However, the proportion of research that uses qualitative and mixed methods is also not small. These results are in line with the research objectives identified in Table 2. Research that aims to build a research model or new idea tends to use qualitative or mixed methods, while research that aims to test existing hypotheses or theories tends to use quantitative methods.

Table 3. Classifying Articles based on Research Design

Research Design	**Number of Articles**	**Percentage**
Qualitative	24	30%
Quantitive	43	54%
Both	12	15%
Total	79	

This study found that the data collection methods used in information security studies varied widely. Table 4 shows that data collection through secondary sources (archival) is the most frequently used technique. There are 19 studies that use more than one data collection technique. These studies combined secondary and primary data, so they usually combine archival and other techniques such as interviews or questionnaires. The four studies that used other data collection methods implemented simulation or experimental techniques to obtain the required data.

Table 4. Classifying Articles based on Data Collection Method

Data Collection Method	Number of Articles	Percentage
Interview	3	4%
Observation	9	11%
Archival	28	35%
Questionnaire	16	20%
> 1 method	19	24%
Other methods	4	5%
Total	**79**	

The interesting thing to note is that secondary data collection techniques are not only popular for research aimed at testing existing theory or hypothesis but are also quite popular for research aimed at developing new model or theory. An example of popular topic addressed in these types of studies is examining the hacker community or other information system user communities on the internet [16], [17].

3.2 Information Security Threats in Journal and Other Scientific Publications

The rapid growth of information technology shift how information system users assess fraud or information system security threats that need special priority. Based on review of selected articles published in 2010-2020, this study found that the topic of fraud or security threats that is most discussed in scientific articles is data security. This topic is generally divided into two smaller categories, namely the threat of data security fraud from outside the entity or organization, and threats originating from within the organization. Threats in the organization are also divided into two, namely threats that occur due to negligence of internal parties (non-fraud) and threats that occur due to internal fraudsters (fraud).

Brute force attack discusses fraudulent actions that specifically utilize certain applications or techniques to damage or steal information from an entity's information system. Articles that specifically discuss this topic raise the issue of spyware, virus¸ DDoS attacks, or the weakness of an entity's information system network as a whole. The articles that discuss deceptive activity raises the topic of social engineering and phishing where fraudsters deceive entities to gain access to information systems used by entities. Some articles focus on several types of information system fraud threats at once. This article generally discusses the threats to the entity's information system as a whole so that they consider the various types of threats that can occur.

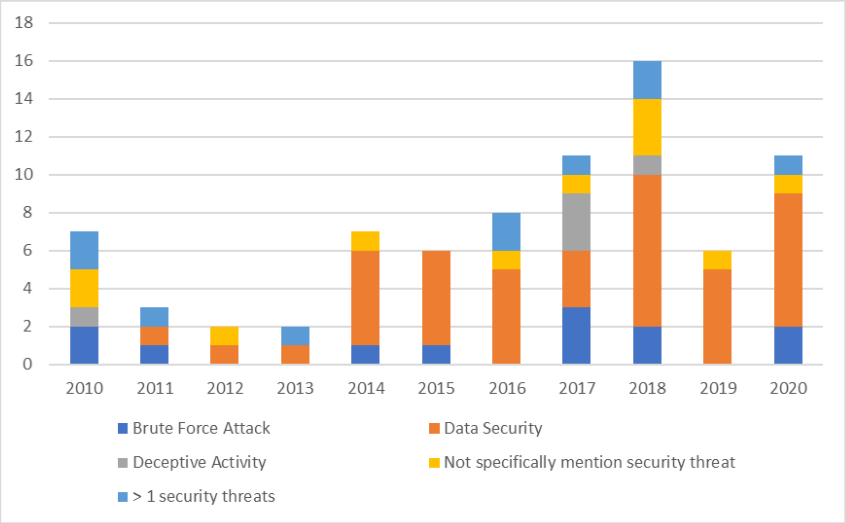

Fig 1: Information System Fraud/Threat Discussed in the Article during 2010-2020

It is also important to pay attention to the distribution of types of fraud or information system threats discussing in articles based on the article's year of publication. This analysis can provide an overview of how much attention the academics pay to a particular threat or information system fraud in a given year. Figure 1 provide the overview.

