Quo Vadis Behavioral Information Security Research?

Completed paper

Nan (Peter) Liang
Stephenson Department of Entrepreneurship and Information Systems
E.J. Ourso College of Business
Louisiana State University
nliang@lsu.edu

Merrill Warkentin
Department of Management and Information Systems
College of Business
Mississippi State University
m.warkentin@msstate.edu

Rudy Hirschheim
Stephenson Department of Entrepreneurship and Information Systems
E.J. Ourso College of Business
Louisiana State University
rudy@lsu.edu

Detmar W. Straub
Fox School of Business
Temple University
straubdetmar@gmail.com

ABSTRACT

After decades of academic endeavors in the field of behavioral information security, a plethora of theories have been introduced, modified, tested, and synthesized to explain and to predict individuals' security related behaviors. In this article, instead of spotting gaps to find nuances, we apply the problematization method to identity assumptions of existing literature. We found that most, if not all, existing studies implicitly assume that protecting information systems security (ISS) is normatively right in itself. However, we argue that, especially from the perspective of those who are not security professionals, protecting ISS is not a normative issue, but is often construed as means to achieve various ends. We introduce the institutional logics perspective to compare these two views. We then propose a new disciplinary question for future research, which extends the current focus on individual behaviors to the logic of the security profession and its coexistence, interaction, and contradiction with logics of other institutional

orders, e.g. logic of corporation. Next, we propose three research areas (i.e. SETA program, different roles of security policy, and the context of InfoSec related behaviors) and corresponding research questions based on this new disciplinary question. Finally, we conclude the paper by briefly discussing the practical implications of the proposed research areas and future research questions.

Keywords

Behavioral information security, policy compliance, institutional logics, information security profession.

INTRODUCTION

Stanton, Stam, Mastrangelo, and Jolton (2006, p. 263) defined *behavioral information security (behavioral InfoSec)* as "human actions that influence the availability, confidentiality, and integrity of information systems." Instead of advancing technical approaches to prevent intrusion into organizations' information assets, behavioral InfoSec research focuses on "behaviors of individuals which relate to protecting information and information assets" (Crossler et al., 2013, p. 91). Behavioral InfoSec research could be traced back to the 1970's work at Stanford Research Institute, which studied the phenomenon of computer abuse (Parker, 1976). Since Straub (1990) introduced this concept (i.e. computer abuse) into the IS field, behavioral InfoSec research, e.g. policy compliance/violation studies, have been an enduring topic for decades (c.f. Chen et al., 2021; Cram, D'Arcy, & Proudfoot, 2019; Cram, Proudfoot, & D'Arcy, 2017; Moody, Siponen, & Pahnila, 2018).

As existing literature has put forth a comprehensive framework to understand individuals' InfoSec related behaviors, this stream of research has researched the level of maturity that a

plethora of behavioral antecedents have been proposed and empirically supported (Cram et al., 2019), systematic literature reviews have been conducted (Cram et al., 2017; Dhillon, Smith, & Dissanayaka, 2021), and unified model of policy compliance has been constructed (Moody et al., 2018). Although these efforts well synthesize existing knowledge and pave the way for future research to *extend* existing literature, evidence exists that current theorization and understanding of InfoSec related behaviors should not only be *complemented* but also be *challenged* in future academic endeavors. For example, although multiple studies (Vance, Siponen, & Straub, 2020) found that moral beliefs are associated with security-related behaviors (or intentions thereof), Moody et al. (2018) question whether employees in organization see insecure acts as morally blameworthy as perceived by security professionals. Also, although security policy compliance is often regarded as the effective method to prevent interruptions to organizations' operations, Karjalainen, Sarker, and Siponen (2019) found that following security policy could actually impede the achievement of other organizational goals.

These examples illustrate that, although complying with security policy, or even secure use of information systems in general, may not always be the singular priority of organizations, it seems to be conceptualized as so in most, if not all, published studies in the field of behavioral InfoSec. We argue that one certain assumption is behind this conceptualization, and it is this assumption that we are to identify, to articulate, and to challenge in this article. To this backdrop, we propose the following three questions:

***First**, are there any unchallenged assumptions embedded in current behavioral InfoSec literature?*

***Second**, how do these assumptions hinder the understanding of InfoSec related behaviors?*

***Third**, how to remedy the state of affairs, and what research agenda could be set forth for future behavioral InfoSec research?*

Note that an intuitive and obvious answer to these questions is that *we are researchers in the field of behavioral InfoSec so we study nothing else but employees' InfoSec related behaviors.* However, we are not satisfied with this intuitive answer because it contributes, if any, trivial knowledge to the field. Therefore, instead of accepting this intuitive answer as taken-for-granted rationale, we critically reflect on existing literature to identify, to articulate, and to challenge assumptions to bring new insights and to shed light on future studies. With this purpose, the rest of this paper is organized as follows: we first apply the problematization methodology (Alvesson & Sandberg, 2011) to identify underlying assumption in existing behavioral InfoSec literature. Also, we discuss the ramification of these two assumptions on the field of Behavioral InfoSec. We then introduce institutional logic (Friedland & Alford, 1991) as the analytical framework to understand the identified assumption, and to propose alternative assumption. Next, we discuss the theoretical implication of the alternative assumption. Specifically, we contend that, if we no longer consider ISS as normatively right in itself, a new disciplinary question could be raised to enhance our understanding of security phenomenon. After proposing the new disciplinary question, we discuss how this new disciplinary question could contribute to the major problems in existing literature. Finally, we conclude by demonstrating the practical implications via an exploratory study.

USING PROBLEMATIZATION METHODOLOGY TO IDENTIFY ASSUMPTIONS UNDERLYING BEHAVIORAL INFOSEC LITERATURE

The main purpose of study 1 is *not* to identify gaps (i.e. gap-spotting) in existing behavioral InfoSec literature but to challenge assumptions underlying published work. With this purpose, we apply the methodology of *problematization* (Alvesson & Sandberg, 2011; Chatterjee &

Davison, 2021) to critically review behavioral InfoSec research. Unlike gap-spotting approach which critiques the existing literature as incomplete or inadequate so that *gaps* in the literature need to be filled (Locke & Golden-Biddle, 1997), problematization focuses on identifying and challenging *assumptions* shared by existing literature. In this section, we first briefly discuss the difference between gap-spotting and problematization methodologies. We then apply this methodology to identify assumptions embedded in behavioral InfoSec literature. Finally, we evaluate identified assumptions regarding how these assumptions affect the development of knowledge toward understanding behavioral InfoSec phenomenon.

From gap-spotting to problematization

Gap-spotting refers to the approach of reviewing existing literature in order to identify or to create deficiency in it (Alvesson & Sandberg, 2011; Sandberg & Alvesson, 2011). Based on the analysis of 52 articles in premier management journals, Sandberg and Alvesson (2011) identified three basic modes of gap-spotting, namely confusion, neglect, and application spotting. *Confusion spotting* is to spot contradictory evidence or competing explanations in the literature. For example, Anderson and Reeb (2004) reviewed the literature of corporate governance and found two theories, i.e. agency theory and stewardship theory, predict contradictory behaviors of independent director. *Neglect spotting* focuses on areas that are overlooked, under-researched, or lack of empirical support. Case in point, Musson and Tietze (2004) argued that, although cultural meaning making is a well-studied area, the process of meaning creation has been overlooked. *Application spotting* aims to identify topics or issues that need to be extended or complemented (Sandberg & Alvesson, 2011). For instance, Watson (2004) claimed that HRM studies are mostly prescriptive and normative, and should be complemented by critical theory perspectives.

