Information Security Research Challenges in the Process of Digitizing Business: A Review Based on the Information Security Model of IBM

Jason X. S. Wu and Shan Liu

1 Introduction

The rise of big data and cloud computing has brought all types of data analysis techniques into the process of business decision and further reshaped the business process. Analysis of various data, such as macroeconomic, enterprise operational, and consumer behavior data, has greatly improved business decisions. However, some security concerns arise in the process of digitizing businesses.

Existing security research has two categories of issues, namely, data security and system security [44]. With regard to data security, common previous topics have mainly focused on developing all types of encrypting technology to help protect security online, such as key cryptography, secure socket layer, and cookies [44]. However, industry and research communities have added "personnel security" as the third category. Unconscious and malicious organizational insiders should be responsible for nearly half of security breaches because of failure to comply with information security policies (ISPs) of firms. Organizational insiders refer to individuals who are authorized to access organizational internal information system (IS) or other assets. Security managers and researchers have considered three main types of measures to compel these insiders to follow ISPs, including security education, training, and awareness (SETA) programs, fear appeal, and system monitoring [11, 16, 22, 23, 29], which have become new research interests that emerged from the digitization of businesses. Meanwhile, in system security protection, all types of traditional system security protection tools or software have been used against endless attacks, such as firewalls, proxy servers, and virtual private networking [44]. However, the Ponemon Institute reported that 80% of businesses cannot properly manage external cyberattacks, although they spend an average of $3.5 million per year for all types of system security protection deployment [15]. Meanwhile, the

J. X. S. Wu · S. Liu (✉)
School of Management, Xi'an Jiaotong University, Xi'an 710049, China
e-mail: shan.l.china@gmail.com

F. P. García Márquez and B. Lev (eds.), *Data Science and Digital Business*,
https://doi.org/10.1007/978-3-319-95651-0_6

recent studies and industry reports have claimed that consumer awareness of threats caused by privacy risk [8] has been intensified; moreover, consumers have become more concerned about whether organizations are sufficiently capable and willing to protect their ISec although data gatherers tell consumers what they have collected and promise that they will protect their data from illegal usage. Hence, the contradiction between the low efficiency of organizational system security protection and the increasing concerns for user privacy has emerged and has even been intensified with the increased digitization of businesses.

Additional issues, such as anonymization and data masking, lack of legal protections, patents and copyrights concerns, have emerged. Even discrimination may be enhanced by using big data analytics in the process of digital businesses. Different from the existing discrimination concerns, big data analysis allows a type of "automated" discrimination. For example, the racial or sexual orientation of an applicant is not allowed to be disclosed to the financial organization in the existing process of business decision. However, this information can be easily inferred through data analysis based on various data collected online. Thus, conducting targeted studies to explore the possible countermeasures is urgently needed.

To sum up, when we focus on the security of an organization, aside from data, IS (or IT, adopted and deployed by the organization), human behavior (including insiders and consumers of the organization), business process as the new type of object must be emphasized and its interaction with other objects (e.g., data, human and system) must be explored. Before adopting and utilizing big data analytics, organizations should consider and be requested not to infringe on consumer privacy and to avoid creating additional hidden security concerns. As discussed above, all types of ISec research and new challenges have emerged. However, knowledge about whether the academic research has responded to the requirements of industry well, especially in the process of digital business, is insufficient. Hence, a summary of existing research can serve as a guideline for industry application. It can also serve as a theoretical basis and literature in determining possible ways of managing new security challenges and provide new directions for subsequent researchers.

This chapter aims to review and compare academic studies and existing requirements of industry to provide insight into the matching extent of literature and practice. This review also further identifies some research directions, especially new emergent research topics or challenges due to the digitization of businesses for further ISec research by IS researchers. We adopt the ISec framework of IBM as a representative of the requirement of industry to cluster the existing security studies published in the mainstream IS journals in the past four years.

The following section will introduce the research method. This section specifies the manner in which journals and papers are selected and each paper is coded, from which we provide a comprehensive overview of ISec research. This section also imparts some important insights. The next section briefly presents current ISec studies based on the IBM security model, which provide us a basis to determine the four important security objects (i.e., data, human behavior, IT/IS, and business processes) in organizations. The subsequent section will further examine the interactions between different objects and some recommendations for the research and industry communities are identified and provided. Finally, we provide a comprehensive conclusion and limitations of our review.

2 Review Method

Guidelines of Webster and Watson [66] are adopted to conduct this review through four steps. First, we decide on the research fields, search items, and criteria for the inclusion or exclusion of a paper. Second, we limit the sample after searching through all the identified sources. Third, analysis of the texts of the selected set of studies is conducted, considering the IBM ISec capability reference model. Finally, we categorize and structure the content of our review. Before introducing the details of our review method, we first introduce the IBM ISec capability reference model.

2.1 Core ISec Themes: IBM ISec Capability Reference Model

IBM always stands at the frontline of the ISec battlefield and provides the timely response and effective solutions to the security threat of industry to maintain leadership of the security market and be a competitive ISec service provider. Thus, security solutions of IBM is a good representative of the requirements of industry and can provide a good guideline for the academic community. The IBM Information Security Capability Reference Model is a comprehensive model that addresses technical, behavioral, and managerial issues related to ISec. Thus, the model supports our initial argument, which emphasizes on the four objects (i.e., data, human behavior, IT/IS, and business processes) in organizations. Using this model, IBM can help businesses with security troubles in assessing their enterprise security posture and then provide all types of measures for improving their security level. The eight security themes of this framework are shown in Table 1. Although the themes of the model cover broad areas of ISec, the assessment factors help us to limit potential research areas associated with each theme. Zafar and Clark used this model to review the security literature in mainstream IS journals from their founding to 2007 and proposed ISec economics as a ninth theme into this model [70]. This chapter will use the final model adapted by Zafar and Clark to classify the latest security research published in six leading IS journals in the past four years.

2.2 Journal Selection and Paper Identification

Journals in the IS field are selected because we focus on what IS researchers have contributed to ISec research. To ensure the quality of selected papers over quantity,

Table 1 Zafar and Clark's adaption of IBM Information Security Capability Reference Model

Security themes	Assessment	
Governance	• Strategy and information • Security policy • Security compliance	• Security risk management • Governance structure • Information security advisory
Privacy	• Policy, practices and controls • Privacy and information Management strategy	• Data, rules, and objects
Threat mitigation	• Network segmentation and boundary protection • Vulnerability management	• Content checking • Incident management
Transaction and data integrity	• Business process transaction security • Database security	• Message protection • Secure storage • Systems integrity
Identity and access management	• Identity proofing • Access control	• Identity lifecycle management
Application security	• Systems development life cycle	• Application development • Environment
Physical security	• Site management physical	• Asset management
Personnel security	• Workforce security	
Information security economics	• Information security investment	• Consumer choice

we selected six mainstream IS journals from the "Basket of Senior IS Scholars" that are deemed high quality [36, 37]. The six journals are as follows.

MIS Quarterly
Information Systems Research
Journal of Management Information Systems
Journal of the Association for Information Systems
European Journal of Information Systems
Information Systems Journals

To be included in our review, each journal article must include security or privacy as a key construct and be relevant to organization security in response to our focus. In our search for literature, which involved identifying papers on ISec in web of science core collection using keywords "security" and "privacy," we found 65 articles related to ISec in the target journals and the defined years. During the first review, we removed six articles that were not organization security studies in the actual sense but only contained references on security concept. Finally, we obtained 59 articles for in-depth coding.

2.3 Coding Methods

According to the traditional coding method, we coded each paper's "author–time," "research questions", "theoretical basis", "research method", "research findings and practical implication", and "limitation". Aside from these items, we also coded each paper as one or more themes of IBM security model suited to our purposes. One paper may relate to two or more topics. Accordingly, each paper was assessed to focus on one or more types of objects (i.e., data, human behavior, IS/IT, and business processes) and their interaction. The details of coding result are shown in the appendix.

3 Overview of ISec Research

3.1 Papers Distributions by Journal and Period

Table 2 shows that 59 ISec papers published in the selected journals from January 2014 to 2017 have focused on the organizational security. Except for 2017, published ISec papers are increasing with years, which shows the importance of ISec research in the IS field. When journals are considered, JMIS and MISQ are the top two journals that publish most ISec studies with emphasis on organizational ISec.

3.2 Contribution of ISec Research to Industry Requirements

Figure 1 shows the number of papers for each theme of the IBM ISec model. Most work of IS research community refers to the "governance" theme, which involves the development of strategic and compliance programs, mechanism, and structure. In addition, "personnel security" and "threat mitigation" are the second and third themes explored. The former mainly considers how to confine and normalize the behaviors of the insiders and users of organizations to avoid information leakage, whereas the latter focuses on threat or vulnerability detection and incidence management.

In view of the focus of this review, we are interested in the security concerns and findings in the process of digitizing businesses. This topic is closer to the "transaction and data integrity" and "privacy," which lack extensive research. We further counted the number of papers of important and less important themes in each year and observed the papers' number change with years, as shown in Fig. 2.

