EMERGENCE OF TECHNICAL SOCIOLOGY: IMPACTS ON TECHNOLOGY AND CYBERSECURITY MANAGEMENT

Dr. Laura Mitchell
Florida Institute of Technology, USA

ABSTRACT

Researchers are forecasting the global cost of cybercrime in 2019 to reach over 2 trillion dollars. Research revealed that 80-90% of security breaches are due to human-enabled errors in the U.S. and the U.K. Technology is not the only solution in cybersecurity as organizations encounter a barrage of cybersecurity threats that prey on the propensity of human error and a lack of understanding around the social and people aspects of change management, business process improvement, training, and organizational behavior. As a result, there is an emergence of a new area of research development around technical sociology or digital sociology as domain to explore the people perspectives, group dynamics, and social aspects of cybersecurity and technology management. 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 issues and contributes to them through the exploration and comprehension of social learning systems around groups, organizations, and individuals. This domain is concerned with sociological research and its implications for improving applied theory, policy, and professional practice concerning the effective management of technology and its consequences on social systems, organizational systems, and individual systems.

KEYWORDS: Technology management, Engineering management, Human computer interation, Human-enabled errors, cybersecurity, technical sociology, organizational behavior, technological resistance to change, change management, information security.

1. INTRODUCTION

Researchers are forecasting the global cost of cybercrime in 2019 to reach over 2 trillion dollars (Morgan, 2016). Research revealed that 80-90% of security breaches are due to human-enabled errors in the U.S. and U.K. (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 are the study of human interaction with information systems, networks, and practices in an information security environment (Alavi, Islam, & Mouratidis, 2016). Nonetheless, cybersecurity, computer science, and information technology certification and training programs have failed to implement program content to address organizational behavioral factors, people change management perspectives, and human factors in cybersecurity thus creating a new domain 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 issues and contributes to them through the exploration and comprehension of social systems around groups, organizations, and individuals. This domain is concerned with sociological research and its implications for improving applied theory, policy, and professional practice concerning the effective management of technology and its impacts on social systems, organizational systems, and individual systems.

2. OBJECTIVES

- To describe a framework for a discussion around the need to understand complex intersection between technology management and sociology around cybersecurity and information security.
- 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.

- 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.

3. RESEARCH GOALS

- To look at organizational behavior and technology management from a social science vantage point to spur more research and discourse around technical sociology as an emerging field requiring more research by those in cybersecurity, technology management, human factors psychology, and human computer interaction.

4. METHODS

- This is a content analysis of theoretical literature and previous research around social systems in cyber security, technology management, and organizational behavior.

To really understand and explore the nature of technology and its hazards requires an understanding that social science theory is that attempts to explore social dynamics and its inherent set of relations to explain how distinct phenomena function. Therefore, social science theorizing or formulation and modifications of those interpretative explanations, then, is an ongoing process of observing and analyzing applied scientific knowledge and its intersection with everyday interaction (Newman, 2018). Sociology theory is the implicit in the nature of interpersonal relationships in ways that attempts to explain people's relation to their social, organizational, and individual systems (Newman, 2018).Whether we are doing with technology, technological innovations, technological hazards, we are faced with a set of interpretive assumptions, defined within the context of a particular organizational cultural setting, which account for what occurs and how it occurs. Thus, the comprehension of sociology theory 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 an understanding of the phenomenon being explained through the relationships in various societal and organizational institutions.

In sociology this comprehension is often explained and explored in several ways. One, general theory which conceptualizes societal and organizational institutions as a functioning interconnected system. Two, general theory which focuses on societal and organizational institutions as dynamic, changing, conflict-heavy systems driven by intense competition and exploitation. Three, theories which 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 system, organizational system, and individual systems in ways attempt to understand their relationships to each other.

Organizations leverage information systems to gain the competitive and strategic advantage to pursue business objectives; consequently, as the complexity of information systems and technologies increase, humans become more susceptible to mistakes (Alavi, Islam, & Mouratidis, 2016; Blair, 2017). Kraemer and Carayon (2007) classified a human factor error as, "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). An employee's action and decision making when engaging in work duties are intended to help advance the goals of the organization, instead of purposely engaging in actions or behaviors that would harm the organization. The result is often human error or mistakes in human decision making that create information security problems (Van-Zedlhoff, 2016).