Although gap-spotting consists of complex, constructive, and creative processes (Alvesson & Sandberg, 2011) and plays an important role in both quantitative and qualitative research projects (Sandberg & Alvesson, 2011), this approach has severe limitations (Chatterjee & Davison, 2021). Most importantly, because the gap-spotting approach mainly extends or complements previous research, it often leads to underproblematizing the research focus (Alvesson & Sandberg, 2011). However, as Davis (1986) argued, what makes a theory interesting is that it challenges underlying assumptions of existing theories in significant ways. In this sense, because "gap-spotting does not deliberately try to challenge the assumptions that underlie existing literature, it is less likely to raise the proportion of high-impact theories within the management field" (Alvesson & Sandberg, 2011, p. 251).

Unlike gap-spotting, the problematization methodology directly aims to identify, to articulate, and to challenge assumptions underlying existing literature. Note that although the term problematize is often used interchangeably with other terms, e.g. critique, *problematization* in this article does not assume the broad conceptualization as defined by Locke and Golden-Biddle (1997), i.e. critiquing existing literature, but is closer to Foucault's (1985, p. 9) conceptualization as an "endeavor to know how and to what extent it might be possible to think differently, instead of what is already know". In their seminal work, Sandberg and Alvesson's description is quite telling about the difference (2011, p. 32):

> *(Unlike broader meaning of problematization as critiquing literature to spot gaps) A central goal in such problematization is to try to disrupt the reproduction and continuation of an institutionalized line of reasoning. It means taking something that is commonly seen as good or natural, and turning it into something problematic. Specifically, problematization as we define it here aims to question the assumptions underlying existing theory in some significant ways.*

Identifying assumptions embedded in the theorization of InfoSec literature

To identify assumptions embedded in the theorization of InfoSec related behaviors, we choose to analyze path-defining studies in the field, as recommended by Alvesson and Sandberg (2011). Specifically, as Moody et al. (2018) identified 10 theories that are applied to explain employees' (non)compliance behaviors (intentions), in Study 1, we chose to analyze articles that are early studies to introduce these 10 theories to behavioral InfoSec research community.

We acknowledge that behavioral InfoSec literature have drawn on many other theoretical foundations other than, as well as some variations of, these 10 theories. For example, Y. Chen et al. (2021) reviewed 112 empirical studies in this area and identified 70 different theories or perspectives in these articles. We also acknowledge that many later articles are at least as influential as the ones introducing specific theories in the field. Therefore, after identifying assumptions from the articles chosen for analysis, these assumptions are discussed in context of recent authoritative summaries of (Cram et al., 2019; Cram et al., 2017; Dhillon et al., 2021; Moody et al., 2018) and a recent influential article (Y. Chen et al., 2021) in behavioral InfoSec literature, to "investigate whether all the assumptions that one finds potentially interesting to challenge are still in operation" (Alvesson & Sandberg, 2011, p. 256). The 10 theories identified in Moody et al. (2018) and corresponding path-defining articles, as well as recent summaries of behavioral InfoSec literature are listed in Table 1.

Table 1. Path-Defining Articles and Recent Summaries of Literature in Behavioral InfoSec Field

Reasons to Include	Articles	Summary of Articles
To identify Embedded Assumptions	Straub (1990)	Straub (1990) applied **Deterrence Theory** to study computer abuse.
	Siponen and Vance (2010)	Siponen and Vance (2010) applied **Neutralization Theory** to study policy violation.
	Ng, Kankanhalli, and Xu (2009)	Ng et al. (2009) applied **Health Belief Model** to study computer security behavior.

	Herath and Rao (2009)	Herath and Rao (2009) applied **Protection Motivation Theory** to study security policy compliance.
	Bulgurcu, Cavusoglu, and Benbasat (2010)	Bulgurcu et al. (2010) applied **Theory of Planned Behavior** to study security policy compliance.
	Pee, Woon, and Kankanhalli (2008)	Pee et al. (2008) applied **Theory of Interpersonal Behavior** to study nonwork-related computing in workplace.
	Bulgurcu et al. (2010)	Bulgurcu et al. (2010) applied **Rational Choice Theory** to study security policy compliance.
	Johnston and Warkentin (2010)	Johnston and Warkentin (2010) applied **Extended Parallel Processing Model** to study behavioral intentions associated with recommended computer security actions.
To investigate whether assumptions identified are still in operation	Cram et al. (2017)	Cram et al. (2017) **systematically reviewed** policy behavioral InfoSec literature and proposed a research framework.
	Moody et al. (2018)	Moody et al. (2018) constructed a **unified model** of information security policy compliance.
	Cram et al. (2019)	Cram et al. (2019) conducted a **meta-analysis** of antecedents to security policy compliance.
	Dhillon et al. (2021)	Dhillon et al. (2021) **reviewed existing literature** to explore the gap between ISS practice and research.
	Y. Chen et al. (2021)	Y. Chen et al. (2021) **challenged the assumption** that policy compliance and violation are the opposites of one single construct, and tested a model that incorporated compliance and violation as two dependent variables.

Note: *We only include articles that introduced particular theory, but not articles that applied its extensions. Specifically, Theory of Planned Behavior (TPB) is an extension of Theory of Reasoned Action (TRA). So we only included article that applied TPB (Bulgurcu et al., 2010). Also, Extended Protection Motivation Theory (PMT2) is an extension of original Protection Motivation Theory (PMT). So we only included article that applied PMT (Herath & Rao, 2009).*

following guidelines from Alvesson and Sandberg (2011) to problematize the existing literature, our careful reading of the path defining articles reveals that there indeed exists an assumption. We articulate the assumption embedded in these path-defining articles as **Normative Assumption**:

> ***Normative Assumption****: Protecting the availability, confidentiality, and integrity of information systems is normatively right.*

We then supplement the analysis with broader readings of authoritative review articles and recent influential articles (Chen et al., 2021; Cram et al., 2019; Cram et al., 2017; Dhillon et al., 2021; Karjalainen et al., 2019; Moody et al., 2018). We found that this assumption is still in operation. In the next section, we apply institutional logics perspective to first elaborate on the

rationale of the Normative Assumption, and propose an alternative assumption, i.e. Instrumental Assumption.

STUDYING INFOSEC RELATED BEHAVIORS WITHOUT IMPOSING THE NORMATIVE ASSUMPTION: AN INSTITUTIONAL LOGIC PERSPECTIVE

Alvesson and Sandberg (2011) suggested that, after identifying the assumption in existing literature, alternative or counter assumptions should be raised and evaluated. In this section, we first briefly discuss the theoretical basis to raise the alternative assumption, i.e. institutional logics perspective (Thornton, 2004; Thornton et al., 2012). We then discuss that, from this perspective, protecting ISS is indeed normatively right *according to the logic of the security profession*. However, protecting ISS is not always a normative issue and could also serve purposes other than maintaining norms of the security profession (i.e. the logic of the security profession), e.g. to increase efficiency and profits of organizations (i.e. the logic of market), or to increase size and diversification of firm (i.e. the logic of corporation). Finally, we articulate the alternative assumption based on these discussions.

