



Discovering the Emergence of Technical Sociology in Human Capital Systems and Technology-Driven Organizations

Darrell Norman Burrell, The Samuel D. Proctor Institute for Leadership, Equity, and Justice, USA*

 <https://orcid.org/0000-0002-4675-9544>

Calvin Nobles, Illinois Institute of Technology, USA

 <https://orcid.org/0000-0003-4002-1108>

ABSTRACT

In 2019 the global cost of cyber-crime was over 2 trillion dollars. Current research literature outlines that 80-90% of security breaches are due to human-enabled errors in the U.S. and the U.K. Organizations encounter a barrage of cybersecurity threats that prey on the propensity of human error, human inaction, human behavior, and human misbehavior. As a result, there is an emergence of a new area of research development around technical sociology or digital sociology as a domain to explore the human capital perspectives, group dynamics, and social aspects of cybersecurity and technology management. The paper uses a relational content analysis of the literature as the research approach aimed to determine the presence and relationships of common themes and concepts. The results were creation of a concept matrix model of interrelated co-occurring concepts. The approach used was outlined by Krippendorff who asserts that concepts are “ideational grains”; these grains can be thought of as emblems which develop connotation through their connections to other emblems.

KEYWORDS

Automation, Cybersecurity, Human Factors Cybersecurity, Human-Computer Interaction, Organizational Behavior, Sociology, Technical Sociology, Technological Resistance to Change, Technology Management

INTRODUCTION

In 2019 over 2 trillion was the global cost of cybersecurity crime (Morgan, 2016). In the U.S. and U.K., mistakes and poor decision making on the part of employees account for up to 90% of the information security breaches (Maglaras, He, Janicke, & Evans, 2016). Humans are notably the weakest link in security and risk management because organizations struggle to understand and mitigate behavioral-based risk in information security (Alavi, Islam, & Mouratidis, 2016; Proctor & Chen, 2015). Human factors study social interaction with information systems, networks, and practices in an information security environment (Alavi, Islam, & Mouratidis, 2016). The increase in cyber-attacks, the need to protect critical organizational data, and demand for organizations to

DOI: 10.4018/IJHCITP.300324

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

leverage data for competitive advantage have pushed a necessity to explore the impact of technology in new ways and from new perspectives.

According to Nobles (2018), cybersecurity, computer science, and information technology certification and training programs have failed to implement program content to address organizational behavioral factors, change management perspectives, and human factors in cybersecurity. This incongruence can create a developmental new domain of technical sociology. Technical sociology provides a diagnostic and investigative context for comprehending the social frameworks around technological human interaction, technology adoption, technological resistance, the overuse of technology, the misuse of technology, change management, and human error around the use of technology. This new domain draws from the traditional sociological matters and human-computer interaction issues around employee groups, organizations, and workers that manage and use technology. This domain is concerned with sociological research and its implications for improving technology management's professional practice through a lens of interconnected social systems, organizational systems, and individual systems.

To understand and explore the nature of technology and its hazards requires an understanding that social science theory attempts to explore social dynamics and its basic set of relations to explain how distinct phenomena function (Burton, 2019; Burton, 2017). Therefore, social science theorizing or formulation and modifications of those interpretative explanations is an ongoing process of observing and analyzing applied scientific knowledge and its intersection with everyday interaction (Newman, 2018). Sociology theory is the inquiry of interpersonal relationships in ways that attempts to explain people's relation to their social, organizational, and individual systems (Newman, 2018). Whether employees are experiencing technology, technological innovations, technological hazards, they encounter a set of interpretive assumptions. These assumptions are defined within the context of a particular organizational cultural setting, which accounts for what occurs and how it occurs (Burton, 2019). Thus, the sociology theory's comprehension is neither strictly abstract nor distinctly practical; it's an intersection of both (Newman, 2018).

Furthermore, the foundation or emergence of technical sociology is a process by which individuals explain and interpret their relationship to various aspects of technology in their physical and social environments. Thus, comprehending the value of technical sociology as an area for needed research and exploration requires understanding the phenomenon manifested through the relationships in various societal and organizational institutions.

In sociology, this comprehension is often explained and explored in several ways. One way could be a general theory that conceptualizes societal and organizational institutions as a functioning interconnected system (Jaccard & Jacoby, 2009). Two, a general philosophy that focuses on societal and organizational institutions as dynamic, changing, conflict-heavy systems driven by intense competition and exploitation (Jaccard & Jacoby, 2009). Three theories deal with social interactions and their implications on shaping the views, beliefs, and behaviors of those in societal and organizational institutions (Jaccard & Jacoby, 2009). Technical sociology as a framework makes sense for a variety of reasons. It looks at human, information systems, and technology interaction through the collective aspects of decision-making behaviors and practices from a social network, organizational system, and individual systems in ways that attempt to understand their relationships.

Kraemer and Carayon (2007) outlined that poor decision making made by employees and mistakes as the human error or people component around cybersecurity, which is, "Any action leading to an undesired result." Often, employees are tricked by an outsider into engaging in problematic behavior and may not mean to cause an adverse event for the organization (Van- Zadelhoff, 2016). The result is often human error or mistakes in human decision making that create information security problems and technology use problems in organizations (Van-Zedlhoff, 2016; Nobles, 2018). Metalidou (2014) outlined that human mistakes account for a more prominent weakness than technology in organizations, which provides a level of evidence that technology alone is not a comprehensive approach to managing cyber and information security risks (Dykstra, 2017; Nobles, 2018).