From Fig. 2, although themes including "governance" and "personnel security" have more relevant papers, papers in both themes decreased with years. Increasing unimportant theme includes "identity and access management". Meanwhile, "privacy", "threat mitigation", and "information security economics" seem to be increasingly important themes because papers for these themes increased with years (we

Table 2 The number of papers published by each journal in each year

Target journal	2014	2015	2016	2017	Total
Information systems research	2	4	4	1	11
MIS quarterly	2	5	2	3	12
Journal of management information systems	3	4	8	2	17
European journal of information systems	4	1	4	2	11
Journal of the association for information systems	1	1	2	0	4
Information systems journals	2	2	0	0	4
Total	14	17	20	8	59

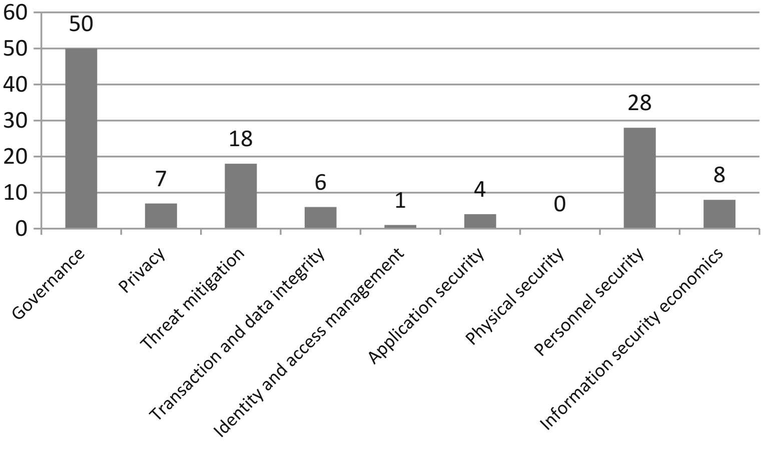

Fig. 1 The number of papers located in each theme

only searched papers from 2014 to 2017). "Application and physical security themes" seem to become farther from the sight of the IS scholars, which may be attributed to the themes being closer to computer science research topics.

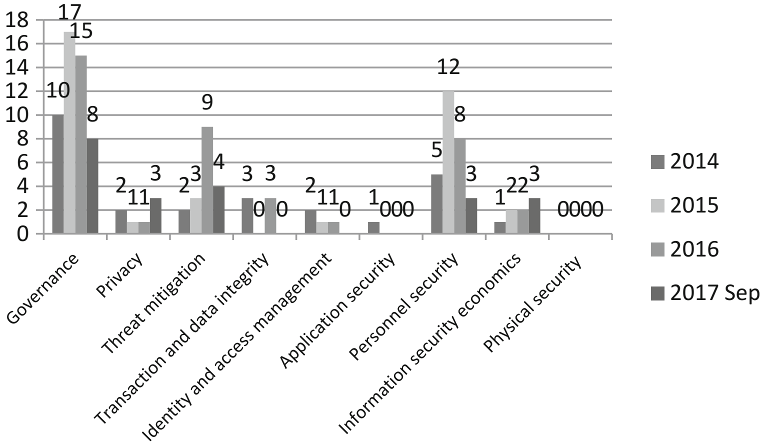

Fig. 2 The number of papers located in each theme in each year

Finally, "transaction and data integrity" seems to have no rule to identify its importance. However, when we consider the three months left in 2017, we expected more related papers would be published. Nevertheless, we can still consider the theme as an important topic because more than 10% of papers are about this topic.

To sum up, the IS community has contributed more to the following three themes of IBM ISec model: "governance", "threat mitigation", and "personnel security". Among these themes, "threat mitigation" has become increasingly important. However, the other two seem to be excessive studied by ISec scholars. "Privacy" and "transaction and data integrity" are also worth of emphasis and further analysis.

3.3 Main Theories and Methods Conducted in Each Theme

We also summarized a brief description of the research methods and theories for each theme. Table 3 shows how varied research in ISec is and how it can be advanced further. More sociological theories (especially in the "personnel security" theme) and organizational theories were adopted, and qualitative and quantitative research methods were used.

4 Research Streams Summary

In this section, we provide a brief overview of each of the articles according to theme and method of assessment.

Table 3 Theories and methods adopted in each theme

Themes	Theory basis	Methods used
Governance	Persuasion theory; Motivation theory; Social control theory; Information foraging theory; Deterrence theory; Compliance theory; Theory of knowledge retention; Accountability theory; Social network analysis; Habituation Theory; Institutional theory; Strain theory	Design science; Behavioral experiment; Modeling; Case study; Scenario-based survey;
Privacy	Theory of unintended consequences; Self-control theory; Theory of planned behavior; Social learning theory; Mindfulness theory; Universal philosophical theories of ethics; Opportunity theory of crime; Institutional anomie theory; Routine activity theory; Actor-network theory; structuration theory; Contextualism; Selective organizational rule violations model; Dual-task interference theory; Justice Theory; Sanction Theory; context-updating theory; Organizational control theory; Reactance theory; Fairness theory; Extended parallel process model; Behavioral decision-making; Traditional monitoring methods; Expectation confirmation theory; Technology Threat Avoidance Theory (TTAT)	A growth mixture model approach; Functional magnetic resonance imaging; Grounded theory Ethnography; Theory development; Approach development; Interview; Experiment
Threat mitigation	K-anonymity framework; regression tree; Privacy impact assessment; Selective organizational rule violations model; Strain Theory; General deterrence; Expectation confirmation theory; Theory of Justice; Psychological Contract theory; Institutional Theory	Algorithm; Experiment; Approach development; Theory development; Grounded theory; Scenario-based survey; A growth mixture model approach; Case
Transaction and data integrity	Persuasion theory; Motivation theory; Diffusion of innovation; Context sensitive theory; Coping theory; Interpersonal deception theory; Social distance theory; Media richness theory; Opportunity theory of crime, Institutional anomie theory; Institutional theory; Trait theory	Experiment; Modeling; Survey; Data mining/machine learning; Case study; Integration-analytics technologies; Design science; Algorithm

(continued)

Table 3 (continued)

Themes	Theory basis	Methods used
Identity and access management	Protection motivation theory(PMT); Detection tool impact theory; Context-updating theory; Justice Theory; Sanction Theory; Extended parallel process model; Behavioral decision-making; Text mining technologies; Mindfulness theory; Expectation confirmation theory; Psychological contract theory; Habituation Theory	Scenario-based survey
Application security	K-anonymity framework; Regression tree; Cultural dimensions; Migration theory; Technology Acceptance Model (TAM); TTAT; PMT; Four-factor theory; Leakage theory; Verbal cues; Static Dynamic Linguistic; Competence model of fraud detection; Information manipulation theory; Criteria-based content analysis; Scientific content analysis; Reality monitoring; Channel expansion theory; Interpersonal deception theory; Interaction adaptation theory; Text mining technologies	Functional magnetic resonance imaging
Physical security	PMT; TTAT; Economic theory TAM	Experiment; Case study; Data mining/machine learning; Survey; Algorithm
Personnel	Theory of planned behavior; Expected utility, deterrence, and ethical work climate theory	Experiment; Factorial Survey; Modeling; Survey

4.1 Governance

Organizational ISec governance aims to form a stable management framework, which includes the mechanisms, processes, and structures by which organizational ISec is controlled and directed. The governance mechanisms are realized by the development of and compliance with ISec strategies and policies. Governance processes mainly include information objective setting and pursuit in the context of social, regulatory, and market environments. Organizations should focus on security risk management. Governance structures and principles aim to build bodies that will identify the responsibility of different participants in monitoring and governing organizational security. Following is a brief discussion of how governance, as applied to ISec, has been addressed in our selected journals. Most of papers are located in the development and compliance of strategy and information security policy.

In terms of strategy and information security policy, D'Arcy et al. [14] explored how complicated and unclear ISec requirements cause "security-related stress" to employees. Bhattacherjee and Park [7] explained the reason for users to move from client-centric computing to cloud computing. Choudhary and Zhang [13] explored the impact of a change in the distribution of defect-related costs on a vendor's release time and patching strategy under SaaS. Tsohou et al. [57] proposed a framework to guide designing and implementing ISec awareness programs by considering changes that happened in an organization. Vance et al. [60] found that users' perceived accountability could be increased by the UI design of broad-access systems and further reduce their intentions to violate access policies. Steinbart et al. [55] focused on what influences users' (dis)continuance to adopt security behavior from the UI design perspective. Johnston et al. [29] explored the effectiveness of an enhanced fear appeal rhetorical framework using a hypothetical scenario research design involving three unique threat/behavior pairs that were typical of fear appeal implementations in practice. Hsu et al. [22] clarified and examined the role of extra-role behaviors and social controls in organization on ISP effectiveness. Chen and Zahedi [11] investigated the differences in security behaviors between the people from United States and China on a relatively large scale based on context-sensitive theory. Kim et al. [31] examined the effect of cultural difference on security concerns on e-transactions. Ji et al. [27] analyzed a size-based security monitoring policy with and without profiling. Choi et al. [12] developed a model that shows how the recovery measures of firms influence customer behavior online after data breach. Goode et al. [17] explored how a breached organization could best determine the optimal level of customer compensation in response to data breach. Jensen et al. [26] developed a new way to conduct security training given that some employees are used to training based on rules. Wang et al. [62] suggested that companies should improve employees' coping adaptiveness, which is combined by task-focused coping, emotion-focused coping, and avoidance coping in the process of phishing email detection. Niemimaa and Niemimaa [45] explored the manner in which the best practice of IT service provider of information security system can be converted into contextualized practices. Khansa et al. [30] investigated the cyberloafing behavior of employees and its antecedents after an announcement of formal organizational controls.