Data security threat is an issue that is growing in importance. Figure 1 shows that the number of scientific articles on this topic had increased for the last few years. The importance of data security grows along with the spread of technology that requires data sharing, such as the Internet of Things (IoT) or virtual office. However, this study also notes that deceptive activity, which includes social engineering issues and other similar fraud methods, is the least discussed topic. Several surveys found that there is an increasing number of targeted phishing email, which is one of the social engineering schemes [2], [3]. Various literatures often mention the user or human aspect of information system as one of the main elements of weakness in an entity's information system. Therefore, this topic should receive more attention from academics.

3.3 Security Measures Against Information System Threat in Journal and Other Scientific Publications

After discussing various types of fraud and information system threats that have been addressed in previous studies, the next step is to identify various prevention or countermeasures against information system security threats.

This study found that the security measure that is most discussed by academics is preventive measures. Topics that are often raised related to this security measure are discussions about company security policies, employee perceptions, factors that affect the success of a security policy, and other similar topics. The popularity of preventive measures as a research topic is natural because various studies and references mention preventive measures as the most effective and inexpensive step in fighting fraud [15].

The least discussed topic is response actions. The articles that address this topic specifically discuss methods to minimize impacts if a company becomes a victim of digital environmental fraud. The methods in general can be divided into two smaller groups. First, articles that discuss steps to improve the system. Second, articles that discuss customer relationship management to overcome customer dissatisfaction and concerns if a company experiences information system fraud.

All articles that address several security measures in their study usually combine preventive measures and other security measures such as detection and response. The combination of prevention and detection is considered the most effective security measure because it focuses on preventing fraud before its impact is felt by customers or other stakeholders of the entity.

3.4 Thematic Analysis

Cluster analysis was used for thematic analysis which aims to identify most discussed topics in articles related to fraud in the digital environment. The analysis is used to find important topics in previous studies, which have not been included in the previous descriptive analysis. Researchers summarized nine topics often discussed in previous studies, as follows.

- Data sharing risk, data security, and data privacy
- User and human aspect on information security risk management
- Designing information system security management to fight against cyber criminals
- How industry and stakeholders perceive cybersecurity challenges and impacts
- Cyberespionage

3.4.1 Data sharing risk, data security, and data privacy

The growing value and importance of data encourages businesses to consider data management in their operation. Data management issues tend to differ greatly between one business and another. They are also greatly varied between different industries.

Research in data security often focus on health industry. Health industry keeps improving its information technology adoption in its operasion to facilitate patients' needs. However, the increased use of information technology in health industry also increase the chance of data breach, especially regarding patient data [18]. Information system security certification for health agencies also become a special concern for several studies, especially regarding its effectiveness in suppressing the data breach of patient information [19].

One of the main challenges for entities related to data security is deciding who has access to company data. Outsourcing is often seen as an option in providing inexpensive and customizable corporate information systems, but there are new risks caused by allowing third parties to access company data [20]. There is also an idea to create an industrial community to share certain data and information [21], but this idea was stalled by the possible risk of weakening individual business's position against competitors [22].

3.4.2 User and human aspect on information security risk management

The human user of an information system is one of the main elements of an information system, which unfortunately is often judged as a loopholes or weakness in an information system security [23]. This idea encourages many businesses to take steps in reducing the information system risks caused by employees, whether they occur due to negligence (error) or intentional (fraud) [24].

The most common security measures used by entities to reduce the impact caused by user negligence or insider threats are policies and rules. Entities usually focus on policies that regulate the use and management of information system security [24]–[28] and specific rules governing individual access to data and information systems infrastructure [29].

3.4.3 Designing information system security management to fight against cyber criminals

In general, the topic of designing information system security management can be divided into three smaller groups. First, design and policies that focus on the user. Two steps for managing information system users, namely access policies and settings, have been discussed in 3.4.2. Another step that needs to be considered is the extent to which system users are given the opportunity to participate in information security risk management [30] as well as continuous training models which can increase user resilience in the face of information security threats [31]. Second, the design and mechanism to early identify hackers or potential threats to prevent or detect early any attacks on corporate information systems [17], [32], [33]. Third, the technical design of corporate information systems that make it difficult for hackers or other security threats to hack into the company's overall system [34]–[36].