These trends make it critical for emerging research and discourse in the domain of technical sociology as an area of exploration around the social consequences and causes of human interactions around technology. This discourse aims to understand the nature of social systems around human error and human behavior as a significant factor in creating productive organizational cultures that can better manage information security risks and incidents.

Technology managers, within most organizations readily admit that cybersecurity is one of their biggest concerns (Nobles, 2018). Many in these roles are still look at cybersecurity as only a technologically driven issue and often underestimate the importance of engaging people and changing the social systems that build more cyber-aware culture among their employees and senior-level management (Nobles, 2018). Its social norms more broadly define organizational culture. Creating an organizational culture where employees understand their role in the minimization of information security risks requires a shift from technology-driven solutions to employee engagement, and organizational development ones demand a change in the way organizations treat security (Goel, Williams, & Dincelli, 2017). Many organizations fail to fully understand the risks of people's actions and inactions around cybersecurity (Nobles, 2018). Organizations often lack the required expertise to understand what an active cybersecurity culture should look like or how to develop the social learning systems necessary to have a fully engaged cyber-aware workforce (Nobles, 2018). When it comes to improving your organization's ability to guard against cyber threats, the best defensive strategy is creating a cybersecurity culture in the workplace that is driven by effective social learning systems that understand how to maximize the interaction between technology, its uses, and people (Nobles, 2018).

OBJECTIVES/RESEARCH GOALS

- This inquiry goal is developmental and exploratory in ways seeking to combine concepts and frameworks that are currently existing in soloed disciplines but are interconnected.
- The intent is to explore the nature of human social relationships in the workplace around cybersecurity and technology management to understand how the introduction of technology shapes human action and consciousness shape.
- An aim is to create a draft framework for a discussion around the need to understand the complex intersection between technology management and sociology around cybersecurity and information security.
- A goal is to understand how organizational behavior can be influenced by the complex social forces and interconnected social factors that affect technology adoption, technology resistance, technology acceptance, and technology management in complex organizations.
- The intent is to engage in a dialog around technical sociology as a viable area for future research and discourse around cybersecurity, human-computer interaction, and technology management systems.
- An aim is to look at organizational behavior around technology management from a social science vantage point.

METHODS

This research inquiry is a content analysis of theoretical literature and previous research around social systems in cybersecurity, technology management, and organizational behavior. This kind of approach has value for scholar-practitioners engaged in business process improvement in organizations because it explores and combines dispersed research. The paper uses a relational content analysis of the literature as the research approach aimed to determine the presence and relationships of common themes and concepts. The results were creation of a concept matrix model of interrelated co-occurring concepts. The approach used was outlined by Krippendorff (1980) who asserts that concepts are

“ideational grains;” these grains can be thought of as emblems which develop connotation through their connections to other emblems.

Method for Reviewing the Literature for the Content Analysis

A dynamic literature search commenced in a way that involved a systematic search for studies and aims for a transparent report of study identification. Over 188 peer-reviewed articles/documents were evaluated and reviewed from keyword searches that included the concepts of human factors, human-computer interaction, management information systems, business information systems, technology acceptance, automation, technological resistance to change, human relations, technology management, social science, sociology, organizational behavior, cybersecurity, information security, cyber risk management, human error, change management, and organizational culture with an emphasis of these terms in the context of technology in organizations. This keyword search was generated from an initial review from a list of some of the most highly cited articles from Google Scholar, highly downloaded articles from Academia.edu, and highly downloaded articles from Research Gate in cybersecurity, technology management, and information technologically as a baseline search topic. These keywords evolved from a scan of abstracts where these words were frequent. After the keywords were established, articles that were reviewed came from the following databases. Their hosts (shown in parentheses) included *ACM* Digital Library, ABI Inform Complete (ProQuest), Academic Search Premier (EBSCO), Business Source Premier (EBSCO), ERIC (EBSCO), DOAJ (Directory of Open Access Journals), KESLI-NDSL (Korean National Discovery for Science Leaders), Baidu Scholar, WorldCat (OCLC), The Indian Citation Index, Index Copernicus International, and Google Scholar. Usage of these databases allowed a degree of assurance about the authority of the data retrieved. The literature content analysis went through a rigid, meticulous, and controlled evaluation process.

LITERATURE REVIEW

Based on current and emerging literature (Nobles, 2018; Burton, 2019; Burton 2017; Burrell, 2018; Burrell, Diperi, Weaver, 2020), understanding the people aspects of organizational social systems influences the introduction of cybersecurity best practices includes:

1. Outlining cyber and data security risks. Outlining these risks requires engaging in creating social learning systems and networks where those with expertise can share knowledge and educate others. Without proper recognition and identification of risks, it can be hard to change the social systems that create a strong cybersecurity organizational culture.
2. Active organizations share cybersecurity best practices with all employees in various formats for creating the proper environment. This level of sharing is about engaging people to understand the ideal best practices social and the desired organizational system.
3. Educate employees on the actual costs and impacts of cybersecurity breaches.
4. Educate employees on the crucial role that employee actions and behaviors can provide both positive and negative consequences in cybersecurity breaches.
5. Communicate through a variety of methods with employees to encourage transparency. Communication is useful when it clarifies why specific procedures and policies are in place and what they mean to safeguard the organization.
6. Creating a strong and effective cybersecurity culture means engaging organizational and individual social systems in ways that continually test how well employees are following protocols.
7. It is creating an organizational systems culture where employees feel comfortable about questions around cybersecurity. Organizational cultural change about creating a highly responsive and open environment that encourages employees at all levels are encouraged and comfortable talking about cybersecurity issues with cybersecurity experts.