In terms of security compliance, some scholars focus on the organizational level and others pay more attention to individual level. As to the former, Wall et al. [61] introduced a selective organizational rule violation model into organizational privacy and security contexts and proposed a selective organizational information privacy and security violation model. Sen and Borle [50] examined some public policies, such as public disclosure of vulnerabilities, IT security investment, and data breach laws, which would influence the data breach risk for a state and for organizations within an industry. Parks et al. [47] introduced a theoretical framework that explains the process by which the intended and unintended consequences of implementing privacy safeguards impact organizational privacy compliance. Angst et al. [3] examined whether the way of regulation rule adoption (i.e., symbolic and substantive) had a moderation effect on the relationship between IT security investments and follow-up data security breaches. Lee et al. [35] investigated how firm security would be influenced by a government's standard, especially with verifiable and unverifiable controls on security.

For the individuals' compliance to ISP, Li et al. [36, 37] identified extrinsic and intrinsic motivation for users' compliance to internet use policy (IUP). Moody (2015) proposed a new integrated model to understand the motivations for employees to accept new ISPs and react negatively against them. Sojer et al. [53] explored drivers of unethical programming behavior in individuals. Chatterjee et al. [10] developed a considerably thorough model to understand unethical IT use from different perspectives of individual, philosophy, sociology, economics, and technology. Boss et al. [9] extensively reviewed protection motivation theory (PMT) and its conventional practice in ISec research to identify opportunities for potential theoretical and methodological improvements on which to build this literature. Lowry et al. [42] explained the behavior of employees to blame organizations and even retaliate against them upon being informed of enhanced ISPs. Hu et al. [23] examined why individuals intentionally violate ISPs via a new paradigm with event-related potentials (ERPs). Posey et al. [48] researched the effect of insiders' organizational commitment levels on threat coping behavior and considered the interconnection of threat and coping appraisal via perceived response cost. Foth [16] explored the factors influencing the intention to comply with data protection in hospitals. Warkentin et al. [65] examined what insiders experience neurologically when faced with fear appeals. Jenkins et al. [25] conducted a behavioral experiment using fMRI and found that alerts in personal computing should be bounded in their presentation, which would cause interruptions to users and make them disregard the alert. Anderson et al. [1] examined the way of habituation to security warning development in the brain through fMRI. Anderson et al. [2] used a type of cognitive neuroscience method called Neuro IS to explore user response to security messages. Johnston et al. [28] identified key factors to explain employees' intention to violate ISPs from the perspectives of disposition and situation.

In terms of security risk management, Wang et al. [63, 64] characterized and distinguished different IS threats in terms of their risk characteristics and further explored the relation of risk characteristics to public searches for information on IS threats. Wright et al. [69] explored why certain influence techniques are especially dangerous when used in phishing attacks. Vance et al. [59] explored an accurate security risk perception measurement and its relationship with security behavior. Oetzel and Spiekermann [46] adopted a privacy impact assessment method to consider privacy issues systematically. Kim and Kim [32] examined how developers of security software learn from managing malware problems. August et al. [4] developed an understanding of how a software vendor approaches the versioning problem and how consumers separate across product variants to diversify security risk when both software as a service (SaaS) and on-premise versions are available. Mitra and Ransbotham [43] explored the relationship between two types of information disclosure (i.e., full and limited) and the diffusion of ISec attacks. Wang et al. [63, 64] showed how application risk from illegal access of insiders could be foreseen through application characteristics. Han et al. [19] investigated the critical antecedents that motivate students to comply immediately with messages from campus emergency notification systems. Zahedi et al. [71] explained how user's reliance on detection tools is influenced by the performance and cost of the tools. Guo et al. [18] explored the propagation process of malware with a structural risk model. Wolff [68] found that defenses could cause the opposite effect, which exposes the protected systems to new and unpredicted vulnerabilities in the context of complex computer systems. Hui et al. [24] examined whether deterring distributed denial-of-service (DDOS) attacks could be decreased by implementing convention on cybercrime.

4.2 Personnel Security

Personnel security relates to the workforce of an organization. Assessment factors include awareness training, code of conduct, and employment life cycle management. The issue of ethics in security varies from behavioral research to building a network infrastructure. Personnel plays an important role in establishing and maintaining ISec within an organization. Unless IT usage is frequently trained and security awareness and organizational code of conduct are promoted, personnel can inadvertently introduce threats into the organization.

In terms of the external threat targeted on employees, Wright et al. [69] explored why certain influence techniques are especially dangerous when used in phishing attacks to employees. Ho et al. [21] demonstrated the use of different language–action cues of deceivers in different contexts. Wang et al. [63, 64] characterized and distinguished different IS threats in terms of their risk characteristics and further explored how risk characteristics related to public searches for information on IS threats.

In terms of the violation behavior, Sojer et al. [53] explored what drove unethical programming behavior in individuals. Chatterjee et al. [10] developed a considerably thorough model that illustrates unethical IT use from different perspectives of individual, philosophy, sociology, economics, and technology. Hu et al. [23] examined why individuals intentionally violate ISPs through a new paradigm with ERPs. Liang et al. [40] examined and validated several characteristics of malicious insiders noted in the extant literature. D'Arcy et al. explored how complicated and unclear ISec [14] requirements could cause "security-related stress" to employees. Johnston et al. [28] identified key factors to explain employees' intention to violate ISPs, considering disposition and situation. Foth [16] explored the factors that influence employees' intention to comply with data protection in hospitals. Li et al. [36, 37] identified extrinsic and intrinsic motivation for users' compliance to IUP. Lowry and Moody [41] suggested a new integrated model to understand employees' motivations to accept new ISPs and react negatively against them. Lowry et al. [42] explained the behavior of employees to blame organizations and even retaliate against when they are informed about enhanced ISPs. Anderson et al. [1, 2] used Neuro IS, a type of cognitive neuroscience method, to explore user response to the security messages. Anderson et al. [1] used fMRI to examine how habituation to security warnings develops in the brain. Jenkins et al. [25] conducted a behavioral experiment to explain why individuals would disregard alerts in personal computing. Khansa et al. [30] investigated employees' cyberloafing behavior and its antecedents after an announcement of formal organizational controls.

In terms of the coping mechanisms, Twyman et al. [58] proposed an autonomous scientifically controlled screening system and examined its detection function on individuals' purposely hidden information. Hsu et al. [22] clarified and examined the importance of extra-role behaviors and social controls in employees' compliance to organizational ISP. Johnston et al. [29] explored the effectiveness of an enhanced fear appeal rhetorical framework eliciting a compliance response significantly greater than that produced by contemporary usage of fear appeals. Vance et al. [60] found that the perceived accountability of users could be heightened by the UI design of broad-access systems and further reduced their intentions to violate access policies. Wang et al. [63, 64] showed how to foresee applications' risk from illegal access of insiders through the applications' characteristics. Tsohou et al. [57] proposed a framework to help security managers design and implement ISec awareness programs by treating security awareness as a change process. Posey et al. [48] investigated the effect of organizational commitment levels of insiders on threat coping behavior, considering the interconnection of threat and coping appraisal via perceived response cost. Warkentin et al. [65] examined the neurological experience of insiders when faced with fear appeals. Steinbart et al. [55] focused on what influences users' (dis)continuance of adopting security behavior from the perspective of UI design. Wang et al. [62] examined the coping response mechanism of employees in the process of phishing email detection.

4.3 Threat Mitigation

Threat mitigation is concerned with network segmentation (e.g., network security infrastructure, intrusion detection, and remote access), vulnerability management (e.g., scanning, patching, and standard operating procedures), content checking (e.g., data filtering and virus protection), and incident management issues (e.g., forensics and event correlation). Related reviewed papers are summarized as follows.

In terms of vulnerability management, Wright et al. [69] explored why certain influence techniques are especially dangerous when used in phishing attacks, which helped identify this type of vulnerability. Guo et al. [18] explored the propagation process of malware using a structural risk model. Sen and Borle [50] examined some public policies, such as public disclosure of vulnerabilities, IT security investment, and data breach laws, would influence the data breach risk for a state and for organizations within an industry. Chen and Zahedi [11] considered the effect of cultural difference on security behaviors based on context-sensitive theory. Li et al. [36, 37] found that organizational justice and personal ethics are two effective levers to mitigate the risk of violation of IUP. Wang et al. [62] suggested that emotion-focused coping of employees and avoidance coping in phishing email coping will cause vulnerability. Jenkins et al. [25] found that alerts pervasive in personal computing will create vulnerability if they are not bounded in their presentation.

In terms of content checking, Zahedi et al. [71] explained how user's reliance on detection tools is influenced by their performance and cost. Ho et al. [21] demonstrated that deceivers would use different language–action cues in different contexts. Siering et al. [51] derived different linguistic and content-based cues that were used as input for various fraud detection classifiers. Li et al. [38] developed advanced text mining techniques to analyze multilingual textual traces in underground economy and identify key international underground economy sellers. Liang et al. [40] examined and validated several characteristics, which could be used to identify malicious insiders.