Brief Introduction of Institutional Logics

Because of its adherence, prominence, and scholarly generativity (Ocasio, Thornton, & Lounsbury, 2017), literature of institutional logics, which was first introduced as a theory of institution (Friedland & Alford, 1991), has grown dramatically and spread beyond management disciplines (Faik, Barrett, & Oborn, 2020; M. Lounsbury, Steele, Wang, & Toubiana, 2021; Ocasio et al., 2017). Besides institution analysis, institutional logics perspective has also been applied to study a variety of issues such as social change (Faik et al., 2020), social impact of

universities (Cinar & Benneworth, 2021), technology innovations (Slavova & Karanasios, 2018), love (Friedland, Mohr, Roose, & Gardinali, 2014), etc.

Thornton and Ocasio (2008, p. 101) defined *institutional logic* as "socially constructed, historical patterns of cultural symbols and material practices, including assumptions, values, and beliefs, by which individuals and organizations provide meaning to their daily activity, organize time and space, and reproduce their lives and experiences." Friedland and Alford's (1991) seminal work introduced the institutional logics perspective as a new theory of institution, to criticize the prevailing concept at the time that institutionalization stems from the structuration of the institutional fields (DiMaggio & Powell, 1983). Unlike early institutionalism (e.g. DiMaggio & Powell, 1983) that perceives the survival and success of organization depends on the legitimacy of institution which is rooted in coercive, normative, and mimetic sources (Scott, 1994), institutional logics perspective contends that legitimacy is not a universal commodity that institutions could possess, but a condition reflecting consonance with different, societal-level institutional orders, e.g. family, religion, etc., because these institutional orders constitute a frame of reference that precondition actors' perception of interest and norms (Friedland & Alford, 1991; Scott, 1994; Thornton, 2004; Thornton et al., 2012).

The institutional logic perspective is commonly represented by two dimensions. The horizontal X-Axis consists of institutional orders which is defined as different domain of societal level institutions that govern a unique area of life (Thornton et al., 2012). Thornton et al. (2012) identified seven different institutional orders, including family, community, religion, state, market, profession, and corporation. The vertical Y-Axis consists of "elemental categories or building blocks, which represent the cultural symbols and material practices particular" to each

order (Thornton et al., 2012, p. 54). Figure 1 (Thornton et al., 2012, p. 56) illustrates these seven institutional orders and their corresponding elemental categories.

Figure 1. Seven Institutional Orders and Their Elemental Categories

Y-Axis:	X-Axis: Institutional Orders						
Categories	**Family 1**	**Community 2**	**Religion 3**	**State 4**	**Market 5**	**Profession 6**	**Corporation 7**
Root Metaphor 1	Family as firm	Common boundary	Temple as bank	State as redistribution mechanism	Transaction	Profession as relational network	Corporation as hierarchy
Sources of Legitimacy 2	Unconditional loyalty	Unity of will Belief in trust & reciprocity	Importance of faith & sacredness in economy & society	Democratic participation	Share price	Personal expertise	Market position of firm
Sources of Authority 3	Patriarchal domination	Commitment to community values & ideology	Priesthood charisma	Bureaucratic domination	Shareholder activism	Professional association	Board of directors Top management
Sources of Identity 4	Family reputation	Emotional connection Ego-satisfaction & reputation	Association with deities	Social & economic class	Faceless	Association with quality of craft Personal reputation	Bureaucratic roles
Basis of Norms 5	Membership in household	Group membership	Membership in congregation	Citizenship in nation	Self-interest	Membership in guild & association	Employment in firm
Basis of Attention 6	Status in household	Personal investment in group	Relation to supernatural	Status of interest group	Status in market	Status in profession	Status in hierarchy
Basis of Strategy 7	Increase family honor	Increase status & honor of members & practices	Increase religious symbolism of natural events	Increase community good	Increase efficiency profit	Increase personal reputation	Increase size & diversification of firm
Informal Control Mechanisms 8	Family politics	Visibility of actions	Worship of calling	Backroom politics	Industry analysts	Celebrity professionals	Organization culture
Economic System 9	Family capitalism	Cooperative capitalism	Occidental capitalism	Welfare capitalism	Market capitalism	Personal capitalism	Managerial capitalism

Protecting ISS is Indeed Normatively Right According to Logic of the Security Profession

One critical contribution of the institutional logics perspective is that it objects to the claim that norms in operation at various organizations stem from world-level taken-for-granted rules and conventions as proposed by Meyer and Rowan (1977); instead, norm is "a variable element or attribute" (Thornton et al., 2012, p. 43) of different institutional orders, e.g. norm of profession is different from norm of religion. In this sense, InfoSec related behaviors are not only behaviors that are authorized (or prohibited) by organizational policy as conceptualized in existing literature (e.g. Cram et al., 2019; Straub, 1990), but also *behavioral treatments prescribed by information security professionals*. Profession draws legitimacy from personal expertise (Thornton et al., 2012) and abstract knowledge (Abbott, 1988), and forms norm based on

membership in professional guild (Thornton, 2004); therefore, as long as activities to protect ISS are prescribed by the security profession (i.e. membership in professional association) and are based on security knowledge (i.e. personal expertise), abiding these prescribed activities will be considered as *the normatively right things to do in the eyes of the security profession*.

Protecting ISS is Not Always a Normative Issue

Profession is not the only institution order that might affect individual and organizational activities. In other words, if the organizational operation is (1) *not all about* information security and is (2) *not all up to* information security, then the logic of the security profession might coexist, interact, or even contradict with logics of other institutional orders that have different focus of attentions, e.g. to increase efficiency and profits of organizations (i.e. the logic of market), and to increase size and diversification of firm (i.e. the logic of corporation). To this backdrop, we propose the alternative assumption as following, and discuss the implication of this assumption to future research in the next section.

> **Instrumental Assumption:** *Besides being construed as normatively right things to do, protecting the availability, confidentiality, and integrity of information systems could also serve as means to support the goals enunciated by institutional logics other than the logic of the security profession.*

IMPLICATION FOR THE PRACTICE OF THEORIZING INFOSEC RELATED BEHAVIORS

In this section, we discuss the implications of Institutional logics perspective for the process and products of theorizing InfoSec related behaviors, which are essential to produce native and innovative theories of a field (Hassan, Lowry, & Mathiassen, 2021; Hassan, Mathiassen, & Lowry, 2019). Specifically, we contend that, if applied to understand InfoSec related behaviors,

the institutional logics perspective could be used to raise new disciplinary questions that address the logic of the security profession, as well as its interaction with logics of other institutional orders, as the object of study. In this section, we first briefly elaborate on the concept of disciplinary question and identify the current disciplinary question. Next, we propose a new one from the institutional logics perspective and propose research questions for future studies.

The current and new disciplinary question

A *disciplinary question* "addresses an *object of study* as a problem requiring solution based on the field's rules of discourse and pattern of inquiry" (Hassan et al., 2021, p. 9. Italics added by the authors). Because disciplinary question not only describes the phenomenon of interest but also frames and addresses the phenomenon based on the field's rules of inquiry, disciplinary question distinguishes one discipline from other disciplines (Hassan et al., 2021; Hassan et al., 2019). For example, Durkheim (1951/1897, p. 324), although posed a question regarding suicide that was extensively studied by other disciplines, posed the question that "why in every society, a definite proportion of people commit suicide in any given period?" In this example, because Durkheim didn't approach the suicide problem focusing on state of mind or the physical well beings, instead linked the suicide phenomenon to societal-level inquiries. Durkheim thus distinguished his discourse of sociology from other disciplines such as medical or psychological disciplines.