8. Creating cybersecurity training focused on positive organizational and individual change. This training should engage all employees with the goal of the following:
 - a. Teaching all employees proper security behavior.
 - b. Teaching all the right protocols and procedures to follow.
 - c. Teaching employees what to do if there is a breach.
 - d. Teaching employees their role in data security.
 - e. Teaching employees about the nature of common threats.
 - f. Explaining to employees whom to contact with their issues, questions, and concerns around cybersecurity.
 - g. Comprehensively explaining why following organizational procedures and protocols is vital.

THE SOCIOLOGICAL ASPECTS OF HUMAN FACTORS

An organization's business strategy should encompass, creating a sufficient information security-oriented organization (Van-Zedlhoff, 2016). There is a critical need to understand the levels of engagement that create policies that perpetuate a culture where employees will realize their roles and responsibilities in organizational information security (Albrechtsen, 2007). According to Ritzer (2015), social science research frames how interpersonal interactions have significant complexity and try to effectively balance personal goals and values from organizational goals and values. Workers are socialized into many of the habits that they formulate in the organization (Ritzer, 2015). According to symbolic interaction framework, organizational culture is created, shaped, maintained, and structured through the everyday behaviors and interactions by the members of the organization (Hegar, 2011). Ultimately, creating an enlightened security culture requires employee engagement and organizational development approaches to educate all employees, not just those information technology, on the social consequences and social causes of proper and improper human behavior concerning information and cybersecurity (Buckhead, 2014). A historical content analysis outlines the nature of social forces and human factors that influence poor actions or neglectful inaction on the part of employees around information and cybersecurity (Van-Zedlhoff, 2016). Organizational social and learning cultures that fail to develop practical information security training fail to instill in all employees that cybersecurity is everyone's responsibility, or that fail to help people understand risks are examples of note (Van-Zedlhoff, 2016).

Researchers and practitioners postulate that the impact of malicious cyber activity targeting humans remains underexplored in existing research (Mancuso, Strang, Funke, & Finomore, 2014). Mancuso et al. (2014) acknowledge that the current research gap in human performance and behavior in cybersecurity requires urgent attention from social factors practitioners and psychology-based experts.

Risk management is the key to creating an active information security culture that can limit information security intrusions (Van-Zedlhoff, 2016). People and their behaviors, not technology, are the most significant risks to be managed around creating social, organizational cultures that support safe security behaviors over risky or complacent ones (Albrechtsen & Hovden, 2010; Buckhead, 2014). According to Dhillon (2001), Schultz (2005), and Buckhead (2014), more research is needed around the social forces, and human factors that influence why some people are information security compliant and others are not. This research could add content around emerging discourse in the domain of technical sociology.

Theory of Planned Behavior

Ajzen (1991) framed the fundamental theory of planned behavior (TPB), which outlines the social forces and human factors that influence behavioral actions. The TPB provides a lens for understanding the cognitive and motivational influences around a person's decision-making processes around deciding to act (Ajzen, 1991). TPB has a viable application to understanding the nature and manifestation of technical sociology around exploring employee behaviors, human factors, and organizational business

strategy around cybersecurity and information security. The ability to positively influence employees' social and group behavior is critical to creating an organizational culture that effectively manages and addresses cybersecurity risks that require more exploration from social interaction and professional relationship contexts (Nobles, 2018; Burton, 2019; Burton, 2017).

Risk Information Seeking and Processing (RISP) Model

The Risk Information Seeking and Processing (RISP) model of information behavior (Griffin, Dunwoody, & Neuwirth, 1999) aims to predict information seeking and processing based on information sufficiency, or the assessment that current knowledge meets a threshold of confidence that an individual would like to have about a particular risk. This model has some very relevant applications around human factors, human error, and social behavior around cybersecurity. According to Griffin, Dunwoody, and Neuwirth (1999), the perception of subjective informational norms is theorized to influence the understanding of information sufficiency, such that an individual's belief that others expect her to know more than she does about a topic could ultimately drive information-seeking behavior. The understanding of a cybersecurity hazard should predict information (in) sufficiency and thus lead to the data seeking, although this relationship is mediated by the individual's affective response (such as fear or concern) regarding that hazard (Nobles, 2018). In basic terms, this means that knowledge, comprehension, and experience influence a person's understanding and perception of risk and confidence in managing that risk (Griffin, Dunwoody, & Neuwirth, 1999).