In terms of incident management, Goode et al. [17] explored how a breached organization could best determine the optimal level of customer compensation in response to data breach, which is about incident management. Choi et al. [12] developed a model to show how firms' recovery measures influence customers' behavior online after data breach. Angst et al. [3] examined whether the manner in which regulation rules were adopted (i.e., symbolic and substantive) had a moderation effect on the relationship between IT security investments and follow-up data security breaches. Jensen et al. [26] found that participants who received mindfulness training could better avoid the phishing attack that those who did not. Mitra and Ransbotham [43] explored the relationship between two types of information disclosure (i.e., full and limited) and the diffusion of ISec attacks.

4.4 ISec Economics

Some scholars have argued that the focus of IT security management is shifting from what is technically possible to what is economically efficient. ISec economics refers to using economic theory in handling ISec decisions, such as the ISec investment and consumer choice. The former is about how an organization makes decision on ISec investment based on the return and loss without investment. The latter explores how transaction security can be enhanced from the economics perspective to increase the transaction intention of consumers. Related reviewed papers are summarized as follows.

Lee et al. [35] investigated how firm security would be influenced by a government's standard, especially when verifiable and unverifiable controls on security concerns are available. August et al. [4] explained how a software vendor approaches the versioning problem and how consumers separate across product variants to diversify security risk when both SaaS and on-premises versions are available. Choudhary and Zhang [13] explored the impact of a change in the distribution of defect-related costs on the release time of vendors and patching strategy under SaaS. Sen and Borle [50] examined some public policies (e.g., public disclosure of vulnerabilities, IT security investment, and data breach laws) that would influence the data breach risk for a state and for organizations within an industry. Ji et al. [27] analyzed a size-based security monitoring policy with and without profiling. Jensen et al. [26] developed a novel security training method given that some employees are used to training based on rules. Goode et al. [17] studied how a breached organization could best determine the optimal level of customer compensation in response to data breach.

4.5 Privacy

In this study, information privacy is assigned to the area of using privileged information with malicious intent, which includes the following parts: (1) Policy, practices, and controls. This part includes development of taxonomies, as well as rule definitions, impact assessments, and awareness and training: (2) Privacy and information management strategy. This assessment includes description of privacy information strategies, requirements, and compliance processes, as well as incident response situations: (3) Data, rules, and objects. This part includes the development of classification and/or business process models. Related reviewed papers are summarized as follows.

Li and Sarkar [39] proposed a dynamic value-concatenation method for data privacy protection and data quality preservation for application. Oetzel and Spiekermann [46] adopted a privacy impact assessment method in considering privacy issues systematically. Wall et al. [61] introduced a selective organizational rule violation model into the contexts of organizational privacy and security. Parks et al. [47] evaluated the intended and unintended consequences of implementing privacy safeguards and their impacts on organizational privacy compliance. Goode et al. [17] investigated how a breached organization could best determine the optimal level of customer compensation in response to data breach. Choi et al. [12] developed a model showing how firms' recovery measures influence customers' behavior online after data breach. Angst et al. [3] examined whether symbolic and substantive adoption would moderate the effect that IT security investments had on reducing the incidence of data security breaches over time.

4.6 Transaction and Data Integrity

Transaction and data integrity is concerned with business process transaction security (e.g., fraud detection and transaction security), database security (e.g., configuration and control), message protection (e.g., encryption and message security), secure storage (e.g., data storage, archiving, retrieval, and destruction), and system integrity (e.g., secure system management and business continuity planning). Six papers we reviewed have been identified as the following.

Li and Sarkar [39] proposed a dynamic value-concatenation method that could protect data privacy while preserving data quality for application. Kim et al. [31] indicated that cultural difference is an important element in designing e-commerce websites and security protection for multinational companies for a worldwide audience. Bhattacherjee and Park [7] explained why users move from client-centric computing to cloud computing. Herath et al. [20] explored users' intention to adopt an email authentication service. Siering et al. [51] derived different linguistic and content-based cues used as input for various fraud detection classifiers, which helped identify the fraud. Li et al. [38] developed advanced text mining techniques to identify the key sellers in Cyber Carding Community.

4.7 Identity and Access Management

This part includes identity proofing through background screening and alternative methods of credential management. Identity access management focuses on identifying users, protecting confidential information from unauthorized users, and providing authorized users secure and controlled access to resources. Related reviewed papers are summarized as follows.

Steinbart et al. [55] showed that poor performance (login failures) of identity authentication resulted in discontinuance of a secure behavior and the adoption of less-secure behaviors. Vance et al. [60] found that the perceived accountability of users could be increased by the UI design of broad-access systems and further reduced their intentions to violate access policies. Roßnagel et al. [40] examined whether individuals would like to pay when using federated identity management. Herath et al. [20] investigated users' intention to adopt an email authentication service.

4.8 Application Security

An application security assessment entails code review, secure coding practices, and secure policies and procedures to manage SDLC (Systems Development Life Cycle). Preventing a security error is generally less costly than fixing it once it occurs. SDLC includes procedures that ensure security throughout its process. In papers we reviewed, only one pertained to application security. Sojer et al. [53] explored the drivers of unethical programming behavior by individuals in the processes of systems development.

4.9 Physical Security

Security is not an issue that can exclusively be handled with software. Requirement for physical barriers exists as well. Physical security describes the measures taken to protect facilities from potential attackers. In the IBM model, two topics are considered, namely, site management and physical asset management. No reviewed papers have discussed this theme, which can be explained that this topic related to other disciplines. Furthermore, other physical security concerns will emerge with the development of artificial intelligence. IoTs will force various intelligent devices, which may expose organizations to new vulnerabilities. For this reason, we retained this theme in our discussion.

5 Recommendations

To some extent, the identification of research streams based on IBM security model can help us learn about the relationship of ISec research and industry requirements. However, the next steps for industry and research communities still need further study. Thus, on the basis of existing literature, we focused on four objects in organizations, namely, data, human behavior, business processes, and IT/IS, as shown in Fig. 3. From the dynamic view, we considered the interaction between two objects. An organization can make policies to manage each flow to minimize security risk. Based on this framework, some main findings in existing research are summarized, and the recommendations for industry and research communities are discussed and provided.

We will explain each object and then consider the flow or interaction between them. First, we define data as the core object in the process of business digitization and therefrom ISec management. Data of organizations include the internal and external data that mainly originate from two sources, namely, human behavior related and business processes related, such HER of patients [33], online customer behavior data [12], and organizational operation and financial data [35]. Organizations should consider using which type of IS/IT to record, store, transfer, and protect data while

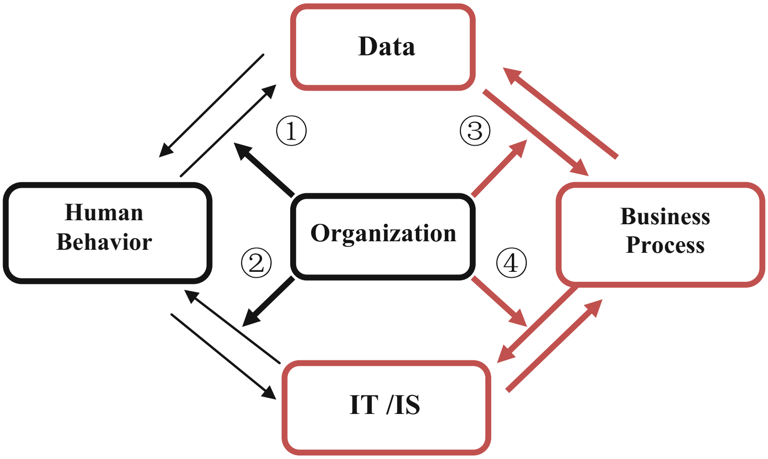

Fig. 3 Proposed ISec research framework in the process of business digitization

restraining human behavior (insiders and consumers) and encrypting the business process to protect data security; thus, these three objects are considered as another three objects.

Determining the IT/IS that supports and accomplishes the business process (e.g., OA, ERP, and CRM) with the IT/IS protection security (e.g., firewall technology, intrusion detection system, proxy servers, and virtual private networking) is necessary. The former is the infrastructure of digital businesses, and its vulnerability raises new threats to organizations [43]. Hence, the latter is designed and deployed to protect the former. Data are flowing in the system, and insiders should follow standard system usage.

Two main types of human behavior are considered by organizations, namely, insiders and consumers (users). The former is considered among the greatest threats to organizational ISec [42]. Insiders' violation to ISPs has caused great loss to organizations, and consumers' insecurity behavior also expose organizations to the threats. Moreover, consumer behavior will generate the data collected and analyzed by organizations to make managerial decisions, which is the main component of digital businesses. However, the illegal usage of collected behavioral data is an increasing concern for consumers.

With regard to the business processes considered as the core object in this study, we adopted the definition from Wikipedia, "Business process is a collection of related, structured activities or tasks that produce a specific service or product (serve a particular goal) for a particular customer or customers." This definition is closer to that of operational processes rather than the management and supporting processes. Operational processes are the core business and realize the primary value stream, such as opening an account in a bank after taking orders from customers. However, management processes, which mainly include "corporate governance" and "strategic management" govern systems operation. Supporting processes include health and safety, accounting, recruitment, call center, and technical support.