Although not explicitly stated in the literature, we argue that the disciplinary question of existing behavioral InfoSec research is:

> **Current disciplinary question**: *Why, in various types of organizations, some individuals act to enhance or protect the security of information assets, while others behave in ways that pose risk and threat to them*?"

According to the institutional logics perspective, we propose a new disciplinary question:

> **New disciplinary question**: *How does the logic of the security profession change the activities of organizations and their employees?*

Note that this new disciplinary question isn't meant to replace the existing one but to expand it. Compared to the disciplinary question of existing behavioral InfoSec literature, the disciplinary question that we propose here addresses a different set of the objects of study other than overt behaviors that could affect the cybersecurity of organizations. In the rest of this section, we propose the three areas of study based on the new disciplinary question for future InfoSec research.

Research Area 1: Logic of the security profession

What we know: The emerging logic changes the activities of organizations and individuals

Institutional studies found that the newly emerged logic in an organization or even in a field would transform the activities of organizations and individuals. For example, Suddaby and Greenwood (2005) found that, after purchasing a law firm in 1977, Ernst & Young experienced the emergence of the logic of law profession within the firm. The discursive struggle between the logic of two professions, i.e. law and accounting, dramatically change how Ernst & Young, as well as its employees, practice their business. Also, Durand, Szostak, Jourdan, and Thornton (2013) found that the emergence of a managerialist logic in design industry redirect firms' attention from technique and aesthetics focus to marketing focus. Furthermore, Pallas, Fredriksson, and Wedlin (2016, p. 1662) reported how the media logic, i.e. "a set of ideas, norm, principles, routines and activities guiding journalistic work", change the routines and practices of different professions in a government agency.

What we know: The Security, Education, Training, and Awareness (SETA) research in ISS

SETA programs are organizational initiatives to enhance employees' awareness of security risk, to improve employees' consciousness of security policies, and to provide training of security knowledge and skills (D'Arcy, Hovav, & Galletta, 2009). The behavioral InfoSec community has generally agreed on the necessity of SETA program for organizations to protect the security of their information systems (Karjalainen & Siponen, 2011; Posey, Roberts, & Lowry, 2015; Puhakainen & Siponen, 2010). This belief is also corroborated by empirical evidence demonstrating the positive effects of SETA program on employees' compliance (or intention thereof) with security policy (e.g. Bulgurcu et al., 2010; Puhakainen & Siponen, 2010; Silic & Lowry, 2020). To ensure the effectiveness, researchers suggest to design and to implement SETA program based on organizational and individual factors of the target audience (Bauer, Bernroider, & Chudzikowski, 2017; Hu, Hsu, & Zhou, 2021; Karjalainen & Siponen, 2011; Silic & Lowry, 2020).

What we need to know: Future Research Questions

From the institutional logics perspective, SETA programs should not only focus on training employees to be aware of security risk and how to properly use information systems, but also on issues related to the cultivation of logics, such as fostering relational networks between non-security personnel and security professionals, encouraging non-security personel to participate in security associations, and increasing personal reputation of the security profession among non-security personel. To be best of our knowledge (Hu et al., 2021), these topics have not drawn sufficient attention in the SETA literature. Future research that studies these topics will not only broaden our understanding of SETA programs, but also will provide a basis for designing and implementing effective SETA programs.

Research Question 1a: *How to define and to measure the instantiation of the logic of security profession in various organizations?* Instantiation of the logic refers to the concrete evidence of the existence of the logic (Thornton et al., 2012). Institutional logic reserch show that, even for the same profession, logic of profession could be instantiated into different variations. For example, Rao, Monin, and Durand (2003) shows that logic of chefs (i.e. a profession) underwent significant changes during the nouvelle cuisine movement. Regarding the logic of the security professions, we encourage future research into how various elementary categories (Thornton et al., 2012), i.e. Y-axis in Figure 1 including source of legitimacy, basis of norm, basis of strategy, etc., are instantiated in different organizations, *especially among non-security personnel*. For example, what is the *relationship network* among security professionals and non-security personnel? To what extent non-security personnel are invovled in the activities of security department/association/guild? To what extent are the security expertise recognized, appreciated, or respected by non-security personnel?

Research Question 1b: *How to effectively foster or cultivate the logics of the security profession in organizations?* We argue that the cultivation of the logics of the security profession is of crucial importance because individuals would not integrate security practices into their daily practices and routines if the logic of the security profession is not avaiable or accessible to them. From this perspective, future research on SETA program should not limit their attention to the content and delivery methods of the SETA program. Instead, we encourage future research to take a holistic view and to study means to foster the logics of the security profession at multiple levels and in various context, *even outside the organizational boundary*. For example, if organizations design initiatives to help employees to improve the *cybersecurity of their home*,

will these initiatives have spillover effects on employees' adoption of the logic of the security profession in their workplace?

Research Question 1c: *How to effectively foster or to cultivate the logics of security professionals in **different** organizations?* Research in SETA have demonstrated that there does not exist a one-size-fit-all program (Hu et al., 2021). We encourage future research, while exploring means to cultivate logic of the security profession, take into consideration the characteristics of various types of organizations.

Research Area 2: The different roles of Information security policy

Adoption of information security policy has been considered as a fundamental approach to safeguard the security of orgnanizational information systems (Cram et al., 2017). After surveying various definitions of security policy in existing literature, we found that the portrayals of the purposes of security policy could be classified into two categories, namely security-oriented and management-oritented. Specifically, *most* studies describe the purpose of security policy as to *ensure information security*. For example, Bulgurcu et al. (2010, pp. 526-527) contends that policy is "to safeguard the information and technology resources of their organizations". D'Arcy and Lowry (2019, p. 44) descrbies the purpose of policy is to "specify the proper uses of organizational information and technology resources". Ifinedo (2014, p. 78) states that the goal of policy is to "safeguard organizational IS assets from intention abuse or destruction". On the other hand, a small portion of studies depict the purpose of security policy as to *support security management*. For example, L. Cheng, Li, Li, Holm, and Zhai (2013, p. 448) defines security poicy as the "written statement that defines the requirements for the orgnizational security management". Sommestad, Karlzén, and Hallberg (2015, p. 200) argue that security policies are "aimed at governing and supporting employees".

The difference between security-oriented and management-oriented purposes might seem rethorecal and trivial. However, from institutional logics perspective, they represent goals from two distinct logics. Specifically, the security-oriented definitions reflect the *logic of the security profession* which focuses on the achievement of security. The management-oriented descriptions, on the other hand, represent the *logic of corporation* which aims at effective organizational controls.

Besides *safeguarding information assets* (i.e. goals prescribed by the logic of the security profession) and *supporting security management* (i.e. goals prescribed by the logic of corporation), we argue that organizational security policy could also play another role to serve goals that are not discussed in existing literature. Specifically, adoption of security policy could serve as *organizational response to institutional pressures* (i.e. goals motivated by the pressure from other institutional orders such as state regulation and stakeholders' demand). Organizations often adopt policies, e.g. equality policy, environmental policy, diversity policy, etc., as response to pressures from state regulation or shareholders' demand (Bromley & Powell, 2012). Cybersecurity related regulations have been passed, e.g. Health Insurance Portability and Accountability Act (HIPPA), Gramma-Leach-Bliley Act, and Federal Information Security Management Act (FISMA), and proposed, e.g. Data Security and Breach Notification Act (Blackburn, 2015), to regulate organizational security practices. Therefore, we speculate that organizations would also adopt policy as responses to these regulations.