The RISP model is particularly relevant for explaining employees' information and social behaviors around the complex sociological nature of human-computer interaction. This model has utility in including both perceived hazard characteristics and affective response around cybersecurity risks and the behaviors required to protect the organization from those risks. It is possible that even the presence of very severe cybersecurity risks (which would drive information seeking about the aspects of those risks). The RISP model provides a framework to explore the manifestation of perceived hazard characteristics. The RISP model is useful in explaining information and social behaviors around areas like human error, security fatigue, and paranoia around the ability to manage cyber and information security organizational risks. The RISP model provides a typology of behaviors related to how vital information and data are handled, processed, and maintained in complex social, organizational systems (Griffin et al., 1999).

Applied Sociological Aspects of Change Management

Change management is all about understanding and managing the social and organizational systems that can influence change around how technology and information security are managed within an organization. Kotter (2012) stated that leadership must present its people with an understanding of change; if the information provided is compelling and logical, an avenue can exist. A change is a process of moving from one defined state to another, i.e., every improvement occurs with a product, method, or system (Anderson & Anderson, 2010). Change management is a socially dynamic process concerning behaviors and interactions around the management of change (Cameron & Green, 2015; Worley & Mohrman, 2014).

The change management process's primary objective is to remove resistance by engaging users and managers early in the process and before implementation (Turner & Rindova, 2012). Building awareness of the purpose and value of the initiative can result in positive attitudes and perspectives, and ultimately the willingness to relinquish the former ways of conducting business and embrace new technologies and processes (Cameron & Green, 2015). As new cyber threats arise, managers who can effectively manage the social and organizational systems around change concerning technology management are paramount from a social aspect of the behaviors, actions, and practices of people (Nobles, 2018).

Kotter's (2012) model delineates eight steps in the change process.

Creating a Climate for Change

1. **Increase Urgency:** Helping others see the need immediately change.
2. **Build a Guiding Team:** Assembling a group of people with the necessary power and influence to collectively lead organizational change.
3. **Develop the Right Vision:** Creating a clear vision and developing strategies for achieving that vision.

Engaging and Enabling the Organization

4. **Communicate for Buy-in:** Making sure as many as possible understand and accept the vision and the strategy.
5. **Enable Action:** Identifying and removing obstacles to change.
6. **Create Short-term Wins:** Identify and plan for early and visible achievements and recognize and reward employees involved.

Implementing and Sustaining Change

7. **Hold Gains, Build on Change:** Building and using organizational change management successes to increase buy-in and people's commitment to effective organizational change.
8. **Institutionalize Change:** Celebrating and publicizing the impact of change in ways that allow everyone in the organization to understand how the effective implementation of change can lead to more productivity and organizational success (Kotter, 2012).

Models of Behavior Change

Prochaska's (2013) Transtheoretical Model of Behavior Change can provide a context to understand the social forces and human factors around technology management and creating active information security cultures. Prochaska's (2013) Transtheoretical Model of Behavior Change outlines strategies that help people make and maintain changes, including cybersecurity and technology management, including:

1. **Consciousness Raising:** Increasing awareness about proper or appropriate behaviors.
2. **Dramatic Relief:** Emotional arousal about the proper or appropriate behaviors, whether positive or negative arousal.
3. **Self-Reevaluation:** This is about realizing and understanding the proper or appropriate behaviors that are part of whom they want to be.
4. **Environmental Reevaluation:** Social reappraisal to realize how their improper or inappropriate behaviors affect others.
5. **Social Liberation:** This is the environmental opportunities that exist to systems support or encourage proper or appropriate behaviors.
6. **Self-Liberation:** Obligation to change behavior based on the trust that attainment of the suitable or fitting performances is probable.
7. **Helping Relationships:** Establishing cooperative social relationships that provide a positive influence for change or performance improvement.
8. **Counter-Conditioning:** Substituting proper or appropriate behaviors over the thoughts for improper or inappropriate behaviors and practices.
9. **Reinforcement Management:** This is about rewarding superior performance and constructively addressing undesired performance or behaviors without lenience.
10. **Stimulus Control:** This is about creating cultures that underpin correct performance and proper behavior and that confront behavior that is unacceptable or improper (Prochaska, 2013; Prochaska, Prochaska, & Levesque, 2001).

Dhillon's (2001) study of human behavior and interactions in organizations outlines the importance of organizational development actions, interventions, and practices that create appropriate the social systems, organizational systems, individual systems around the integration of innovations, new technologies, new processes, existing process improvement, and further training implementation around technology management (Dhillon, 2001). Exploring research in social science contexts provides a rationale for understanding the human interaction between technology and people.

Implementing change can cause resistance and pushback from stakeholders and other parties of interest (Appelbaum, Habashy, Malo, & Shafiq, 2012). The idea of change can be alarming because it can impose major or minor disruptions that can lead to delays or setbacks (Kotter, 2012). Change initiatives can alter systems that could cause potential concerns that can affect other business units (Senge, 2014). Stakeholders must understand the process and future resistance systematically to make a logical approach to change (D'Ortenzio, 2012). A holistic approach change management can also be devalued because, typically, stakeholders who hold a leadership role often lead and provide all the implementation of the change process (Kotter, 2012). The change process can be more receptive to employees if the stakeholders also involved participants as subject matter experts and are included in the various aspects of the change management (Burton, 2019).