The development of organizational business process management (BPM) involves three stages. The first stage started with advances in the data-driven methods. In this stage, data storage and retrieval technologies have made great progress. Most of the IS was developed with data-modeling method; thus, BPM had to adapt to the system neglecting business processes. BPM reached the second stage with the emergence of various enterprise resource planning software in the 1990s, when the business-process-oriented management system increasingly dominated the market. In the third stage, e-businesses, which benefitted from the development of internet technologies, realized the automated business processes across organizations. This automated process created a platform that integrated sellers and buyers online and promoted collaboration and integration of people, systems, processes, and information within and across enterprises.

Currently, some newly emerged information technologies, such as cloud computing, social network, mobile technology, and big data analytics, are reforming BPM. For example, cloud computing technology has significantly increased the computing power of companies with low cost and has eliminated the restraint of location. Social media and smartphones have produced new channels for organizations to reach their

Table 4 Summary of recommendations for information security research

Directions	Suggestions for researchers	Suggestions for organizations	Related themes in IBM security model

Interaction between data and human behavior	1. Before data breach, how to encourage compliance from the perspective of positive employee
	2. After data breach, how to conduct repair strategy
		1. Watching out for the side effect of enhanced ISPs
		2. Balance between compensation and over-compensation
			Governance;
			Personnel security;
			Privacy

Interaction between human behavior and IT/IS	1. For employees: emotions' effect on unethical IT usage behavior
	2. For consumers: dual effect of IT/IS used for security protection on transaction behavior
		1. Pay more attention to users' emotional management
		2. Balance between security protection measures and interference
			Governance;
			Personnel security;
			Threat mitigation;
			Identity and Access management

Interaction between IT/IS and business process	1. Data analytics technologies used for business fraud detection
	2. Information security economics used for security investment researches
		1. More IT security investment doesn't mean more security, especially in complex system	Governance;
			Application security;
			Physical security;
			Information security economics

Interaction between business process and data	1. How to jump out of the dilemma: privacy protection and personalized service 2. How to choose a suitable data view: right or commodity	1. New data analytics method need to be developed 2. Cross-order transaction should consider the different privacy view hold by two trading parties	Governance; Transaction and data integrity

customers. Various customer data collected through these channels have led to a significant growth in business analytics based on big data technologies, which can help managers to make effective managerial decisions and serve their customers well.

To sum up, business processes must reconsider its relationship with IT/IS and data. In the following, we proposed four directions by examining the interactions between different objects to identify the potential research opportunity for subsequent researchers and provide some suggestions to industry community based on 59 reviewed papers in this chapter (Table 4).

5.1 *Interaction Between Data and Human Behavior*

For the interaction between data and human behavior, data generation based on consumer behavior and data protection conducted by employees are two important themes to consider. For data generation, consumers worry about data security and they may give up accepting services especially when they do not believe the organization. Kohli and Tan [33] claimed that patients' privacy calculus may impact their EHR data sharing. Failure to protect consumer data and prevent privacy breaches can cause great damage to the reputation and finances of a company [46]. Considering the leaked behavior of organizations, except for organizational malicious leaked behavior, Wall et al. [61] demonstrated that organizations intentionally choose to violate users' data security protection rules required by the government to decrease the excessive cost of safety protection. With the increasing cases of privacy breach, some researchers have begun to explore how a breached organization can decide on customer compensation after a data breach and retain their consumers [12, 17].

For data protection, employees' compliance to ISPs has been an extremely popular topic. Among the 59 papers we reviewed, 28 papers have referred to this topic [9, 14, 16, 22, 28–30, 36, 37, 40, 41, 48, 57, 62, 65]. Data breach resulting from insiders' security policy violation behavior can be seen as the unintentional leaked behavior of organizations. Although organizations often develop various policies to restrain employees' behavior [16], most of the security losses are caused by such behavior.

5.1.1 Suggestions for Researchers and Organizations

Before data breach: Paying attention to the side effect of enhanced ISPs
ISPs can significantly improve organizational security situation. However, researchers are increasingly realizing that excessive ISPs has brought "security-related stress" to employees [14]; thus, employees react negatively and even retaliate against the organization by intentionally violating enhanced ISPs [41, 42]. Some scholars have explored solutions to this phenomenon. Balozian and Leidner [6] argued that well-justified security additions are useful to improve employees' attitude to enhanced ISPs. Hsu et al. [22] suggested that the extra-role behavior of employees should be emphasized and that social control from colleagues can complement the formal ISPs of organizations. Researchers have set an inappropriate assumption about negative employees. Organizations keep increasing their ISPs because they think that employees often attempt to violate policies. On the basis of the effect of enhanced ISPs, researchers can eliminate this assumption and explore how to encourage employees' compliance to ISPs from the perspective of positive employees. Organizations should be careful in introducing new ISPs by using suitable methods. Employees will be irritated and react negatively if managers ignore their rights and freedoms as humans when introducing potentially freedom-restricting policies [41]. Respect and fairness are two basic factors that organizations should show to employ-

ees [42]. If necessary, providing sufficient justification of the enhanced policies is suggested.

After data breach: more attention to repair strategies
When data breach happens, organizations have to respond to it even if a great damage has already occurred. Existing service failure literature has shown that effective repair strategies play an important role in retaining consumers and improving their repurchase intention. Therefore, exploring effective repair strategies after data breach is necessary. In our reviewed papers, only two papers have focused on this question [12, 17]. Based on Sony's data breach case, Goode et al. [17] presented an adapted model to explain customer responses to a data breach recovery action. Organizations should provide compensation depending on breach severity; however, overcompensation is not a good idea. With the advent of social media, researchers have been interested in exploring how customers spread comments (positive and negative) in their social network after data security breaches and how spreading of data breach will influence organizational compensation packages and outcomes.

5.2 Interaction Between Human Behavior and IT/IS

With regard to the interaction between human behavior and IT/IS, we initially considered the security concerns in the process of IT/IS usage. In this perspective, we identified the unethical IT usage behavior in the literature. Four reviewed papers discussed this topic [10, 30, 53, 55]. However, IT/IS can be also regarded as tools to be used to detect malicious user behavior and monitor employees' behavior. In this perspective, developing a detection system has been a popular research topic [21, 23, 58], including UI design [1, 2, 55, 60]. In addition, Neuro IS technologies are increasingly adopted by IS scholars [1, 2, 25].

How to adopt countermeasures according to different unethical IT/IS usage behaviors?
To decrease the vulnerability of organizational IS, taking effective measures is necessary to respond to different unethical behaviors of employees. Unethical IT usage behavior is complex, and Chatterjee et al. [10] found that it would be influenced by a wide range of individual, philosophical, social, economic, and technological factors. Three different unethical IT usage behaviors, namely, malicious, intentional but not malicious, and unintentional, are identified to address unethical IT usage behavior effectively. For unintentional unethical IT usage behavior, enhancing user's risk awareness of their behavior by SETA programs is necessary [57]. For example, cyberloafing behavior of employees is a representative type of behavior; it exposes the organization to internet threats. Khansa et al. [30] found that cyberloafing behavior is mainly influenced by past tendencies to cyberloaf and others' influence. Organizations can significantly decrease this behavior by adopting formal controls (e.g., penalty). Steinbart et al. [55] also found that employees' habits on technology usage in daily life would carry over to the workplace, which shows the importance of secu-

rity awareness training. For intentional but not malicious unethical IT usage behavior, sanctions are more effective [10]. For example, for unethical programming behavior as a representative of this type of behavior, Sojer et al. [53] explored its drivers and encouraged firms to prevent it by informing developers of its negative consequences. Finally, for malicious unethical IT usage behavior, identifying and minimizing it by security training or sanction controls is difficult, especially when users pretend to follow organizational ISPs. To address these problems, some scholars have attempted to develop or adopt different IT/IS to detect this behavior. This topic is discussed as follows.

How to develop/adopt IT/IS to deal with security concerns related to human behavior?
The perspective of IT/IS as infrastructure supporting business process has changed to IT/IS as tools identifying insecurity behavior or enhancing security behavior intention. For example, Twyman et al. [58] proposed autonomous scientifically controlled screening systems that can detect information hidden by individuals. Hu et al. [23] proposed a new paradigm based on event-related potentials that can be used to identify individual violations of ISPs based on their self-control difference. Moreover, Ho et al. [21] found that specific language–action cues influenced by context can be used to identify computer-mediated deception. In addition, Neuro IS technologies, such as fMRI and eye movement-based memory, have been adopted by scholars to learn individuals' real intention based on their physiological change when exposed to security risk or warning/alerts of organizations [1, 2, 25, 59]. Aside from using IT/IS to identify insecurity behavior, UI design is developed to help users continue to adopt security behavior [55] and not to violate access policies [60]. This complementary measure is suggested because it can target repetition suppression in users' brain, such as the polymorphic warning, which can elicit positive effect in milliseconds without additional cost [1].

5.2.1 Suggestions for Researchers and Organizations

For employees: effect of emotions on unethical IT usage behavior
Most of the existing studies are from the perspective of rational behavior, which is based on PMT [9, 48] and deterrence theory [16, 25] without fully considering the emotion of individuals, such as rage, anger, and despair. However, an increasing number of scholars have realized that the emotional state of individuals is an important foundation for them to make rational decisions. Formal sanctions will be effective for individuals who perceive low to moderate level of anger, but neither formal nor informal sanctions will lose efficacy on individuals who perceive high level of anger. Willison and Warkentin [67] indicated that a new stream of research for the IS security field is to examine the relationship between emotions and deterrence. For example, will organizational injustice result in negative emotions or will this emotion further influence individuals' unethical IT usage behavior as revenge [42]? Do emotions moderate the effect of threat of sanctions on unethical IT usage

behavior or does the extent of emotions play different roles? Organizations should pay more attention to employees' emotion management to ensure the efficacy of the ISPs, especially with sanctions.