Considering these two goals other than safeguarding information systems security, we first briefly discuss two relevant areas of research, namely organizational control (Cardinal, Kreutzer, & Miller, 2017) and policy-practice decoupling (Bromley & Powell, 2012). We then propose research questions for future studies in the field of behavioral InfoSec research. Note that the

three different roles are analytical dimensions. They are analytical because these three roles of policy often overlap in practice, especially between ensuring security of information systems and supporting security management. However, we argue that perceiving information security policy as playing these three different roles could shed light on our understanding of security practices in organizations, raising research questions that tap on important areas regarding the security management.

What we know: Organizational control

Cardinal et al. (2017) conducted a systematic review of organizational control research published in top management journals from 1965 to 2015. Cardinal and colleagues identified three dimensions constituing various frameworks of organizational control. These three dimensions are control famality (formal control vs. informal control), control coerciveness (coercive control vs. enabling control), and control singularity (singular control vs. weak/strong holistic control). The first two dimensions, i.e. control formality and control coerciveness, focuse different types of control in organizations. The third dimension, i.e. control singularity, represent "whether empirical researchers take a singular or holistic" view of control in their studies.

Regarding the first two dimensions, *formal control* are codified, visible, and explicit institutional mechanism such as written procedures and regualtions (Kreutzer, Cardinal, Walter, & Lechner, 2016); while *informal control* comprise "unwritten, unofficial…less objective, uncondified" (Cardinal, Sitkin, & Long, 2004, p. 414) forms of control. *Coercive control* places paramout priority on "compliance, following rules, and hierarchical supremacy" (Cardinal et al., 2017, p. 567; Weber, Gerth, & Mills, 2013 (first published in 1946)). *Enabling control*, on the other hand, suggest a form of control that "provides needed guidance and clarifies responsibilitites, threby

easing role stress and helping individuals be and feel more effective" (Adler & Borys, 1996, p. 61).

For the third dimension, control singularity relates to the approach used to study control. Studies employing *singular view* of control often conceives only one type of control as useful in a given context. Types of control include *behaviour-control* (Ouchi & Maguire, 1975) that evluates controlee's adherence to prescribed procedures or actions, *outcome control* (Morris, Zhong, & Makhija, 2015) that evaluates the extent to which controlee has accomplished the output targets, clan control (Kirsch, Ko, & Haney, 2010) that utilizes common values, consensus, and pledges to coordinate controlee's action, and self-control that allows controlees to set their own goals and manage themselves (Kirsch & Cummings, 1996; Liu, 2015). Studies employing *holistic veiw* of control, instead of studying and theorizing one single type of control, assumes that organizational control inherently consists of multiple approaches; therefore, control studies should focus on how these approaches interact, substitute, or complement with each other (Cardinal et al., 2004; Kreutzer, Walter, & Cardinal, 2015).

What we know: Decoupling research

Organizational research show that organizations sometimes only signal the adoption of certain policy, but, in actuality, take limited actions to implement and to enforce the policy in practice (Heese, Krishnan, & Moers, 2016; Westphal & Zajac, 2001). The gap between symbolic adoption and actual implementation is referred as decoupling, a topic that has been well studied in organizational research (Bromley & Powell, 2012; Crilly, Zollo, & Hansen, 2012; Heese et al., 2016; Tilcsik, 2010; Westphal & Zajac, 2001). Decoupling has been employed by organizations as a mean to maintain external legitimacy without significantly interrupting their internal structures or practices (Heese et al., 2016). Recent literature distinguish two forms of decoupling,

namely policy-practice decoupling and means-end decoupling (Bromley & Powell, 2012; Heese et al., 2016).

Policy-practice decoupling is also referred as symbolic *adoption* (Heese et al., 2016, p. 2180) where organizations "respond ceremonially rather than substantively" by adopting the policies but not implementing them. For example, Edelman (1992) found that organizations responded to Equal Employment Opportunity and Affirmative Action (EEO/AA) law by creating forma structures and policies so that signs of compliance is visible. However, little organizational resources are directed to implement these policies and to change practices. Also, Tilcsik (2010) found that a post-communist government agency adopted a new budget system and policy based on scientific methods due to the critics from the public. However, the budgeting practice were not substantively affected by the policy. Instead, the government agency circumvented procedures and standards by allocating resources that are recorded in "a bunch of fragmented, obscure documents" (Tilcsik, 2010, p. 1483).

Means-end decoupling is also called *symbolic-implementation* (Heese et al., 2016) where organizations *vigorously but selectively* implement adopted policies to support goals of the organization, e.g. financial goals, instead of goals intended by the regulation (Wijen, 2014). For example, companies might adopt and implement sustainability-related policies because the sustainability certification grants companies substantial competitive advantages and financial interests (Henson, Masakure, & Cranfield, 2011).

What we need to know: Future research questions

Research Question 2a: *If information security policy is adopted as compliance to government or industrial regulation (logic of the state), how would this change the practices of organizations and individuals?* A recent study by D'Arcy and Basoglu (2022) found that the companies

respond differently to the guidance issued by US Securities and Exchange Commission (SEC, 2011), selectively disclosing their cybersecurity incidents. This is classic example of decoupling between policy adoption and implementation. We encourage future to follow this path (D'Arcy & Basoglu, 2022) and study the phenomenon of decoupling regarding how organization and its members respond to cybersecurity regulations.

Research Question 2b: *How to use multiple control methods to achieve better security performance?* The control perspective has been widely adopted in behavioral InfoSec research. Factors related to organizational controls such as deterrence (e.g. Straub, 1990), informal sanctions (e.g. D'arcy & Herath, 2011), persuasive communication (e.g. Barlow, Warkentin, Ormond, & Dennis, 2013), and accountability (e.g. Vance, Lowry, & Eggett, 2015) have been well studied in the field. From organizational control perspective, these studies take a *singular approach* to study the effectiveness of certain control method, without studying how different methods interact and complement with others. The most studied control method includes behavior control, e.g. policy compliance or violation, or outcome control, e.g. number of computer abuses (Straub, 1990). However, "As means-ends relationship become less clear, behavior control is expected to be less effective, and as the reliability and validity of outcome measures decrease, outcome control is deemed infeasible" (Kreutzer et al., 2015, p. 1317). We argue that this is exactly the case in security management as it is very difficult, if not impossible, to contend that every policy violation will lead to security incident, and it is also very hard to measure the number of security incidents accurately and reliably in organizations other than those high-profile ones. We therefore encourage future research to take a holistic view, to study and to theorize how different control mechanisms interact and complement with each other.