3.4.4 How industry and stakeholders perceive cybersecurity challenges and impacts

An important idea of how cybersecurity affects is the importance of an integration between various parties to fight cybercrime effectively. A study recommend to create integrated policies and procedures at all levels of public-private-government partnerships as a line of defense against cybersecurity threats in the United States [37]. All parties must be willing to be involved because problems with one entity can continue to other entities an create ripple effects, so there is great chance that market mechanisms can punish parties who are considered reluctant to contribute to cybercrime prevention [38].

3.4.5 Cyberespionage

The topic of cyberespionage is a new information security issue that is starting to emerge. Articles discussing this issue were only published in 2020. In general, this article discusses structured and targeted forms of data and information theft, where the perpetrator is no longer an individual, but an organization. One form of cyberespionage is embedding spyware on smartphones or other devices that allow continuous transfer of information [39].

4. CONCLUSIONS AND RECOMMENDATION

This study found that the most discussed information system fraud topic in previous studies was the threat to data security, which was then followed by brute force attacks which included various technical attacks of viruses, worms, and hacker attacks. Deceptive activity is an information system threat that is rarely discussed in previous studies. The analysis of topics per year shows that there has been a steady increase in recent years related to scientific articles on the topic of data security. However, there is only small number of articles discussing deceptive activity while the industry faces rising number of this type of information system fraud. Most information system security articles address preventive measures as the most commonly discussed security measures, which are then followed by detection and response.

Several topics commonly discussed in previous studies were (1) data sharing and data security, (2) User and human aspect on information security risk management, (3) designing information system security management to fight against cyber criminals, (4) how industry and stakeholders perceive cybersecurity challenges and impacts, and (5) cyberespionage.

This study recommended future researchers to address many types of deceptive activity in digital environment. Deceptive and social engineering are fraud techniques that have become increasingly popular fir the last few years. However, the number of articles on this topic is still few and far between in recent years. Research on this topic is urgently needed along with the increasing use of the internet. Cyberespionage is also an interesting topic to be pursued by future studies. The topic is still rarely discussed by scientific articles in the field of information security and fraud. Generally, this topic is still considered similar with data security. However, the increasing popularity of electronic devices that utilize the Internet of Things (IoT) increase the importance of this topic in the future.

5. ACKNOWLEDGMENTS

This study was funded by Faculty of Economics, Universitas Negeri Yogyakarta.

REFERENCES

[1] S. Kurnia, J. Choudrie, R. M. Mahbubur, and B. Alzougool, “E-commerce technology adoption: A Malaysian grocery SME retail sector study,” *J. Bus. Res.*, vol. 68, no. 9, pp. 1906–1918, 2015, doi: 10.1016/j.jbusres.2014.12.010.

[2] Symantec, *Internet security threat report*, vol. 21. 2016.

[3] Symantec, “Internet Security Threat Report VOLUME 24, February 2019,” *Netw. Secur.*, vol. 21, no. February, p. 61, 2019, [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1353485805001947.

[4] A. Yassir and S. Nayak, “Cybercrime: A threat to Network Security,” *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 12, no. 2, p. 84, 2012, [Online]. Available: http://paper.ijcsns.org/07_book/201202/20120214.pdf.

[5] D. Rahmawati, R. Yudhiyati, and A. Putritama, “How Micro and Small Enterprises Perceive Information Technology Fraud: A Study of Indonesian’ Small Businesses,” *5th Int. Conf. Comput. Eng. Des. ICCED 2019*, 2019, doi: 10.1109/ICCED46541.2019.9161104.

[6] R. Yudhiyati, A. Putritama, and D. Rahmawati, “What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case,” *J. Information, Commun. Ethics Soc.*, 2021, doi: 10.1108/JICES-03-2021-0035.

[7] R. Bhowmik, “Detecting Auto Insurance Fraud by Data Mining Techniques,” *J. Emerg. Trends Comput. Inf. Sci.*, vol. 2, no. 4, pp. 156–162, 2011.