Metalidou et al. (2014) lament that businesses pursue technological solutions to resolve behavioral-based risk rather than addressing the issue from a human factors perspective, which highlights the disregard for understanding human decision-making and interaction with information systems. One study indicates that humans (86%) are the most prominent security weakness followed by technology (63%) (Metalidou, 2014). It is common knowledge that human-enabled errors account for more than 80% of all cyber-attacks, data breaches, and ransomware attacks (Soltanmohammadi, Asadi, & Ithnin, 2013). Technology alone will not eliminate

human error in cybersecurity as organizations encounter a barrage of cybersecurity threats that prey on the propensity of human error and employee's lack of knowledge about the nature of attacks (Dykstra, 2017).

Cybercriminals persistently take advantage of hyperconnected systems, technology-induced vulnerabilities, human-enabled errors, and underprepared organizations. The most prominent cyber threats in the past 12 months are (a) phishing, (b) spyware, (c) ransomware, and (d) Trojans (Keely, 2017). Malware-less threats are emerging as the weapon of choice for malicious cyber actors seeking to compromise credentials (Keely, 2017). The top three threat vectors are (a) email links and attachments sent to employees, (b) employees engaging in problematic web-based downloads, and (c) application vulnerability (Keely, 2017). These trends make it critical for emerging research and discourse in the domain of technical sociology to understand the nature of social systems around human error and human behavior as a significant factor in creating effective organizational cultures that can better manage information security risks and incidents.

The sociological aspects of human factors

Schultz (2005) has stated the implication of the dearth of professionals and information research on the important role social factors and people make around cybersecurity breaches and employee information security misconduct. Schultz (2005) has outlined the critical importance of understanding how the work environment and work culture influence the development or non-development of knowledgeable employees that engage in adequate and proper security-oriented behaviors. According to Schultz (2005), human behavior has often been an overlooked focus in information security research and organizational business strategy. As a result, the growth security breaches driven by human factors will continue to create disparaging organizational results, causing bankrupt reputations, enormous customer dissatisfaction, business losses, and significant governmental sanctions (Buckhead, 2014; Van- Zadelhoff, 2016).

Kraemer and Carayon (2007) classified a human or people mistake error as, "Any action leading to an undesired result." Often, employees are tricked by an outsider into engaging in problematic behavior that can lead to an organizational an information security breach (Van- Zadelhoff, 2016). An employee's action and decision making when engaging in work duties are intended to help advance the goals of the organization, instead of purposely engaging in actions or behaviors that would harm the organization. The result is often human error or mistakes in human decision making that create information security problems (Van-Zedlhoff, 2016).

Van-Zedlhoff, (2016) stressed that human errors or human factors as one of the highest areas of organizational vulnerability. Solutions for information protection should consider human error and flawed decision making as one of the most significant aspects of information security (Schultz, 2005). An organization's business strategy should encompass creating an effective information security-oriented organization (Van-Zedlhoff, 2016). Understanding 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 has a significant amount of complexity then trying 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 is one where employees will purposefully increase their knowledge and concern for in the importance of information security in a manner where they will understand that this is an aspect of everyone's job not just those with information technology job titles and duties (Buckhead, 2014). Historical and 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 cyber security (Van-Zedlhoff, 2016). Organizational social and learning cultures that fail to develop effective information security training, fail to instill in all employees that cybersecurity in 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 require urgent attention from human factors practitioners and psychology-based experts.

Risk management is the key to creating effective information security cultures that limit the impact of propensity of information security intrusions (Van-Zedlhoff, 2016). People and their behaviors, not technology, is one the biggest 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 in 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), 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 or not act (Ajzen, 1991). TPB has viable application to an understanding of nature and manifestation of technical sociology around exploring the nature of employee behaviors, human factors, and organizational business strategy around cybersecurity and information security.

Considering cybersecurity from the context of TPB, employee attitudes towards a behavior is significantly influenced by individual dogmas about the results of the performance of the conduct (behavioral beliefs). If employees believe that the expected consequence of performing a behavior is positive, that employee will have an encouraging attitude about engaging in that behavior (Ajzen, 1991). That means if proper and effective information security behavior is taught, highly acknowledged, and heavily rewarded, then employees will feel more positive about promoting and engaging in the appropriate behaviors (Ajzen, 1991). On the contrary, if employees have limited knowledge, no vested interest, and are frustrated in a way strongly that creates a convincing belief that performing a behavior is negative, the employees will have an adverse attitude towards a behavior (Ajzen, 1991). The ability to positively influence the social and group behavior of employees is critical to creating an organizational culture that is effective in managing and addressing cybersecurity risks requires more exploration from a sociological context.