Emerging research in the domain of technical sociology can help with understanding why people resist the adoption and use of new technology or fail to properly follow information security protocols (Young & Leveson, 2013). Lawton (1998) outlined that many security violations are based on social forces and human factors that describe that violations are often the manifestation of employees that are just trying to meet deadlines and get work done. Short deadlines, emphasis on higher worker productively, and increased job duties that force employees to seek ways to complete work projects create human error risks and poor decision making in organizations (Young & Leveson, 2013; Buckhead, 2014; Lawton 1998).

It is imperative to change the philosophical viewpoint on human error by welcoming by adding training in change management, organizational behavior, and human-enabled error perspectives in cybersecurity (Nobles, 2018). It is critical to align influential social forces that create cultures that encourage information security diligence, and compliance is essential to cybersecurity risk management success (Albrechtsen & Hovden, 2010; Buckhead, 2014). Alfawaz et al. (2010) outlined the importance of employee engagement in creating organizational cultures where social forces perpetuate proper employee conduct and compliance. Management needs to ultimately help everyone commit to realizing that information security and cybersecurity are everyone's jobs, not just those with information technology job titles (Nobles, 2018). According to Buckhead (2014), organizational leaders need to perpetuate a climate where everyone feels a sense of personal ownership in activities that mitigate all elements of information security risk. Coffey (2017) points to the weakness of cybersecurity training as a comprehensive approach to improve employee behavior and employee commitment concerning risk management and risky decision making. Active organizations need to engage and develop people in ways that create an organizational learning culture (Coffey, 2017). Having an involved social learning culture looks to capitalize on people's relationships and social systems to assist cybersecurity and technology managers in more effectively managing cybersecurity plans, risks, incidents, and responses in ways that leverage the interaction between technology and sociology.

Sociology of Diffusion of Innovation

The diffusion of innovation, as posited by theorist Everett Rogers (2003), pushed to describe how innovations are adopted, integrated, and accepted in a population. Rogers (2003) asserted that an innovation is an idea, behavior, or object that its audience perceives as new. The diffusion of innovation is where an innovation has disseminated within a field, progressively, and among those that embrace the innovation (Crawford & Di Benedetto, 2008). The related concept explored processes

at the individual level, where diffusion refers to embracing technology in an anytime and anyplace environment (Crawford & Di Benedetto, 2008).

Rogers (2003) groundbreaking research set the mode for predictions about the process of social change. Rogers examined how innovations communicated and adopted within a social system over time evolve (2003). Since this communication involved a new idea or innovation, the theory suggests five characteristics of innovation perception. These characteristics explained why different innovations were adopted at varying rates. The five aspects are relative advantage, computability, complexity, tri-ability, and observability (Rogers, 2003). The net effect of these characteristics is the now-familiar stages of innovation that include innovators, early adopters, early majority, late majority, and laggards (Rogers, 2003). These stages of adoption describe incremental change following a bell curve pattern (Rogers, 2003). Organizations with technology managers attempting to get non-technical employees to create an organizational culture focused on cybersecurity must understand the complex social nuances of Rogers's perspective (2003).

Davis (1989) defined diffusion as the process by which technology extends across a population of organizations. Davis' Technology Acceptance Model (Davis, 1989) and Roger's Diffusion of Innovation theory (2003) explore social systems on an individual and organizational level around technology adoption, technology integration, technology resistance, and the complexities around change. Understanding the complex nature of cultural change and innovation adoption is critical to comprehending the complex social dynamics around addressing cybersecurity organizational risks from a context of the interaction between technology and sociology.

The Status Quo Bias Theory

Kim and Kankanhalli (2009) postulated the Status Quo Bias Theory, which essentially says that employees will resist and even question the need or utility of new technology due to their comfort and familiarity with an existing technology or approach. This occurrence of resistance is driven by a longing to stick with the status quo (Kim & Kankanhalli, 2009). A social science context considers that people display a bias towards preferring existing habits and processes over the choice to engage in new ones (Polites & Karahanna, 2012). In the context of Status Quo Bias Theory, the introduction of new technologies often leads to resistance because people magistrate a verdict to adopt a new technology or process as a cost adjunct accompanying the latest technology (Kim & Kankanhalli, 2009; Polites & Karahanna, 2012). Understanding the social system nuances of behavioral change is critical in developing productive cyber security-oriented cultures and security compliant employees (Nobles, 2018).

INFORMATION TECHNOLOGY CONFLICT-RESISTANCE THEORY

I.T.I.T.Meissonier and Houzé (2010) suggested that information technology (I.T.) Conflict-Resistance theory proposed that two sets of assumptions, conflict theory, and resistance theory, as relevant theories t.I.T.gh which to understand resistance (Meissonier & Houzé, 2010). The I.T. conflict-resistance theory explores the complex nature of social systems around organizational behavior in a pre-implementation context. Meissonier and Houzé (2010) outline the critical importance of organizational behavior around employee engagement to address conflict and resistance to adopting and utilizing new technologies. Meissonier and Houzé (2010) argue for proactive organizational and managerial intervention through comprehension of the social and organizational systems around conflict and technological resistance. Effective organizational cultural change management means that new processes, approaches, and protocols around cybersecurity and information security should be vetted to a level where complex consequences of integration are considered and planned for in advance (Nobles, 2018).