Research Area 3: The context of InfoSec related behaviors

What we know: The importance of context

Johns (2006, p. 386) defines context as "situational opportunities and contraints that affect the occurrence and meaning of organizaitonal behaviors as well as functional relationships between variables". The importance of context to the practice of theorizing has been well recognized in the behavioral InfoSec field (Crossler, Di Gangi, Johnston, Bélanger, & Warkentin, 2018; Dhillon et al., 2021; Siponen & Vance, 2014; Vance, Eargle, Eggett, Straub, & Ouimet, 2022), Information Systems discipline (Burton-Jones & Volkoff, 2017; Davison & Martinsons, 2016), and the general mangement discipline (Bamberger, 2008; Johns, 2017). Although debate exists regarding whether generablity or context is more important (c.f. Z. Cheng, Dimoka, & Pavlou, 2016; Martinsons & Davison, 2016; Sarker, 2016), it is generally agreed that studying the mechanism through which context affects behaviors is of critical importance to understand the individuals' behaviors (Burton-Jones & Volkoff, 2017; Martinsons & Davison, 2016), especially InfoSec related behaviors (Aurigemma & Mattson, 2019; Siponen & Vance, 2014).

What we know: Research on the context of InfoSec related behaviors

Various studies related to the context of InfoSec related behaviors have operationlized context differently. For example, Siponen and Vance (2014) and Aurigemma and Mattson (2019) contend that specific types of security policy violation, e.g. passord usage is different from locking computers, constittue important context for general policy violation. Dinev, Goo, Hu, and Nam (2009) investigated cultural difference between Korea and United States as the context of user behaviors. Johnston, Warkentin, McBride, and Carter (2016) studied situational factors of policy compliance. Other researchers include work-related factor as the context of InfoSec

related behavior, e.g. Vance et al. (2022) analyzed how different levels of task primary impact users' response to security-related persuasive message.

What we know: Institutional logics provide both opportunities and constrains for individuals to act

As early as the inception of the institutional logics perspective, Friedland and Alford (1991) indicated that institutional logics could not only explain phenomenon at macro level, such as the formation and changes of organization, but also micro level individual behaviors. On one hand, the coexistence of different institutional logics provides individuals the opportunities of agency to exploit the differences or even contradictions (Ocasio, 2011; Thornton, 2004; Thornton et al., 2012). On the other hand, the availability and accessibility of various institutional logics constitute repertoire of principles to organize behaviors and to channel interests (Thornton et al., 2012). This mechanism that institutional logics influence behaviors is corroborated by many empirical studies. For example, Thornton (2002) found that the emergent market logic in higher education publishing industry contradicts with the previously dominant logic, i.e. editorial logic which is one type of professional logic. This contradiction shifts the attention of organization from author-editor network to resource competition. This shift of attention, in turn, affects the behaviors of both organizations and editors.

What we know: Organizations in different fields have different field-level logics

Ocasio et al. (2017, p. 61) descrbed institutional field as consisting of "participants take one another into accounts as they carry out interrelated categories of symbos and practices within and

across individuals and organizations". Generally speaking[1], institutional field is constituted of individuals or organizations that practice similar activities. Examples of institutional fields include thrift industry (Haveman & Rao, 1997), public college and university (Gumport, 2000), restaurant (Rao et al., 2003), mutal fund industry (Michael Lounsbury, 2002), hospital (Nigam & Ocasio, 2010), etc. Besides being influenced by societal-level logics as listed in Figure 1, organizations in different fields also follow distinct field-level logics. For example, because a hospital and an investment bank belong to different fields, they will have different assumptions, beliefs, and principles to organize their material practices and cultural symbols. In other words, they follow different field-level logics.

What we need to know: Future research questions

As discussed before, logic of the security profession is raraly the only logic in operation. Therefore, we argue that the coexistence, interaction, and contradiction between logics of the security profession and other logics provide both opportunities and constraints for individuals to act, constituting the context of InfoSec related behaviors. From this perspective, studying how logic of the security profession interact with other logics could provide valuable insights regarding the context of InfoSec related behaiors.

Research Question 3a: *What characteristics of different institutional fields affect the InfoSec related behaviors?* Besides contextual factors already studied in existing literature, we contend that characteristics of different institutional fields also constitute important contexts for InfoSec

[1] We acknowledge that the definition and conceptulization of institutional field is a long last debate in institutional research (DiMaggio & Powell, 1983; Friedland & Alford, 1991; Thornton & Ocasio, 2008; Thornton et al., 2012). However, it it not the intent of this article to review these definitions based on various theoretical perspectives. Therefore, we decide not to engage with these debates to avoid distractions to readers.

related behaviors. We speculate that, because different fields have distinct goals, operations, and ways of utilizing information systems, required behaviors to protect ISS could vary significantly arcoss different institutional fields. For example, federal agents and contractors in defense sector are definitely subject to stricter security procedures than those regulating the employees of restaurants.

Research Question 3b: *How do characteristics of different institutional fields affect the InfoSec related behaviors?* We suggest future research not only study *what* characteristics of different institutional fields constitute context of InfoSec related behaviors, but also, most importantly, *how* these characteristics affect behaviors by providing both opportunities and constraints. A recent study by Karjalainen et al. (2019) shed light on this *how* question. By interviewing employees of a global company in the energy market and the marine industry, Karjalainen et al. (2019) identified four dialectical tensions that could affect policy compliance, i.e. trust vs. suspicion, individual vs. collective, instrumental vs. socio-emotional, and immediate vs. long-term focus. We encourage future research to study other institutional fields to explore issues such as whether these four tensions also exist in different contexts, are there any other tensions in different context, how are characteristics of fields related to different tensions, etc., to better understand how field-level characteristics constitute the contexts of InfoSec related behavior, and how different contexts affect InfoSec related behaviors.

Research Question 3c: *How do macro-level institutional logics affect individual-level behaviors?* Institutional logics exist in multiple levels (Friedland & Alford, 1991; Thornton et al., 2012), e.g. societal level logic such as logics of family and religion, field-level logic such as logics of the financial films, or even individual level such as the logic of love (Friedland et al., 2014), etc. These logics at different levels would, we argue, impose cross-level effects on

individuals' behavior, constituting context of InfoSec related behaviors. Therefore, we encourage future studies to investigate the mechanisms through which macro-level logics affect individual level behaviors to better understand the context of InfoSec related behaviors. One possible mechanism is through the *focus of attention* (Thornton, 2004; Thornton et al., 2012), because the limited attention of individual is directed by the interaction between different logics. In the context of behavioral InfoSec, we believe that if the dominant logic is not the logic of security, then individuals' attention might be directed at goals and acting schema other than those to protect the security of information systems. A recent study by Vance et al. (2022) corroborate with our proposal, as they found that the effects of feal appeal is moderated by task primacy, indicating that, if individuals attention is not directed by the logic of security, i.e. cognitive engagement with the security task is low (Vance et al., 2022), their actions are less likely to be programed by the logic of security.

CONCLUSION

Although the major contribution of this article is to propose a new theoretical perspective for future studies, we contend that the three areas and corresponding research questions that we proposed also have the potential to contribute to security practices. The major implication for security practice is that the research questions proposed in this article tackle the problem of information security and security management from non-security professional's perspective. Although there is no denial of the importance of the security professional in organizational security practice, we belive that non-security professionals also assume critical roles in security management. Therefore, the research areas and corresponding questions could shed light on how to coordinate actions between security professionals and non-security personnel, facilitating the

achievement of not only security goals, but other organizational goals that are important to organizations' survial and success.

REFERENCES

Abbott, A. (1988). *The system of professions. An Essay on the division of expert labor*. Chicago, IL: University of Chicago Press.