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 human behavior around cybersecurity. According Griffin, Dunwoody, and Neuwirth (1999) the perception of informational subjective norms is theorized to influence he perception 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. Also, the relationship between information (in)sufficiency and information behavior is moderated by beliefs about channels of risk information (such as credibility and usefulness) as well as by an individual's perceptions of their information gathering capacity or the skills needed to successfully reach the threshold of information sufficiency. The perception of a cybersecurity hazard is also expected to

predict information (in)sufficiency and thus lead to the information seeking, although this relationship is mediated by the individual's affective response (such as fear or concern) regarding that hazard.

The RISP model is particularly relevant for explaining the information and social behaviors of employees 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 be expected to drive information seeking about the aspects of those risks. The RISP model provides a framework to explores the manifestation of perceived hazard characteristics, rather than actual hazard characteristics, may be most 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 information behaviors related to risk information, with information seeking being separated into routine and non-routine and processing being separated into heuristic and systematic types (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 is managed within an organization. Kotter (2012) stated that leadership must present its people with an understanding of change; if the information is given is compelling and logical an avenue can exist for change. A change is a process of moving from one defined state to another, i.e., every improvement done to a product, method, or system (Anderson & Anderson, 2010).

Change management is the socially dynamic process concerning behaviors and interactions around the management of change (Cameron & Green, 2015; Worley & Mohrman, 2014).

The primary objective of the change management process 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 that can effectively manage the social organizational systems around change concerning technology management is paramount from a social science context.

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 people with the required 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 – Identifying and planning for early and visible achievements and recognize and reward employees who were 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 effective information security cultures.

Prochaska's (2013) Transtheoretical Model of Behavior Change outlines strategies that help people make and maintain changes, which include both cybersecurity and technology management including:

1. Consciousness Raising - Increasing awareness about the 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 is 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 helpful social relationship that provide positive influence for change or performance improvement.
8. Counter-Conditioning - Substituting proper or appropriate behaviors over the thoughts for improper or inappropriate behaviors.
9. Reinforcement Management - Rewarding the superior performance and constructively addressing undesired performance or behaviors without lenience.
10. Stimulus Control – 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 organizations makes a compelling case that human factors and organizational culture can be changed and positively influenced by change management knowledge. Dhillon study outlined the importance of employee engagement as a useful tool for change management. Dhillon (2001) defined the vital value of forming cooperative organizational cultures that focus on ways to leverage the intellectual capital of everyone, which aligns creating appropriate the social systems, organizational systems, individual systems around the integration of new innovations, new technologies, new processes, existing process improvement, and new training implementation around technology management. Dhillion's (2001) research outlines the importance of the entire work system, including the organizational culture and human factors as it relates to the effective engagement of cybersecurity management. Exploring research in social science contexts provides a rationale for understanding the interaction between technology and sociology.

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 cause alterations of systems that could cause potential concerns that can affect other business units (Senge, 2014). It is imperative that stakeholders understand the process and future resistance systematically to make a logical approach to change (D' Ortenzio, 2012). Change management can also be devalued because typically stakeholders who hold a leadership role lead change (Kotter, 2012). The change process can be more receptive by employees if the stakeholders also involved participants as subject matter experts.

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 following information security protocols (Young & Leveson, 2013). Lawton (1998) outlined that many security violations are based on social forces and human factors that outline that violations are often the manifestation of employees that are just trying to meet deadlines and get work done. Time pressure, workload, and using a "quicker way of working" were among some of the human factor issues that influence the engagement in risky actions by employees 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. Creating social forces that create cultures that encourage information security diligence and compliance in critical to

cyber security 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 become committed to the realization that information security and cybersecurity is everyone's job not just those with information technology job titles. According to Buckhead (2014) it is vital to perpetuate a climate where everyone feels a sense of personal ownership the mitigation of information security risk. Coffey (2017) argues that existing cybersecurity training and awareness is restrictive in scope because training programs fail to modify end user's behavior. For organizations to influence the behavior of end-users, require fostering an environment that transforms the organizational climate to active and engaged learning culture (Coffey, 2017). Having an involved social learning culture looks to capitalize on people 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 is perceived as new by its audience. Diffusion of innovation is the process where an innovation has disseminated within a field, progressively, and among different types of adopters (Crawford & Di Benedetto, 2008). The related concept explored processes at the individual level where diffusion refers to the whole of embracing of 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 a 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 that are attempting to get non-technical employees to create an organizational culture focused on cybersecurity must understand the complex social nuances of Rogers perspective (2003).