TECHNOLOGY ACCEPTANCE MODEL (TAM)

The Technology Acceptance Model (TAM) provides a viable framework to explore the social and organizational systems around technology management and information security (Cheung & Vogel, 2013). TAM described a series of incremental cognitive adjustments that individuals make to accept new technology. The model built on two factors that influence acceptance perceived usefulness and perceived ease of use (Cheung & Vogel, 2013). These two factors affected the attitude and intention to use or acceptance of technology (Cheung & Vogel, 2013). Davis (1989) outlined that people will embrace or cast off newly introduced technology if they find the technology more user-friendly and comfortable to grasp. Organizational and social dynamics around technology acceptance, technology management, and new technology introductions have significant managerial and human capital implications around technology utilization and implementation (Burton, 2019). Exploring and understanding these perspectives requires intense study of the actions, behaviors, and interactions of people from the world of research and the world of practice in the areas of social science, human factor psychology, cybersecurity, human-computer interaction, technology management, and organizational behaviors (Nobles, 2018).

CONCLUSION

Pfeffer and Sutton (2000) avow that so often, organizations prefer to talk, conceptualize, and rationalize about issues and organizational dynamics rather than confront them directly. Human social behavior within the organization is impacted by organizational behavior (Lussier, 2016). The organizations that embrace, introduce, and utilize new technologies are affected in a two-fold manner: (a) by the individual behavior within the organization; and (b) by the organization impacting the behavior of the individuals in the organization (Lussier, 2016). Organizational social behavior changes human behavior (Lussier, 2016). When social behavior is altered, habits and thinking are changed (Lussier, 2016). And when the social aspects of behavior, practices, and thinking change, human performance can improve the organization (Lussier, 2016). Correspondingly, the organization can impact the performance and behavior of employees (Lussier, 2016).

The contingency approach is a theoretical perspective that serves as the theory-practice gap (Lussier, 2016). This theory outlines that organizational effectiveness results from aligning organizational characteristics (i.e., structure, environment, organizational size, and organizational strategy) to contingencies that augment the situation of the organization (Lussier, 2016).

Contingency thinking provides a lens for understanding the existence of human dynamics and social behaviors around technology by offering leaders a way to thoroughly analyze the interrelationship between internal needs and external conditions within an organization (Lussier, 2016). The contingency theory perspective is grounded in the ideology that recognizes social behavior in an organization and its impact on performance. The complex result of many micro and macro behaviors and the way someone behaves in the organization is contingent on the many different variables present (Lussier, 2016).

For an organization to be both efficient and effective, the structures of the organization should be designed to react to the various contingencies that shape the organization, and the decision(s) regarding the organization should be dependent on the particular situations that the organization faces (Lussier, 2016). Improving performance comes from a multiplicity of facets, yet none more critical than the ones derived from the actions of human social behavior guided by the organizational systems and structures in which the leader and the organization create (Lussier, 2016). High-performing organizations do not emerge by accident but rather through the intentional focus and direction of both human and organizational behavior (Lussier, 2016). The understanding of human factors and human social behavior becomes critical as more organizations become more technologically reliant and more technically focused (Nobles, 2018).

Technical sociology provides a critical perspective to explore the social contexts and dynamics around technological human interaction, technology adoption, technological resistance, and the overuse of technology, the misuse of technology, change management, and human error around the use of technology. An exploration of various domains of the literature provides allows for the understanding of the interconnected and complex aspects around the emergence of technical sociology as an area of human-computer interaction field of potential significance.

The Burrell Technical Sociological Framework Model developed through a content analysis of the literature provides a roadmap with contexts to explore in the domain of Technical Sociology. Table 1 D. Burrell Technical Sociology Framework Model (2020) outlines a conceptual model of the provinces of human behavior that can be explored or classified within an understanding of the importance and human capital utility of Technical Sociology as an important area for future specialized research emphasis.

RECOMMENDATIONS FOR FUTURE RESEARCH OR FUTURE WORK

Significant further research could include various exploratory qualitative studies focused on the views of different job roles, genders, and multi-levels of a hierarchy concerning the manifestations, perceptions, and organizational importance of the various providences in the Technical Sociology Framework Model.

Table 1. D. Burrell Technical Sociology Framework Model (2020)

Complexity variables	D. Burrell Technical Sociology Framework Model (2020)
Province 1	Technological human-computer interaction and the implications around those interactions on social systems, organizational systems, and individual systems in ways focused on enhanced usability, augmented learning, communication facilitation, and information analysis.
Province 2	The social perspectives around technology adoption and the rate and speed of how that technology is introduced.
Province 3	Technological resistance to change and its manifestation within social systems, organizational systems, and individual systems
Province 4	The overuse of technology and the overreliance on technology and its implications on social networks, organizational systems, and individual systems.
Province 5	The misuse of technology and its implications for social systems, organizational systems, and individual systems
Province 6	The social networks, organizational systems, individual systems applications of change management approaches around the integration of new innovations, new technologies, new processes, existing process improvement, and further training implementation around technology.
Province 7	The exploration of human factors and human error around the use of technology on social systems, organizational systems, and individual systems
Province 8	The comprehension of the factors around problems within social networks, organizational systems, and individual systems related to data management, data usage, and data overload.
Province 9	Security complacency explores the social forces and human factors that influence employees to relax their vigilance around adequate information security and cybersecurity behaviors
Province 10	Technology fatigue, which outlines the social systems around employee frustration with the rapid introduction of new technologies and frustrations around the learning curve, is required to utilize each new technology fully.

