Issues in Information Systems
Volume 24, Issue 3, pp. 1-14, 2023

DOI: https://doi.org/10.48009/3_iis_2023_101

Foundation of cybersecurity infoscapes: it's all about the culture

Debra J. Borkovich, *Middle Georgia State University, debra.borkovich@mga.edu*
Robert J. Skovira, *Robert Morris University, skovira@rmu.edu*
Frederick Kohun, *Robert Morris University, kohun@rmu.edu*

Abstract

Cyberculture is an evolving concept that dominates organizational security. Business cybersecurity breaches often occur due to the lack of a healthy cyberculture. This paper identifies, defines, and explores the concept of cyberculture and offers practical advice for approaching organizational culture change to embrace a proactive cyberculture. We identify and review key academic research, subject matter experts, and think-tank surveys of cybersecurity professionals. Qualitative interpretation of the literature suggests there are underlying themes and patterns relevant to achieving a healthy cyberculture. Findings indicate that cyberculture plays a key role in successful organizational cybersecurity, aligning strategic business objectives with security governance and controls to mitigate risk. Interpretation reveals that improved cyber strategy and skilled people play key roles in the adoption of cyberculture at every organizational level, while awareness, communication, influencers, and a clear reporting structure between boards, management, security leadership, and all employees, build cyber resilience. We propose that businesses will benefit from the creation and adoption of holistic positive cybercultures as integral to the overall organizational culture; and conclude that such a pragmatic path forward provides an improved nexus between a digital business culture and its cyberculture. Therein, we proffer that creating a cyberculture by which a pattern of shared basic assumptions that support both the aspects of information security, business strategy, and trust as a daily behavioral practice is a major step toward a positive cyber solution.

Keywords: cyberculture, cybersecurity, cyber resilience, organizational culture, occupational culture, information communication technology

Introduction

Cybercultures are social, technological, web-based, and global. They are based upon entangled information transmitted via social media, emails, texts, documents, cell phones, biometric software, media streaming, e-purchasing, e-business, e-government, e-libraries, e-learning platforms, etc.; and these interwoven and matrixed webs of social, institutional, and economic significance affect every aspect of our lives. Geertz (1973, p. 5) described culture as "webs of significance," and this statement can be no truer than today. "We continue to spin technological webs into increasingly sophisticated forms, to weave devices of information and communication into every aspect of our lives, and to further entangle ourselves in their multifarious snares" (Kozinets, 2019, p. 620). Cybercultures are infoscapes (Skovira, 2010) created from entangled disruptive web-based human information systems; and they are considered sub-cultures of the greater overall organizational culture.

Traditionally, the Information Communication Technology (ICT) Department is responsible for communicating and teaching cyberculture behavior, practices, meanings, and security measures to the

organizational members; however, many are unsuccessful despite their well-written and disseminated policies, procedures, and routine training programs. Sometimes these programs succeed in improving cybersecurity-related behaviors, but many do not. We proffer that employees' cyber behavior at every level is directly related to the security culture espoused by the organization, *or a lack thereof.* A healthy cybersecurity culture promotes self-sustaining patterns of positive behavior and perceives how an organization addresses security measures. But an ineffective cyberculture can promote negative, unwitting, or apathetic cyber behavior eliciting human vulnerabilities, errors, and misconduct.

We conceptualized our Literature Review of published studies and articles by cybersecurity subject matter experts, business management academics, philosophers, and scholars by exploring the entanglements and disruptions caused by positive and negative cybercultures within organizations. In lieu of a formal methodology we developed a Theory of Cyberculture in organizations and their respective challenges with communicating and interpreting their entangled and often disruptive infoscapes of cyber behavior, practices, values, and meanings. We curated a published review of over 50 articles, 10 books, and 8 cybersecurity survey reports to constitute and support our study by highlighting a range of influential academic opinions and scholarly findings in the cyberculture arena. The intent of this research was to extend the current quantitative approach of cybersecurity surveys and questionnaires to include a qualitative approach to inquiry by digging deeper into the topic of cyberculture to learn how and why some cybercultures are healthy and others fail, and not merely what and how many do exist. Rich descriptive and detailed literature provided this avenue for qualitative research through the review of voluminous amounts of digitally published data resources. Our purpose was to collect data and provide findings to a results-oriented business or workplace community whose cybersecurity decision-support system and strategic objectives rely upon relevant information to help executives and management solve cyber problems and make good business decisions.

Therefore, by studying patterns, trends, and anomalies in the literature, *our research purpose was to learn how and why some cybercultures thrive successfully in organizations and others fall short, even if established cybersecurity policies and procedures are well-written and disseminated and training programs are routinely offered and updated.* This narrative continues with our Theory, Literature Review, and Interpretive Discussion of the research findings. A Conclusion recaps our paper and offers a pragmatic path forward to provide a nexus between the business organizational culture and its cybersecurity sub-culture with recommendations for mitigation and improvement within strategic organizational frames.