[8] Y. D. Shin, “New model for cyber crime investigation procedure,” *J. Next Gener. Inf. Technol.*, vol. 2, no. 2, pp. 1–7, 2011, doi: 10.4156/jnit.vol2.issue2.1.

[9] M. Silic and A. Back, “Information security: Critical review and future directions for research,” *Inf. Manag. Comput. Secur.*, vol. 22, no. 3, pp. 279–308, 2014, doi: 10.1108/IMCS-05-2013-0041.

[10] H. Zafar and J. G. Clark, “Current state of information security research in IS,” *Commun. Assoc. Inf. Syst.*, vol. 24, no. 1, pp. 557–596, 2009, doi: 10.17705/1cais.02434.

[11] W. R. King, J. He, and J. H. Katz, “Understanding the Role and Methods of Meta- Analysis in IS Research,” *Commun. Assoc. Inf. Syst.*, vol. 16, no. 16, pp. 665–686, 2005, [Online]. Available: http://aisel.aisnet.org/cais%0Ahttp://aisel.aisnet.org/cais/vol16/iss1/32.

[12] T. Mcnulty, A. Zattoni, and T. Douglas, “Developing Corporate Governance Research through Qualitative Methods: A Review of Previous Studies,” *Corp. Gov. An Int. Rev.*, vol. 21, no. 2, pp. 183–198, 2013, doi: 10.1111/corg.12006.

[13] J. C. Spender, V. Corvello, M. Grimaldi, and P. Rippa, “Startups and open innovation: a review of the literature,” *Eur. J. Innov. Manag.*, vol. 20, no. 1, pp. 4–30, 2017, doi: 10.1108/EJIM-12-2015-0131.

[14] F. L. Budiono, S. Lau, and W. Tibben, “Cloud Computing Adoption for E-Commerce in Developing Countries: Contributing Factors and Its Implication for Indonesia,” 2018.

[15] W. S. Albrecht, C. O. Albrecht, C. C. Albrecht, and M. F. Albrecht, *Fraud Examination*, 5th editio. Boston: Cengage Learning, 2016.

[16] V. Mookerjee, R. Mookerjee, A. Bensoussan, and W. T. Yue, “When hackers talk: Managing information security under variable attack rates and knowledge dissemination,” *Inf. Syst. Res.*, vol. 22, no. 3, pp. 606–623, 2011, doi: 10.1287/isre.1100.0341.

[17] S. Samtani, R. Chinn, H. Chen, and J. F. Nunamaker, “Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence,” *J. Manag. Inf. Syst.*, vol. 34, no. 4, pp. 1023–1053, 2017, doi: 10.1080/07421222.2017.1394049.

[18] S. H. Kim and J. Kwon, “How do EHRs and a meaningful use initiative affect breaches of patient information?,” *Inf. Syst. Res.*, vol. 30, no. 4, pp. 1184–1202, 2019, doi: 10.1287/isre.2019.0858.

[19] J. Kwon and M. E. Johnson, “Meaningful healthcare security: Does meaningful-use attestation improve information security performance?,” *MIS Q.*, vol. 42, no. 4, pp. 1043–1067, 2018, doi: 10.25300/MISQ/2018/13580.

[20] N. Feng, Y. Chen, H. Feng, D. Li, and M. Li, “To outsource or not: The impact of information leakage risk on information,” *Inf. Manag.*, vol. 57, 2020, doi: 10.1016/j.im.2019.103215.

[21] N. M. Menon, “Information spillover and semi-collaborative networks in insurer fraud detection,” *MIS Q.*, vol. 42, no. 2, pp. 407–426, 2018, doi: 10.25300/MISQ/2018/14433.

[22] C. Y. Jeong, S. Y. T. Lee, and J. H. Lim, “Information security breaches and IT security investments: Impacts on competitors,” *Inf. Manag.*, vol. 56, no. 5, pp. 681–695, 2019, doi: 10.1016/j.im.2018.11.003.

[23] P. Baltzan, J. Fisher, and K. Lynch, *Business Driven Information Systems*, 3e ed. North Ryde: McGraw-Hill Education Australia, 2015.