Davis (1989) defined diffusion as the process by which technology extends across a population of organizations. Davis' Technology Acceptance Model (Davis, 1989) as well as 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 need or utility of a new technology due to their comfort and familiarity an existing technology or approach. This is driven by a longing to stick with the status quo (Kim & Kankanhalli, 2009). A social science context is considering 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 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 new technology (Kim & Kankanhalli, 2009; Polites &

Karahanna, 2012). Understanding the social system nuances of behavioral change is critical in the development of effective cybersecurity-oriented cultures and security compliant employees.

Information Technology Conflict-Resistance Theory (IT-CRT)
Meissonier and Houzé (2010) suggested that information technology (IT) Conflict-Resistance theory proposed that two sets of assumptions, conflict theory, and resistance theory, as important theories through which to understand resistance (Meissonier & Houzé, 2010). The IT conflict-resistance theory explores the complex nature of social systems around organizational behavior in a pre-implementation context. Meissonier and Houzé (2010) outline that the critical importance of organizational behavior around employee engagement to address conflict and resistance around adoption and utilization around 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. This means that new processes, approaches, and protocols arounds cybersecurity and information security should be vetted to a level were complex consequences of integration are considered and planned for in advance.

Technology acceptance models
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 castoff newly introduced technology if they find the technology more user friendly and easier to grasp. Organizational and social dynamics around technology acceptance, technology management, and new technology introductions have significant managerial and human capital implications around cybersecurity and technology management.

Exploring and understanding these perspectives requires collaboration between a variety of actors 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.

RECOMMENDATIONS AND CONCLUSIONS

Technical sociology provides a critical perspective to explore the social contexts and dynamics 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. 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 study

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.

Burrell Technical Sociology Framework Model (2019)

Complexity variables	Burrell Technical Sociology Framework Model (2019)
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 of technology and its implications on social systems, 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 systems, organizational systems, individual systems applications of change management approaches around the integration of new innovations, new technologies, new processes, existing process improvement, and new 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 systems, organizational systems, and individual systems related to data management, data usage, and data overload.
Province 9	Security complacency which explores the social forces and human factors that influence employees to relax their vigilance around effective 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 the frustrations around the learning curve required to fully utilize each new technology.

While technology managers within most organizations today would readily admit that cybersecurity is one of their biggest concerns, many 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 (Burrell, 2018). Organizational culture is more broadly defined by its social norms. Creating a cyber-aware culture demands a shift in the way organizations treat security (Goel, Williams, & Dincelli, 2017). Many organizations fail to fully understand the risks associated with the actions and inactions of people around cybersecurity (Burrell, 2018). Organizations often lack the required expertise to understand what an effective cybersecurity culture should look like or how to develop the social learning systems that are required to have a fully engaged cyber-aware workforce within the organization (Burrell, 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 management and organizational social science.

Understanding the people and social systems aspects of cybersecurity requires an understanding of technology management and sociology intersect in organizations includes:

1. Outlining cyber and data security risks. Outlining these risks effectively requires engaging creating social learning systems and networks where those with the 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. Sharing with all employees organizational and individual cybersecurity best practices for creating the proper environment. This level of sharing is about engaging people to help them understand what the ideal best practices social and organizational systems look like.
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 effective when it provides clarity about why specific procedures and policies are in place and what they mean to safeguarding the organization.
6. Creating a reliable and effective cybersecurity culture means engaging organizational and individual social systems in ways that continually test how well employees are following protocols.
7. Creating an organizational systems culture where employees feel comfortable about questions around cybersecurity. This about creating a highly responsive and open environment that encourages employees at all levels to feel free to talk 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:
    - Teaching all employees proper security behavior.
    - Teaching all the right protocols and procedures to follow.
    - Teaching employees what to do if there is a breach.
    - Teaching employees their role in data security.
    - Teaching employees about the nature of common threats.
    - Explaining to employees whom to contact with their issues, questions, and concerns around cybersecurity.
    - Comprehensively explaining why following organizational procedures and protocols is vital.