For consumers: dual effect of IT/IS used for security protection on transaction behavior
Although enhanced security protection for consumers is adopted by organizations, unexpected results are identified. Kim et al. [31] found that perceived effectiveness of web assurance seal services (WASS) from organizations would influence the transaction intention of American consumers. Steinbart et al. [55] claimed that UI design in mobile paradigm would influence login success rates, which would further result in consumers' discontinuance of a secure behavior. When consumers feel that their consumption is interrupted by over-security measures, they may become impatient and discontinue shopping. Jenkins et al. [25] conducted behavioral experiment using fMRI and found that the presentation of alerts should be carefully controlled because the timing of interruptions strongly influences alert disregard. To sum up, existing research actually requires a balance between IT/IS used for security protection and interference brought by these IT/IS. Although security protection is beneficial to consumers, consumers may still perceive disturbance by excessive and fussy authentication. This phenomenon can be explained by the "dual-task interference" (Anderson et al. [1], which indicates that multitasking is difficult for people. Consumers find it difficult to shop while passing security validation. Thus, designing some IT/IS to protect consumers' security with least interference is challenging. In addition, new IT may bring more complexity to manage consumers' security behavior. For example, since the emergence of mobile technology, more consumers use mobile devices to shop instead of their computers. However, security policies effective on desktop computing paradigm will not work in the mobile paradigm [2].

5.3 Interaction Between IT/IS and Business Process

New emerging IT/IS will be adopted to support business processes at the cost of new channels of vulnerabilities to be exposed to security threat, such as cloud computing [7]. However, new business processes or models based on new IT/IS also trigger new types of attacks, such as business fraud [51], phishing [62, 69], malware propagation [18], and underground economy sellers [38], which urge matched IT/IS investment to provide security protection.

5.3.1 For New IT/IS-Enabled Business Process

Security concerns emerge mainly depending on the characteristics of new business processes or models. Based on reviewed papers, we show different security concerns that occur in different IT/IS-enabled business processes. The first is about the cloud computing service. Cloud service can provide users with universal access to cloud-hosted resources and processing power with low cost [7]. However, the cloud service provider will easily attract and receive denser attacks from hackers. For example, SaaS is a type of business application of cloud computing. August et al. [4] pointed out that the SaaS versioning of software has relatively higher directed risk than the traditional on-premises version because one vulnerability of the SaaS is letting a malicious attacker affect many organizations using this SaaS all at once. Second, for crowdfunding platforms that provide possibility for project realization even with lack of fund, their drawback is the rising risk of fraud related to the project campaigns prevalent on these open online services. Given that project founders often only have project ideas without the actual product during the funding period, judging the legitimacy of the project is difficult [51]. Third, for underground economy, such as Cyber Carding Community, the development of internet technologies and illegal business application of internet also call for solutions. In addition, cross-border e-commerce websites can realize the transaction among different countries online, which greatly reshapes the international business model. However, the cultural differences should be considered to design website authentication in this context. Kim et al. [31] found that the effectiveness of WASS influences transaction intention of US consumers but not Korean consumers. Email has become a daily used business communication software. However, email phishing attack has caused great loss to organizations [62]. Herath et al. [20] explored how to increase the adoption of an email authentication service by controlling this risk to organizations. Finally, malware propagation is also one top security challenge in business processes [18].

5.3.2 For Security Investment on IT/IS for New Business Process

New business processes emerging with new IT/IS expose organizations to new security risk. Therefore, organizations must adopt enhanced or targeted security protection measures. One important topic in this part is organizational security investment decision on IT/IS. When considering security investment, rules of the government will have some restraints on organizational decisions. Angst et al. [3] found that the effectiveness of IT security investments would be weakened by symbolic adoption of government rules and further increase the risk of data breach in business processes. The notion of buying more (and even more expensive) defense technologies and systems is held by many organizations. Companies think that the quantity of security protection technologies will increasingly improve their security of business processes. However, Wolff (68) claimed that more is not always better, especially in defending a complex system. New and unpredictable vulnerabilities will be produced by interactions among different components of system and defense mechanisms. Adding defenses to this type of complex system can actually undermine its security.

5.3.3 Suggestions for Researchers and Organizations

Data analytics technologies used for business fraud detection
IT/IS-enabled business processes show all types of new security threats faced by organizations, especially business fraud detection. To fill this gap, data analytics technologies should be adopted. In our reviewed papers, some scholars have attempted to pioneer. For example, data mining method was adopted by Siering et al. [51] to detect the fraudulent behavior on a crowdfunding platform. Results showed that different linguistic and content-based cues can be used to identify fraud in business processes. Li et al. [38] also developed a novel system using advanced text mining techniques to analyze multilingual textual traces in the underground economy and further identify key sellers. Guo et al. [18] conducted an analysis on the propagation process of malware with social network data. As suggested by Li et al. [38], the question of how to use hacker community data to inform cybersecurity intelligence remains open as hackers increasingly congregate in their communities. Leveraging social media analytics to probe into business fraud awaits further exploration.
ISec economics used for security investment research
Based on the above discussion on security investment of organizations, one important potential research direction is the perverse effects of security investment. Although, taxonomy for the sources of different perverse effects in security has been proposed by Wolff [68], several questions have been opened. What types of defenses cause these effects in practice and why? What is best action to avoid or counteract them? Future research in this area can further elaborate Woff's understanding of when and why perverse effects arise in defending computer systems in business processes and how they may be most effectively mitigated. Organizations' new security investment to protect IT/IS should be reviewed not only for their individual impact but also for their interactions with other system components and usability features.

5.3.4 Interaction Between Business Process and Data

The final and most important type of interaction we considered is the interaction between business process and data. This interaction produces at least two themes. One is the data-driven business process, and the other is data generation and protection in business processes.

5.3.5 For Data-Driven Business Processes: A Dilemma

With data increasingly used for managerial decision, traditional business processes, such as product design, marketing, and customer management, have been reshaped by data and reached the digital business. However, data-driven business processes also bring new challenges to organizations. One important topic is how to keep the balance between privacy protection and personalized service based on analysis of personal data. For example, recommended systems are adopted by an increasing number of companies to analyze the demand of customers and then recommend goods or service to customers. However, whether consumers will feel invaded when they received the recommendation has been one difficult question to answer. Privacy-related paradox has been noticed by some scholars [5, 34, 54, 56], that is, organizations face a dilemma where consumers want to share the benefit of data-driven recommendation but not willing to share their data because of privacy concerns.

5.3.6 For Data Protection in Business Process: Illegal Data Usage and Data Breach

Based on the dilemma discussed above, data-driven business processes have the potential orientation to privacy invasion. For organizations, all types of data protection technologies are required to be deployed to increase consumers' trust and respond to government rules [31]. The effectiveness of IT investment has been discussed in the part of "interaction between IT/IS and business processes." Similarly, if data breach is detected, organizations also need to provide compensation to consumers, as mentioned in the first type of interaction. In this part, we discuss the effect of business decision on data sharing with the restraint of government rules. For example, Mitra and Ransbotham [43] focused on organizational decision on information disclosure of vulnerability and found that full disclosure would lead to greater risk than limited disclosure. Furthermore, Sen and Borle [50] found that the risk of data breach would be significantly influenced by the strictness of laws on data breach disclosure. Moreover, when adopting the commercial perspective of the concept of privacy, privacy will be seen as a type of goods to be traded [54]. For example, when considering the data transforming healthcare, privacy calculus is argued to influence patients' data sharing [33].

5.3.7 Suggestions for researchers and organizations

How to jump out of the dilemma: Innovation on data analytics method
The above discussion on data-driven business processes show the dilemma organizations face. Potential solution still needs to be determined from data analytics itself. For example, regression tree is a type of data analytics method but it can also be used as a tool for mining personal information, such as regression attacks [39]. To address this problem, Li and Sarkar [39] developed a new dynamic value-concatenation method approach. This approach can ensure the quality of data while avoiding privacy infringement. Therefore, this type of data analytics methods should be further studied although it may take a long for researchers. This type of method will encourage customers to share their data without worrying about privacy and then share the benefit from the personalized service.

How to choose a suitable data view: Effect of cultural difference on privacy concerns in business process

Privacy calculus is another way to deal with the organizational dilemma because organizations can buy the personal data when consumers accept the notion of privacy as goods. Thus, an increasing number of scholars has been interested in privacy calculus to some extent. However, one underlying question is whether considering cultural difference is reasonable and applicable. This topic is meaningful with the development of cross-border e-commerce and cross-national companies, especially in the management discipline. Smith et al. [54] summarized two value-based privacy views, namely, privacy as a right and privacy as a commodity, and presented the dissonance between US and European privacy laws. Europe tends to see privacy as more of a property right by consumers compared with the US. When cross-border transaction occurs between countries in Europe and the US, problems may emerge without fully considering the cultural difference. Therefore, further research, which focuses on this question and explores guidelines for organizations, is suggested.