Future research could use a qualitative case study approach to find the best practices concerning organizational development and engagement concerning the various providences in the Technical Sociology Framework Model.

Future research could also ascertain why some organizational behaviors are perceived with greater importance than others, these data findings at minimal may give practitioners and researchers invaluable information about what is impacting performance at the micro and macro level attempting to address complex organizational issues around technology use, technology orientated risks, and technology integration.

FUNDING AGENCY

Publisher has waived the Open Access publishing fee.

REFERENCES

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. doi:10.1016/0749-5978(91)90020-T
- Alavi, R., Islam, S., & Mouratidis, H. (2016). An information security risk-driven Investment model for analysing human factors. *Information & Computer Security*, 24(2), 205–227. doi:10.1108/ICS-01-2016-0006
- Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behavior through dialogue, participation, and collective reflection. An intervention study. *Computers & Security*, 29(4), 432–445. doi:10.1016/j.cose.2009.12.005
- Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: A Behavior compliance conceptual framework. *Eighth Australasian Information Security Conference*, Brisbane, Australia.
- Anderson, D., & Anderson, L. A. (2010). Beyond change management: How to achieve breakthrough results through conscious change leadership. John Wiley & Sons.
- Appelbaum, S. H., Habashy, S., Malo, J. L., & Shafiq, H. (2012). Back to the future: Revisiting Kotter's 1996 change model. *Journal of Management Development*, 31(8), 764–782. doi:10.1108/02621711211253231
- Blair, T. (2017). *Investigating the cybersecurity skills gap* (Order No. 10623377). Available from ProQuest Dissertations & Theses Global. (1989786177). Retrieved from <http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1989786177?accountid=27203>
- Burkhead, R. L. (2014). *A phenomenological study of information security incidents experienced by information security professionals providing corporate information security incident management* (Order No. 3682325). Available from ProQuest Dissertations & Theses Global. (1657429053). Retrieved from <https://search-proquest-com.contentproxy.phoenix.edu/docview/1657429053?accountid=35812>
- Burrell, D. N. (2018). An Exploration of the Critical Need for Formal Training in Leadership for Cybersecurity and Technology Management Professionals. *International Journal of Hyperconnectivity and the Internet of Things*, 2(1), 52–67. doi:10.4018/IJHIoT.2018010105
- Burrell, D. N., Diperi, D. L., & Weaver, R. M. (2020). Creating Inclusive Cultures for Women in Automation and Information Technology Careers and Occupations. *International Journal of Business Strategy and Automation*, 1(2), 37–51. doi:10.4018/IJBBSA.2020040104
- Burton, S. L. (2017). *Leadership Shifts: Perceptions and Consequences, In-person, or Cyber*. In *Encyclopedia of Strategic leadership and Management*. IGI Global. doi:10.4018/978-1-5225-1049-9.ch028
- Burton, S. L. (2019). Grasping the Cyber-World: Artificial Intelligence and Human Capital Meet to Inform Leadership. *The International Journal of Economics, Commerce, and Management United Kingdom*, VII, 707–759.
- Cameron, E., & Green, M. (2015). *Making sense of change management: A complete guide to the models, tools, and techniques of organizational change*. Kogan Page Publishers.
- Cheung, R., & Vogel, D. (2013). Predicting user acceptance of collaborative technologies: An extension of the technology acceptance model for e-learning. *Computers & Education*, 63, 160–175. doi:10.1016/j.compedu.2012.12.003
- Clegg, S., & Bailey, J. R. (Eds.). (2007). *International Encyclopedia of Organization Studies*. Sage Publications.
- Coffey, J. W. (2017). Ameliorating Sources of Human Error in Cyber Security: Technological and Human-Centered Approaches. In The 8th International Multi-Conference on Complexity, Informatics, and Cybernetics, Pensacola (pp. 85-88). Academic Press.
- Crawford, M., & Di Benedetto, B. A. (2008). *New products management*. McGraw-Hill/Irwin.
- D'Ortenzio, C. (2012). *Understanding change and change management processes: A case study* (Doctoral Thesis). University of Canberra. Retrieved to <https://www.canberra.edu.au/researchrepository/items/81c02a90-6a15-91ae-c7a2-ff44c96d60b2/1/>

- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Management Information Systems Quarterly*, 13(3), 319–340. doi:10.2307/249008
- Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, 20(2), 165–172. doi:10.1016/S0167-4048(01)00209-7
- Dykstra, J. (2017). *Cyber Issues Related to Social and Behavioral Sciences for National Security*. The National Academies. Retrieved from: https://sites.nationalacademies.org/cs/groups/dbasssite/documents/webpage/dbasse_177250.pdf
- Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behavior as an aspect of cybersecurity assurance. *Security and Communication Networks*, 9(17), 4667–4679.
- Goel, S., Williams, K., & Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability. *Journal of the Association for Information Systems*, 18(1), 2.
- Griffin, R. J., Dunwoody, S., & Neuwirth, K. (1999). Proposed model of the relationship of risk information seeking and processing to the development of preventive behaviors. *Environmental Research*, 80(2), S230–S245.
- Hegar, K. (2011). *Modern Human Relations at Work*. South-Western Publishing.
- Kim, H. W., & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. *Management Information Systems Quarterly*, ●●●, 567–582.
- Kotter, J. P. (2012). *Leading change*. Harvard Business School Press.
- Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38, 143–154.
- Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28, 509–520.
- Krippendorff, K. (1980). *Content Analysis: An Introduction to its Methodology*. Sage Publications.
- Lawton, R. (1998). Not working to rule: Understanding procedural violations at work. *Safety Science*, 28(2), 77–95.
- Lussier, R. (2016). *Human Relations in Organizations: Applications and Skill Building*. McGraw Hill.
- Maglaras, L., He, Y., Janicke, H., & Evans, M. (2016). *Human Behaviour as an aspect of Cyber Security Assurance*. Academic Press.
- Mancuso, V. F., Strang, A. J., Funke, G. J., & Finomore, V. S. (2014, September). Human factors of cyber-attacks: A framework for human-centered research. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 58(1), 437–441.
- Meissonier, R., & Houzé, E. (n.d.). Toward an I.T. conflict-resistance theory: Action research during I.T. pre-implementation. *European Journal of Information Systems*, 19(5), 540–561.
- Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia: Social and Behavioral Sciences*, 147, 424–428.
- Morgan, S. (2016, May 13). Top 5 industries at risk of cyber-attacks. *Forbes*.
- Newman, D. (2018). *Sociology: Exploring the Architecture of Everyday Life*. Sage.
- Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, 9(3), 71-88. 10.2478/hjbpa-2018-0024
- Pfeffer, J., & Sutton, R. I. (2000). *The knowing-doing gap: How smart companies turn knowledge into action*. Harvard Business School Press.
- Polites, G. L., & Karahanna, E. (2012). Shackled to the status quo: The inhibiting effects of incumbent system habit, switching costs, and inertia on new system acceptance. *Management Information Systems Quarterly*, 36(1), 21–42.

- Prochaska, J. M., Prochaska, J. O., & Levesque, D. A. (2001). A transtheoretical approach to changing organizations. *Administration and Policy in Mental Health, 28*, 247–261.
- Prochaska, J. O. (2013). Transtheoretical model of behavior change. In *Encyclopedia of behavioral medicine* (pp. 1997–2000). Springer.
- Prochaska, J. O., & DiClemente, C. C. (1982). Transtheoretical therapy: Toward a more integrative model of change. *Psychotherapy (Chicago, Ill.), 19*, 276–288.
- Proctor, R. W., & Chen, J. (2015). The role of human factors/ergonomics in the science of security is decision-making and action selection in cyberspace. *Human Factors, 57*(5), 721–727.
- Ritzer, G. (2015). *Introduction to Sociology*. Sage Publishing.
- Schultz, E. (2005). The human factor in security. *Computers & Security, 24*, 425–426.
- Senge, P. M. (2014). *The dance of change: The challenges to sustaining momentum in a learning organization*. Crown Business.
- Soltanmohammadi, S., Asadi, S., & Ithnin, N. (2013). Main human factors affecting information system security. *Interdisciplinary Journal of Contemporary Research in Business, 5*(7), 329–354.
- Turner, S. F., & Rindova, V. (2012). A balancing act: How organizations pursue consistency in routine functioning in the face of ongoing change. *Organization Science, 23*(1), 24–46.
- Van-Zadelhoff, M. (2016, September). The Biggest Cybersecurity Threats Are Inside Your Company. *Harvard Business Review*.
- Worley, C. G., & Mohrman, S. A. (2014). Is change management obsolete? *Organizational Dynamics, 43*, 214–224.
- Young, W., & Leveson, N. (2013). Systems thinking for safety and security. *Proceedings of the 29th Annual Computer Security Applications Conference*.

Darrell Norman Burrell is post-graduate student and a 2017 graduate of the National Coalition Building Institute's (NCBI) Leadership Diversity Institute. He is a Certified Diversity Professional. He is an alumnus of the prestigious Presidential Management Fellows Program www.pmf.gov. Dr Burrell has a doctorate degree with majors in Education and Executive Leadership Coaching from A.T. Still University. Dr. Burrell has an Education Specialist (EdS) graduate degree in Higher Education Administration from The George Washington University. He has two graduate degrees one in Human Resources Management/Development and another Organizational Management from National Louis University. He also has a Master of Arts degree in Sales and Marketing Management from Prescott College. He has extensive years of university teaching experience at several universities.

Calvin Nobles is a Cybersecurity Professional and Human Factors Engineer with more than 20 years of experience. He is a Department Chair and Associate Professor at the Illinois Institute of Technology. He retired from the Navy and worked in the finance industry for several years. He authored a book on integrating technologically advanced aircraft in general aviation. He serves on the Cybersecurity Advisory Board at Stillman College and the Intelligence and National Security Alliance Cyber Council. Currently, he is a Cybersecurity Fellow at Harvard University.