Adler, P. S., & Borys, B. (1996). Two types of bureaucracy: Enabling and coercive. *Administrative Science Quarterly*, pp. 61-89.

Alvesson, M., & Sandberg, J. (2011). Generating research questions through problematization. *Academy of Management Review*, 36(2), pp. 247-271.

Anderson, R. C., & Reeb, D. M. (2004). Board composition: Balancing family influence in S&P 500 firms. *Administrative Science Quarterly*, 49(2), pp. 209-237.

Aurigemma, S., & Mattson, T. (2019). Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research. *Journal of the Association for Information Systems*, 20(12), 7.

Bamberger, P. (2008). From the editors beyond contextualization: Using context theories to narrow the micro-macro gap in management research. *Academy of Management Journal*, 51(5), pp. 839-846.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, 39(Part B), pp. 145-159.

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, 68, pp. 145-159.

Blackburn, M. (2015). H.R.1770 - Data Security and Breach Notification Act of 2015. Retrieved from https://www.congress.gov/bill/114th-congress/house-bill/1770.

Bromley, P., & Powell, W. W. (2012). From smoke and mirrors to walking the talk: Decoupling in the contemporary world. *Academy of Management Annals*, 6(1), 4 pp. 83-530.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), pp. 523-548.

Burton-Jones, A., & Volkoff, O. (2017). How can we develop contextualized theories of effective use? A demonstration in the context of community-care electronic health records. *Information Systems Research*, 28(3), pp. 468-489.

Cardinal, L. B., Kreutzer, M., & Miller, C. C. (2017). An aspirational view of organizational control research: Re-invigorating empirical work to better meet the challenges of 21st century organizations. *Academy of Management Annals*, 11(2), pp. 559-592.

Cardinal, L. B., Sitkin, S. B., & Long, C. P. (2004). Balancing and rebalancing in the creation and evolution of organizational control. *Organization Science*, 15(4), pp. 411-431.

Chatterjee, S., & Davison, R. M. (2021). *The need for compelling problematisation in research: The prevalence of the gap-spotting approach and its limitations* (Vol. 31, pp. 227-230): Wiley Online Library.

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. *Information Systems Research*, 32(3), pp. 1043-1065.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, 39, pp. 447-459.

Cheng, Z., Dimoka, A., & Pavlou, P. A. (2016). Context may be King, but generalizability is the Emperor! *Journal of Information Technology*, 31(3), pp. 257-264.

Cinar, R., & Benneworth, P. (2021). *Why do universities have little systemic impact with social innovation? An institutional logics perspective. Growth and Change*, 52(2), pp. 751-769. doi:10.1111/grow.12367

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, 43(2), pp. 525-554.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, 26(6), pp. 605-641.

Crilly, D., Zollo, M., & Hansen, M. T. (2012). Faking it or Muddling Through? Understanding Decoupling in Response to Stakeholder Pressures. *Academy of Management Journal*, 55(6), 1429-1448. doi:10.5465/amj.2010.0697

Crossler, R. E., Di Gangi, P. M., Johnston, A. C., Bélanger, F., & Warkentin, M. (2018). Providing Theoretical Foundations: Developing an Integrated Set of Guidelines for Theory Adaptation. *Communications of the Association for Information Systems*, 43(1), 31.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, pp. 90-101.

D'Arcy, J., & Basoglu, A. (2022). The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures. *Journal of the Association for Information Systems*, 23(3), pp. 779-805.

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, 20(6), pp. 643-658.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), pp. 79-98.

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1), pp. 43-69.

Davis, M. S. (1986). 'That's classic!'The phenomenology and rhetoric of successful social theories. *Philosophy of the Social Sciences*, 16(3), pp. 285-301.

Davison, R. M., & Martinsons, M. G. (2016). Context is king! Considering particularism in research design and reporting. *Journal of Information Technology*, 31(3), pp. 241-249.

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *Journal of Strategic Information Systems*, 30(4). doi:10.1016/j.jsis.2021.101693

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 147-160.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, 19(4), 391-412.

Durand, R., Szostak, B., Jourdan, J., & Thornton, P. H. (2013). Institutional logics as strategic resources Institutional logics in action, part A: Emerald Group Publishing Limited.

Durkheim, E. (1951/1897). *Suicide: A study in sociology*. New York, NY: Free Press.

Edelman, L. B. (1992). Legal ambiguity and symbolic structures: Organizational mediation of civil rights law. *American Journal of Sociology*, 97(6), 1531-1576.

Faik, I., Barrett, M., & Oborn, E. (2020). How Information Technology Matters in Societal Change: And Affordance-Based Institutional Logics Perspective. *MIS Quarterly*, 44(3), 1359-1390. doi:10.25300/misq/2020/14193

Fletcher, K. E., & Huff, A. S. (1990). Argument mapping. In A. S. Huff (Ed.), *Mapping strategic thought* (pp. 355-402): John Wiley & Sons Ltd.

Foucault, M. (1985). The use of pleasure: *History of sexuality* (Vol. 2). New York, NY: Vintage Books.

Friedland, R., & Alford, R. R. (1991). Bringing society back in: Symbols, practices, and institutional contradictions. In W. W. P. a. P. J. DiMaggio (Ed.), *The New Institutionalism in Organizational Analysis* (pp. 232-263). Chicago, IL: The University of Chicago Press.

Friedland, R., Mohr, J. W., Roose, H., & Gardinali, P. (2014). The institutional logics of love: measuring intimate life. *Theory and Society*, 43(3-4), 333-370. doi:10.1007/s11186-014-9223-6

Gumport, P. J. (2000). Academic restructuring: Organizational change and institutional imperatives. *Higher Education*, 39(1), 67-91.

Hassan, N. R., Lowry, P. B., & Mathiassen, L. (2021). Useful Products in Information Systems Theorizing: A Discursive Formation Perspective. Journal of the Association for Information Systems, 23(2), 418-446.

Hassan, N. R., Mathiassen, L., & Lowry, P. B. (2019). The process of information systems theorizing as a discursive practice. *Journal of Information Technology*, 34(3), 198-220.

Haveman, H. A., & Rao, H. (1997). Structuring a theory of moral sentiments: Institutional and organizational coevolution in the early thrift industry. *American Journal of Sociology*, 102(6), 1606-1651.

Heese, J., Krishnan, R., & Moers, F. (2016). Selective regulator decoupling and organizations' strategic responses. *Academy of Management Journal*, 59(6), 2178-2204. doi:10.5465/amj.2015.0446

Henson, S., Masakure, O., & Cranfield, J. (2011). Do fresh produce exporters in sub-Saharan Africa benefit from GlobalGAP certification? *World Development*, 39(3), 375-386.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.

Hu, S., Hsu, C., & Zhou, Z. (2021). Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems*, 1-13.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1), 69-79.

Johns, G. (2006). The essential impact of context on organizational behavior. *Academy of Management Review*, 31(2), 386-408.

Johns, G. (2017). Reflections on the 2016 decade award: Incorporating context in organizational research. *Academy of Management Review*, 42(4), 577-595.

Johnston, A. C., & Warkentin, M. (2010). The Influence of Perceived source Credibility on end user attitudes and intentions to Comply with recommended it actions. *Journal of Organizational and End User Computing*, 22(3), 1-21.

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.

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective. *Information Systems Research*, 30(2), 687-704.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, 12(8), 3.