[24] Y. Chen, K. Ramamurthy, and K. W. Wen, “Organizations’ information security policy compliance: Stick or carrot approach?,” *J. Manag. Inf. Syst.*, vol. 29, no. 3, pp. 157–188, 2012, doi: 10.2753/MIS0742-1222290305.

[25] P. Ifinedo, “Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition,” *Inf. Manag.*, vol. 51, no. 1, pp. 69–79, 2014, doi: 10.1016/j.im.2013.10.001.

[26] L. Jaeger, A. Eckhardt, and J. Kroenung, “The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis,” *Inf. Manag.*, no. January 2018, 2020, doi: 10.1016/j.im.2020.103318.

[27] A. C. Johnston, M. Warkentin, M. McBride, and L. Carter, “Dispositional and situational factors: Influences on information

security policy violations," *Eur. J. Inf. Syst.*, vol. 25, no. 3, pp. 231–251, 2016, doi: 10.1057/ejis.2015.15.

[28] A. Vance, M. T. Siponen, and D. W. Straub, "Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures," *Inf. Manag.*, vol. 57, 2020, doi: 10.1016/j.im.2019.103212.

[29] A. Vance, P. B. Lowry, and D. Eggett, "Using accountability to reduce access policy violations in information systems," *J. Manag. Inf. Syst.*, vol. 29, no. 4, pp. 263–290, 2013, doi: 10.2753/MIS0742-1222290410.

[30] J. L. Spears and H. Barki, "User Participation in Information Systems Security Risk Management," *MIS Q.*, vol. 34, no. 3, pp. 503–522, 2010.

[31] P. Puhakainen and M. Siponen, "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Q.*, vol. 34, no. 4, pp. 757–778, 2010.

[32] V. Benjamin, B. Zhang, J. F. Nunamaker, and H. Chen, "Examining Hacker Participation Length in Cybercriminal Internet-Relay-Chat Communities," *J. Manag. Inf. Syst.*, vol. 33, no. 2, pp. 482–510, 2016, doi: 10.1080/07421222.2016.1205918.

[33] W. Li, H. Chen, and J. F. Nunamaker, "Identifying and Profiling Key Sellers in Cyber Carding Community: AZSecure Text Mining System," *J. Manag. Inf. Syst.*, vol. 33, no. 4, pp. 1059–1086, 2016, doi: 10.1080/07421222.2016.1267528.

[34] A. Arora, R. Krishnan, R. Telang, and Y. Yang, "An empirical analysis of software vendors' patch release behavior: Impact of vulnerability disclosure," *Inf. Syst. Res.*, vol. 21, no. 1, pp. 115–132, 2010, doi: 10.1287/isre.1080.0226.

[35] O. Temizkan, S. Park, and C. Saydam, "Software diversity for improved network security: Optimal distribution of software-based shared vulnerabilities," *Inf. Syst. Res.*, vol. 28, no. 4, pp. 828–849, 2017, doi: 10.1287/isre.2017.0722.

[36] J. Wolff, "Perverse Effects in Defense of Computer Systems: When More Is Less," *J. Manag. Inf. Syst.*, vol. 33, no. 2, pp. 597–620, 2016, doi: 10.1080/07421222.2016.1205934.

[37] A. Green, K. Dodson, A. B. Woszczynski, and P. Easton, "Responding to cybersecurity challenges: Securing vulnerable U.S. emergency alert systems," *Commun. Assoc. Inf. Syst.*, vol. 46, pp. 187–208, 2020, doi: 10.17705/1CAIS.04608.

[38] A. Hovav and P. Gray, "The ripple effect of an information security breach event: A stakeholder analysis," *Commun. Assoc. Inf. Syst.*, vol. 34, no. 1, pp. 893–912, 2014, doi: 10.17705/1cais.03450.

[39] S. Sharma, N. Kumar, R. Kumar, and C. R. Krishna, "The Paradox of Choice: Investigating Selection Strategies for Android Malware Datasets Using a Machine-learning Approach," *Commun. Assoc. Inf. Syst.*, vol. 46, 2020, doi: 10.17705/1CAIS.04626.