6 Limitations

First, although we have explained that we made a conscious decision to prioritize quality over quantity, we only considered six journals. Thus, more journals are encouraged to be considered. Second, although we analyzed each paper carefully according to the assessment of IBM themes, some subjective assignments are admitted to be inevitable. Moreover, the security model of IBM selected as the representative of industry requirement may ignore some ISec themes or consider other themes (e.g., physical security) that are closer to other disciplines, such as computer science. Hence, determining a suitable security model of industry is encouraged. In addition, we only considered four types of interaction of the four objects because of their relative importance. Other types of interaction also deserve consideration, especially the interaction among three of four objects. Finally, given that big data analytics have developed mainly in the past five years, we only reviewed papers published from 2014. However, expanding the term of our review is also encouraged.

7 Summary and Conclusions

In this chapter, we reviewed ISec research published in MISQ, ISR, JMIS, JAIS, EJIS, and ISJ from 2014 to 2107 and coded each paper into one or more themes of IBM security model. Then, we evaluated the relationship between ISec academic research and ISec industry requirement. Some increasingly popular themes, such as privacy, threat mitigation, and transaction and data integrity, for IS researchers were specified, and four objects related to ISec in organizations were identified. By further coding each paper into one or more objects, we considered the interaction between two objects. Based on each type of interaction, some suggestions for IS researchers and organizations were provided. Based on the topic of this book chapter, we strongly recommend that researchers and organizations pay more attention to the interaction between IT/IS and business processes, and interaction between business processes and data. Both these interactions represent the process of business digitization, from which some security topics are worth to be further explored, especially in the digital era.

Appendix

Appendix: Coded Articles: literature Classification/Theory/Method/Research objects related in each paper

Articles	Themes of IBM security model								
	Governance	Privacy	Threat mitigation	Transaction and data integrity	Identity and access management	Application security	Physical security	Personnel security	Information security economics
Total (59)	50	7	18	6	4	1	0	28	8
1. Wright et al. [69]	√		√					√	
2. Lee et al. [35]	√								√
3. Hsu et al. [22]	√							√	
4. Wang et al. [63, 64]	√							√	
5. August et al. [4]	√								√
6. Steinbart et al. [55]	√				√			√	
7. Mitra and Ransbotham [43]	√		√						
8. Choudhary and Zhang [13]	√								√
9. Johnston et al. [29]	√							√	
10. Han et al. [19]	√								
11. Kim and Kim [32]	√								
12. Li and Sarkar [39]		√		√					
13. Vance et al. [60]	√				√			√	

(continued)

(continued)

Appendix: Coded Articles: literature Classification/Theory/Method/Research objects related in each paper									
Articles	Themes of IBM security model								
	Governance	Privacy	Threat mitigation	Transaction and data integrity	Identity and access management	Application security	Physical security	Personnel security	Information security economics
Total (59)	50	7	18	6	4	1	0	28	8
14. Chen and Zahedi [11]	√		√						
15. Wang et al. [63, 64]	√							√	
16. Boss et al. [9]	√							√	
17. Guo et al. [18]	√		√						
18. Ho et al. [21]			√					√	
19. Wolff [68]	√								
20. Hu et al. [23]	√							√	
21. Chatterjee et al. [10]	√							√	
22. Posey et al. [48]	√							√	
23. Sen and Borle [50]	√		√						√
24. Twyman et al. [58]								√	
25. Sojer et al. [53]	√					√		√	
26. D'Arcy et al. [14]	√							√	
27. Johnston et al. [28]	√							√	
28. Oetzel and Spiekermann [46]	√	√							
29. Tsohou et al. [57]	√							√	
30. Roßnagel et al. [49]					√				
31. Anderson et al. 2016	√							√	
32. Foth [16]	√							√	
33. Kim et al. [31]				√					

(continued)

(continued)

Appendix: Coded Articles: literature Classification/Theory/Method/Research objects related in each paper

Articles	Themes of IBM security model								
	Governance	Privacy	Threat mitigation	Transaction and data integrity	Identity and access management	Application security	Physical security	Personnel security	Information security economics
Total (59)	50	7	18	6	4	1	0	28	8
34. Siponen and Vance [52]	√								
35. Bhattacherjee and Park [7]	√			√					
36. Warkentin et al. [65]	√							√	
37. Wall et al. [61]	√	√							
38. Zahedi et al. [71]			√						
39. Vance et al. [59]	√								
40. Herath et al. [20]				√	√				
41. Li et al. [36, 37]	√		√					√	
42. Lowry et al. [42]	√							√	
43. Lowry et al. [42]	√							√	
44. Wang et al. [62]	√		√					√	
45. Siering et al. [51]			√	√					
46. Parks et al. [47]	√	√							
47. Niemimaa and Niemimaa [45]	√								
48. Liang et al. [40]			√					√	
49. Li et al. [38]			√	√					
50. Kohli and Tan [33]			√						
51. Khansa et al. [30]	√							√	
52. Ji et al. [27]	√								√

(continued)

(continued)

Appendix: Coded Articles: literature Classification/Theory/Method/Research objects related in each paper

Articles	Themes of IBM security model								
	Governance	Privacy	Threat mitigation	Transaction and data integrity	Identity and access management	Application security	Physical security	Personnel security	Information security economics
Total (59)	50	7	18	6	4	1	0	28	8
53. Jensen et al. [26]	√		√						√
54. Jenkins et al. [25]	√		√					√	
55. Hui et al. [24]	√								√
56. Goode et al. [17]	√	√	√						√
57. Choi et al. [12]	√	√	√						
58. Angst et al. [3]	√	√							
59. Anderson et al. [1, 2]	√		√					√	

(continued)

(continued)

Appendix: Coded Articles: literature Classification/Theory/Method/Research objects related in each paper

Theoretical basis	Methodology method	Objects related			
		Data	Business process	Technology/system	Human behavior
		10	16	24	43
Persuasion theory; motivation theory	Experiment				√
Game theory	Modeling	√			
Social control theory	Survey				√
Information foraging theory	Survey				√
Microeconomic theory	Modeling		√		√
Protection motivation theory (PMT) Technology threat avoidance theory (TTAT)	Experiment			√	√
Diffusion of innovation	Modeling		√	√	
Microeconomic theory	Modeling		√		√
Protection motivation theory, deterrence theory	Interview; Experiment				√
(Etzioni's) Compliance theory	scenario-based survey				√
Theory of knowledge retention	Modeling		√	√	

Appendix: Coded Articles: literature Classification/Theory/Method/Research objects related in each paper

Theoretical basis	Methodology method	Objects related			
		Data	Business process	Technology/system	Human behavior
		10	16	24	43
K-anonymity framework; regression tree	Algorithm; Experiment	√		√	
Accountability theory	Factorial Survey			√	√

(continued)

(continued)

Appendix: Coded Articles: literature Classification/Theory/Method/Research objects related in each paper					
Theoretical basis	Methodology method	Objects related			
		Data	Business process	Technology/system	Human behavior
		10	16	24	43
Context sensitive theory; TTAT; PMT; coping theory	Survey				✓
Routine activity theory	Modeling				✓
Protection motivation theory (PMT)	Reviewing; Experiment				✓
Social network analysis	Modeling			✓	
Interpersonal deception theory; social distance theory; media richness theory	Algorithm; Modeling			✓	✓
Theory of unintended consequences	Case study			✓	
Self-control theory	Experiment				✓
Theory of planned behavior (TPB); Universal philosophical theories of ethics	Scenario-based survey		✓		✓
Protection motivation theory	Survey				✓
Opportunity theory of crime, Institutional anomie theory; institutional theory	Modeling	✓	✓		
Orienting theory, defensive response theory	IS development			✓	✓
Theory of planned behavior model; expected utility, deterrence, and ethical work climate theory	Survey			✓	✓
Coping theory; moral disengagement theory Social cognitive theory	Survey				✓

(continued)

(continued)

Appendix: Coded Articles: literature Classification/Theory/Method/Research objects related in each paper

Theoretical basis	Methodology method	Objects related			
		Data	Business process	Technology/system	Human behavior
		10	16	24	43
PMT; general deterrence theory	Survey				√
Privacy impact assessment (PIA)	Approach Development	√		√	
Actor-network theory (ANT), Structuration theory; Contextualism	Action research				√
Economic theory	Modeling; Experiment			√	√
	Experiment			√	√
TPB; general deterrence theory	Survey				√
Cultural dimensions	Survey		√	√	√
	Case study				√
Migration theory	Survey		√		√
Fear appeal theory	Experiment			√	√
Selective organizational rule violations model; Strain Theory; general deterrence	Theory development	√	√		
PMT; detection tool impact (DTI) theory	Experiment			√	√
TPB; context-updating theory Dual-task interference theory	Experiment			√	√
TAM; TTAT; PMT	Survey			√	√
Justice theory; sanction theory	Survey				√
Organizational control theory reactance theory	Survey				√
Fairness theory; reactance theory deterrence theory	Survey				√
Extended parallel process model behavioral decision-making	Survey			√	√

(continued)

(continued)