Kirsch, L. J., & Cummings, L. L. (1996). Contextual influences on self-control of IS professionals engaged in systems development. *Accounting, Management and Information Technologies*, 6(3), 191-219.

Kirsch, L. J., Ko, D.-G., & Haney, M. H. (2010). Investigating the antecedents of team-based clan control: Adding social capital as a predictor. *Organization Science*, 21(2), 469-489.

Kreutzer, M., Cardinal, L. B., Walter, J., & Lechner, C. (2016). Formal and informal control as complement or substitute? The role of the task environment. *Strategy Science*, 1(4), 235-255.

Kreutzer, M., Walter, J., & Cardinal, L. B. (2015). Organizational control as antidote to politics in the pursuit of strategic initiatives. *Strategic Management Journal*, 36(9), 1317-1337.

Liu, S. (2015). Effects of control on the performance of information systems projects: the moderating role of complexity risk. *Journal of Operations Management*, 36, 46-62.

Locke, K., & Golden-Biddle, K. (1997). Constructing opportunities for contribution: Structuring intertextual coherence and "problematizing" in organizational studies. *Academy of Management Journal*, 40(5), 1023-1062.

Lounsbury, M. (2002). Institutional transformation and status mobility: The professionalization of the field of finance. *Academy of Management Journal*, 45(1), 255-266.

Lounsbury, M., Steele, C. W. J., Wang, M. S., & Toubiana, M. (2021). New Directions in the Study of Institutional Logics: From Tools to Phenomena. *Annual review of Sociology*, 47, 261-280. doi:10.1146/annurev-soc-090320-111734

Martinsons, M. G., & Davison, R. M. (2016). People, places and time in research design and reporting: responding to commentaries on particularism. *Journal of Information Technology*, 31(3), 267-268.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340-363.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), 285-311. doi:DOI: 10.25300/MISQ/2018/13853

Morris, S. S., Zhong, B., & Makhija, M. (2015). Going the distance: The pros and cons of expanding employees' global knowledge reach. *Journal of International Business Studies*, 46(5), 552-573.

Musson, G., & Tietze, S. (2004). Places and spaces: The role of metonymy in organizational talk. *Journal of Management Studies*, 41(8), 1301-1323.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815-825.

Nigam, A., & Ocasio, W. (2010). Event attention, environmental sensemaking, and change in institutional logics: An inductive analysis of the effects of public attention to Clinton's health care reform initiative. *Organization Science*, 21(4), 823-841.

Ocasio, W. (2011). Attention to attention. Organization Science, 22(5), 1286-1296.

Ocasio, W., Thornton, P. H., & Lounsbury, M. (2017). *Advances to the institutional logics perspective The Sage handbook of organizational institutionalism* (pp. 509-531): SAGE Publishing.

Ouchi, W. G., & Maguire, M. A. (1975). Organizational control: Two functions. *Administrative Science Quarterly*, 559-569.

Pallas, J., Fredriksson, M., & Wedlin, L. (2016). Translating Institutional Logics: When the Media Logic Meets Professions. *Organization Studies*, 37(11), 1661-1684. doi:10.1177/0170840616655485

Parker, D. B. (1976). Computer abuse perpetrators and vulnerabilities of computer systems. Paper presented at the Proceedings of the June 7-10, 1976, national computer conference and exposition.

Pee, L. G., Woon, I. M., & Kankanhalli, A. (2008). Explaining non-work-related computing in the workplace: A comparison of alternative models. *Information & Management*, 45(2), 120-130.

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. doi:10.1080/07421222.2015.1138374

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 34(4), 757-778. doi:10.2307/25750704

Rao, H., Monin, P., & Durand, R. (2003). Institutional Change in Toque Ville: Nouvelle Cuisine as an Identity Movement in French Gastronomy. *American Journal of Sociology*, 108(4), 795-843. doi:10.1086/367917

Sandberg, J., & Alvesson, M. (2011). Ways of constructing research questions: gap-spotting or problematization? Organization, 18(1), 23-44.

Sarker, S. (2016). Building on Davison and Martinsons' concerns: a call for balance between contextual specificity and generality in IS research. *Journal of Information Technology*, 31(3), 250-253.

Scott, W. R. (1994). *Institutions and organizations: Toward a theoretical synthesis*. In W. R. S. J. W. Meyer (Ed.), Institutional environments and organizations: Structural complexity and individualism (pp. 55-80). Thousand Oaks, CA: Sage.

SEC. (2011). CF disclosure guidance, Topic:2. Retrieved from https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems*, 37(1), 129-161.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-502.

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.

Slavova, M., & Karanasios, S. (2018). When Institutional Logics Meet Information and Communication Technologies: Examining Hybrid Information Practices in Ghana's Agriculture. *Journal of the Association for Information Systems*, 19(9), 775-812. doi:10.17705/1jais.00509

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, 23(2), 200-217.

Stanton, J. M., Stam, K. R., Mastrangelo, P. M., & Jolton, J. A. (2006). Behavioral information security: An overview, results, and research agenda. In P. G. Zhang, DF (Ed.), Human-Computer Interaction and Management *Information Systems: Foundations* (pp. 276-294). Armonk, NY, USA: M.E. Sharpe.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276.

Suddaby, R., & Greenwood, R. (2005). Rhetorical strategies of legitimacy. *Administrative Science Quarterly*, 50(1), 35-67.

Thornton, P. H. (2002). The rise of the corporation in a craft industry: Conflict and conformity in institutional logics. *Academy of Management Journal*, 45(1), 81-101.

Thornton, P. H. (2004). *Markets from culture: Institutional logics and organizational decisions in higher education publishing*. Stanford, CA: Stanford University Press.

Thornton, P. H., & Ocasio, W. (2008). Institutional Logics. In C. O. R. Greenwood, K. Sahlin-Andersson, and R. Suddaby (Ed.), *The Sage handbook of organizational institutionalism*. Thousand Oaks, CA: Sage.

Thornton, P. H., Ocasio, W., & Lounsbury, M. (2012). *The institutional logics perspective: A new approach to culture, structure and process*. Oxford, UK: Oxford University Press.

Tilcsik, A. (2010). From ritual to reality: Demography, ideology, and decoupling in a post-communist government agency. *Academy of Management Journal*, 53(6), 1474-1498.

Vance, A., Eargle, D., Eggett, D., Straub, D. W., & Ouimet, K. (2022). Do Security Fear Appeals Work When They Interrupt Tasks? A Multi-Method Examination of Password Strength. *MIS Quarterly*, 46(3), pp. 1721-1738.

Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing Accountability Through User-Interface Design Artifacts. *MIS Quarterly*, 39(2), 345-366.

Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & Management*, 57(4), 103212.

Watson, T. J. (2004). HRM and critical social science analysis. *Journal of Management Studies*, 41(3), 447-467.

Weber, M., Gerth, H. H., & Mills, C. W. (2013 (first published in 1946)). *From Max Weber: essays in sociology*. New York, NY: Oxford University Press.

Westphal, J. D., & Zajac, E. J. (2001). Explaining institutional decoupling: The case of stock repurchase programs. *Administrative Science Quarterly*, 46, 202-228.

Wijen, F. (2014). Means versus ends in opaque institutional fields: Trading off compliance and achievement in sustainability standard adoption. *Academy of Management Review*, 39(3), 302-323.