REFERENCES

[1] Alavi, R., Islam, S., & Mouratidis, H. (2016). An information security risk-driven
[2] Investment model for analysing human factors. Information & Computer Security, 24(2), 205-227.
[3] Albrechtsen, E. & Hovden, J. (2010). Improving information security awareness and behavior through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29, 432-445.
[4] Alfawaz, S., Nelson, K. & Mohannak, K. (2010). Information security culture: A Behavior compliance conceptual framework. Eighth Australasian Information Security Conference, Brisbane, Australia.
[5] Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50, 179-211.
[6] Anderson, D., & Anderson, L. A. (2010). Beyond change management: How to achieve breakthrough results through conscious change leadership. CA: San Francisco: John Wiley & Sons.
[7] 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.
[8] Blair, T. (2017). Investigating the cybersecurity skills gap (Order No. 10623377).
[9] Available from ProQuest Dissertations & Theses Global. (1989786177). Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1989786177?accountid=27203
[10] 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
[11] 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 (IJHIoT), 2(1), 52-67.
[12] Cameron, E., & Green, M. (2015). Making sense of change management: A complete guide to the models, tools, and techniques of organizational change. Philadelphia, PA: Kogan Page Publishers.
[13] 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.
[14] Clegg, S., & Bailey, J. R. (Eds.). (2007). International Encyclopedia of Organization Studies. Sage Publications.
[15] 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).
[16] Crawford, M., & Di Benedetto, B. A. (2008). New products management. Boston, MA: McGraw-Hill/Irwin.
[17] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.
[18] Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. Computers & Security, 20(2), 165-172.

[19] D' Ortenzio, C. (2012). Understanding change and change management processes: A case study. (Doctoral Thesis) University of Canberra. Retrieved to http://www.canberra.edu.au/researchrepository/items/81c02a90-6a15-91ae-c7a2-ff44c96d60b2/1/
[20] Dykstra, J. (2017). Cyber Issues Related to Social and Behavioral Sciences for National
[21] Security. The National Academies. Retrieved from: http://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_177250.pdf
[22] 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.
[23] Goel, Sanjay; Williams, Kevin; and Dincelli, Ersin (2017). Got Phished? Internet Security and Human Vulnerability. Journal of the Association for Information Systems: Vol. 18: Iss. 1, Article 2.
[24] 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.
[25] Hegar, K. (2011). Modern Human Relations at Work. Nashville, TN: South Western Publishing.
[26] Kim, H. W., & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. MIS Quarterly, 567-582.
[27] Kotter, J. P. (2012) Leading change. Boston: Harvard Business School Press
[28] 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(2007), 143-154.
[29] Kraemer, S., Carayon, P. & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28, 509-520.
[30] Lawton, R. (1998). Not working to rule: Understanding procedural violations at work. Safety Science, 28(2), 77-95.
[31] Maglaras, L., He, Y., Janicke, H., & Evans, M. (2016). Human Behaviour as an aspect of Cyber Security Assurance.
[32] Mancuso, V. F., Strang, A. J., Funke, G. J., & Finomore, V. S. (2014, September).
[33] Human factors of cyber-attacks: a framework for human-centered research. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting(Vol. 58, No. 1, pp. 437-441). Sage CA: Los Angeles, CA: SAGE Publications.
[34] Meissonier, R., & Houzé, E. (2010). Toward an IT conflict-resistance theory: Action research during IT pre-implementation. European Journal of Information Systems, 19(5), 540-561.
[35] Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., &
[36] Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. Procedia-Social and Behavioral Sciences, 147, 424-428.
[37] Morgan, S. (2016, May 13). Top 5 industries at risk of cyber-attacks. Forbes.
[38] Newman, D. (2018) Sociology: Exploring the Architecture of Everyday Life. Los Angeles: Sage.
[39] 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. MIS Quarterly, 36(1), 21-42.
[40] Prochaska, J. O. (2013). Transtheoretical model of behavior change. In Encyclopedia of behavioral medicine (pp. 1997-2000). Springer New York.
[41] Prochaska, J. O. & DiClemente, C. C. (1982). Transtheoretical therapy: Toward a more integrative model of change. Psychotherapy: Theory, Research, and Practice, 19, 276-288.
[42] Prochaska, J. M., Prochaska, J. O., & Levesque, D. A. (2001). A transtheoretical approach to changing organizations. Administration, Policy Mental Health, 28, 247-261.
[43] Proctor, R. W., & Chen, J. (2015). The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. Human factors, 57(5), 721-727.
[44] Ritzer, G. (2015). Introduction to Sociology. London: Sage Publishing.
[45] Schultz, E. (2005). The human factor in security. Computers & Security, 24, 425-426.
[46] Senge, P. M. (2014). The dance of change: The challenges to sustaining momentum in a learning organization. New York, NY: Crown Business.
[47] Soltanmohammadi, S., Asadi, S., & Ithnin, N. (2013). Main human factors affecting
[48] information system security. Interdisciplinary Journal of Contemporary Research in Business, 5(7), 329-354.
[49] 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.
[50] Van- Zadelhoff, Marc (2016, September). The Biggest Cybersecurity Threats Are Inside Your Company. Harvard Business Review.

[51] 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. New Orleans, Louisiana, USA..