Appendix: Coded Articles: literature Classification/Theory/Method/Research objects related in each paper					
Theoretical basis	Methodology method	Objects related			
		Data	Business process	Technology/system	Human behavior
		10	16	24	43
Four-factor theory; Leakage theory Verbal cues; Static Dynamic Linguistic Competence model of fraud detection Information manipulation theory Criteria-based content analysis Scientific content analysis Reality monitoring Channel expansion theory Interpersonal deception theory Interaction adaptation theory	Data mining/machine learning		√	√	
Grounded theory	Interpretive grounded theory	√	√		
Practice theory	Ethnography		√		
Trait theory	Text mining				√
Text mining technologies	Experiment; Case study		√	√	
	Integration -analytics technologies	√			√
Social learning theory	Survey				√
Traditional monitoring methods	Modeling			√	
Mindfulness theory	Design science				√
Functional magnetic resonance imaging (fMRI)	Behavioral experiment			√	√
General deterrence theory; routine activity theory	Modeling				
Expectation confirmation theory;	Longitudinal field study of Sony customers	√	√		√
Theory of justice; Psychological contract theory	Scenario-based survey	√	√		√
Institutional theory	A growth mixture model approach	√	√		
Habituation theory	Functional magnetic resonance imaging			√	√

References

1. Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., & 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), 364–390.
2. Anderson, B. B., Vance, A., Kirwan, C. B., Jenkins, J. L., & Eargle, D. (2016). From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems, 33*(3), 713–743.
3. Angst, C. M., Block, E. S., D'Arcy, J., & 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), 893–916.
4. August, T., Niculescu, M. F., & Shin, H. (2014). Cloud implications on software network structure and security risks. *Information Systems Research, 25*(3), 489–510.
5. Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13–28.
6. Balozian, P. Y., & Leidner, D. (2016. December). *IS security Menace: When Security Creates Insecurity*. Paper presented at International Conference on Information Systems, Dublin, Ireland.
7. Bhattacherjee, A., & Park, S. C. (2014). Why end-users move to the cloud: A migration-theoretic analysis. *European Journal of Information Systems, 23*(3), 357–372.
8. BongKeun, J., Kexin, Z., & Moutaz, K. (2012). Consumer piracy risk: Conceptualization and measurement in music sharing. *International Journal of Electronic Commerce, 16*(3), 89–118.
9. Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & 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), 837–864.
10. Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems, 31*(4), 49–87.
11. Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perception and behaviors: polycontextual contrasts between the United States and China. *MIS Quarterly, 40*(1), 205–222.
12. Choi, B. C. F., Kim, S. S., & Jiang, Z. (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems, 33*(3), 904–933.
13. Choudhary, V., & Zhang, Z. (2015). Patching the cloud: The impact of SaaS on patching strategy and the timing of software release. *Information Systems Research, 26*(4), 845–858.
14. D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(2), 285–318.
15. Forrest, C. (2016). Report: 80% of businesses can't properly manage external cyber attacks. Retrieved from http://www.techrepublic.com/article/report-80-of-businesses-cant-properly-manage-external-cyber-attacks
16. Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and deterrence. *European Journal of Information Systems, 25*(2), 91–109.
17. Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the sony playstation network breach. *MIS Quarterly, 41*(3), 703–728.
18. Guo, H., Cheng, H. K., & Kelley, K. (2016). Impact of network structure on malware propagation: A growth curve perspective. *Journal of Management Information Systems, 33*(1), 296–325.
19. Han, W. C., Ada, S., Sharman, R., & Rao, H. R. (2015). Campus emergency notification systems: An examination of factors affecting compliance with alerts. *MIS Quarterly, 39*(4), 909–930.

20. Herath, T., Chen, R., Wang, J. G., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24*(1), 61–84.
21. Ho, S. M., Hancock, J. T., Booth, C., & Liu, X. W. (2016). Computer-mediated deception: Strategies revealed by language-action cues in spontaneous communication. *Journal of Management Information Systems, 33*(2), 393–420.
22. Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research, 26*(2), 282–300.
23. Hu, Q., West, R., & Smarandescu, L. (2015). The Role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems, 31*(4), 6–48.
24. Hui, K.-L., Kim, S. H., & Wang, Q.-H. (2017). Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *MIS Quarterly, 41*(2), 497–524.
25. Jenkins, J. L., Anderson, B. B., Vance, A., Kirwan, C. B., & Eargle, D. (2016). More Harm Than Good? How messages that interrupt can make us vulnerable. *Information Systems Research, 27*(4), 880–896.
26. Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems, 34*(2), 597–626.
27. Ji, Y., Kumar, S., & Mookerjee, V. (2016). When being hot is not cool: Monitoring hot lists for information security. *Information Systems Research, 27*(4), 897–918.
28. Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems, 25*(3), 231–251.
29. Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113–134.
30. Khansa, L., Kuem, J., Siponen, M., & Kim, S. S. (2017). To Cyberloaf or Not to Cyberloaf: The impact of the announcement of formal organizational controls. *Journal of Management Information Systems, 34*(1), 141–176.
31. Kim, D. J., Yim, M. S., Sugumaran, V., & Rao, H. R. (2016). Web assurance seal services, trust and consumers' concerns: an investigation of e-commerce transaction intentions across two nations. *European Journal of Information Systems, 25*(3), 252–273.
32. Kim, S. H., & Kim, B. C. (2014). Differential effects of prior experience on the malware resolution process. *MIS Quarterly, 38*(3), 655–678.
33. Kohli, R., & Tan, S. S.-L. (2016). Electronic health records: How can IS researchers contribute to transforming healthcare? *MIS Quarterly, 40*(3), 553–573.
34. Lee, D. J., Ahn, J. H., & Bang, Y. (2011). Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection. *MIS Quarterly, 35*(2), 423–444.
35. Lee, C. H., Geng, X. J., & Raghunathan, S. (2016). Mandatory standards and organizational information security. *Information Systems Research, 27*(1), 70–86.
36. Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014a). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal, 24*(6), 479–502
37. Li, L., Gao, P., & Mao, J-Y. (2014b). Research on IT in China: A call for greater contextualization. *Journal of Information Technology*, *29*, 208–222.
38. Li, W., Chen, H., & Nunamaker, J. F., Jr. (2016). Identifying and profiling key sellers in cyber carding community: AZSecure text mining system. *Journal of Management Information Systems, 33*(4), 1059–1086.
39. Li, X. B., & Sarkar, S. (2014). Digression and value concatenation to enable privacy-preserving regression. *MIS Quarterly, 38*(3), 679–698.
40. Liang, N., Biros, D. P., & Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems, 33*(2), 361–392.

41. Lowry, P. B., & 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), 433–463.
42. Lowry, P. B., Posey, C., Bennett, R. J., & 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), 193–230.
43. Mitra, S., & Ransbotham, S. (2015). Information disclosure and the diffusion of information security attacks. *Information Systems Research, 26*(3), 565–584.
44. Ngai, E. W. T., & Wat, F. K. T. (2002). A literature review and classification of electronic commerce research. *Information & Management, 39*(5), 415–429.
45. Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems, 26*(1), 1–20.
46. Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: A design science approach. *European Journal of Information Systems, 23*(2), 126–150.
47. Parks, R., Xu, H., Chu, C.-H., & Lowry, P. B. (2017). Examining the intended and unintended consequences of organisational privacy safeguards. *European Journal of Information Systems, 26*(1), 37–65.
48. Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179–214.
49. Rossnagel, H., Zibuschka, J., Hinz, O., & Muntermann, J. (2014). Users' willingness to pay for web identity management systems. *European Journal of Information Systems, 23*(1), 36–50.
50. Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314–341.
51. Siering, M., Koch, J.-A., & Deokar, A. V. (2016). Detecting fraudulent behavior on crowdfunding platforms: The role of linguistic and content-based cues in static and dynamic contexts. *Journal of Management Information Systems, 33*(2), 421–455.
52. Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems, 23*(3), 289–305.
53. Sojer, M., Alexy, O., Kleinknecht, S., & Henkel, J. (2014). Understanding the drivers of unethical programming behavior: The inappropriate reuse of internet-accessible code. *Journal of Management Information Systems, 31*(3), 287–325.
54. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdiscipliary review. *MIS Quarterly, 35*(4), 989–1015.
55. Steinbart, P. J., Keith, M. J., & Babb, J. (2016). Examining the continuance of secure behavior: A longitudinal field study of mobile device authentication. *Information Systems Research, 27*(2), 219–239.
56. Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly, 37*(4), 1141–1164.
57. Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems, 24*(1), 38–58.
58. Twyman, N. W., Lowry, P. B., Burgoon, J. K., & Nunamaker, J. F. (2014). Autonomous scientifically controlled screening systems for detecting information purposely concealed by individuals. *Journal of Management Information Systems, 31*(3), 106–137.
59. Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems, 15*(10), 679–722.
60. Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly, 39*(2), 345–402.

61. Wall, J. D., Lowry, P. B., & Barlow, J. B. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems, 17*(1), 39–76.
62. Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research, 28*(2), 378–396.
63. Wang, J. G., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly, 39*(1), 91–U491.
64. Wang, J. G., Xiao, N., & Rao, H. R. (2015). An exploration of risk characteristics of information security threats and related public information search behavior. *Information Systems Research, 26*(3), 619–633.
65. Warkentin, M., Walden, E., Johnston, A. C., & 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), 194–215.
66. Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii–xxiii.
67. Willison, R., & Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1–20.
68. Wolff, J. (2016). Perverse effects in defense of computer systems: When more is less. *Journal of Management Information Systems, 33*(2), 597–620.
69. Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research, 25*(2), 385–400.
70. Zafar, H., & Clark, J. G. (2009). Current State of information security research in IS. *Communication of Association Information Systems, 24,* 557–596.
71. Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association, 16*(6), 448–484.