The Cyberculture Theory

In our narrative, we theorize that a positive or negative cyberculture is directly related to the overall success of the organizational culture. We further assert that employees' cyber behavior at every occupational level is also directly related to the security culture espoused by the organization, *or a lack thereof.* Formally adopted security policies, well-defined security governance, controls, and audits generally do not address the cyberculture that lies persistently in the background. A healthy cyberculture promotes self-sustaining patterns of positive behavior and perceives how an organization addresses security measures. But an ineffective cyberculture can promote negative, unwitting, or apathetic cyber behavior eliciting human vulnerabilities, errors, and misconduct. Therefore, we purport that cybersecurity is everyone's responsibility in the digital organization, and not just the responsibility of the ICT Department or its Senior Leadership. Establishing a proactive cyberculture can be established and achieved when the corporate hierarchy from the top-down sets and influences the accountability, awareness, training, standard, communication model, and framework for a healthy cyberculture committed to by all in the organization.

Literature Review

Anthropologists have long associated human cultures with technology embedded within their social environments. Human cultures have developed tools to accelerate their evolution and improve their existence for the past 2.6 million years (Semaw, et al., 2003), indicating that it would be difficult "to imagine human beings as pretechnological" (Nye, 2006, p. 5). In the 20th century, influential philosophers and scholars such as Heidegger (1954), Ellul (1964), and Mumford (1967) associated technology with efficiency-driven techniques ("techne") of machines at work in a society. And the moniker associated with these shared experiences has long been identified and described as technoculture (Penley & Ross, 1991). But in the 21st century, cybertechnologies are framing, reflecting, shaping, connecting, and controlling us (Kozinets, 2019) through the infoscapes created by the dissemination of entangled disruptive matrixed information within our cybercultures. Therefore, we begin with our definition of cybersecurity culture (or cyberculture).

Defining Cyberculture

For our working definition of cyberculture, we drew upon several literature sources. Schein (1996, p. 12) defined organizational culture as "a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and taught to new members as the correct way to perceive, think, and feel in relation to those problems." Next, we reviewed the literature of information security, which considers a security culture to be either present or absent in an organization. Vaibhav (2021, p. 9) defined an information security culture as something that "should support all activities in such a way that information security becomes a natural aspect in the daily activities of every employee. Security culture helps to build the necessary trust between the different actors." We also included a US Army definition that incorporated both approaches in its interpretation of cyberculture as follows: "A pattern of shared basic cultural assumptions that supports information security becoming a natural aspect of the daily activities of all Army personnel who operate in cyberspace" (Paul & Porche, 2011, p. 70). And with a nod to systems theory (Meadows, 2008), we synthesized the definitions above and developed our construct as:

> *A cyberculture is a set of digital customs, practices, behaviors, and beliefs shared by a digital community, comprised of people, processes, and technology, as the accepted way to do things. A healthy cyberculture minimizes and mitigates the risks of being subverted, attacked, or targeted for digital sabotage.*

The conceptual impact of cyberculture accompanies linking technology consumption with cultural, historical, and societal factors (Firat, et al., 1995; Mick & Fournier, 1998). We communicate our cultures and sub-cultures through socialization in the workplace and use our contextualized staged performance in any face (form) from which we want to be perceived by a specific audience. Self-presentation as conceptualized builds on Goffman's (1959) theories of identity and social performance. Social actors engage in complex negotiations to project a desired impression. This impression is maintained through consistently performing coherent and complementary behaviors (Schlenker 1975). Goffman originally termed this process *impression management* but in today's digital arena of *infoscapes*, one might be called an *Influencer*.

Infoscapes, Technoscapes, and Technocultures

An organization is an infoscape or information landscape (Skovira, 2010) that consists of all formal and informal informing systems and informing objects we use in an organization. An organizational culture and

its sub-cultures do not and cannot exist without informing systems. The organization is a metaframe of informing systems within one, multiple, and/or networked matrixed infoscapes, all of which help to define strategic business missions and goals. Appardurai (1990) theorized these radical disjunctures as key aspects of the global cultural economy, conceptualizing them as a range of technical and expressive social media–inflected "technoscapes." Cybercultures require informing systems and informing objects to develop a technoculture's behavior, practices, vocabulary, artifacts, and routines.

Technocultures are defined as the various identities, practices, values, rituals, semiotics, and other sources and structures of meanings that are influenced, created by, or expressed through technology consumption (Postman, 1992; Mick & Fournier, 1998). Selfies, emojis, avatars, memes, GIFs, and augmented reality are contemporary sources of cyber meaning (Ge & Gretzel, 2018; Li, Chan, & Kim, 2019), as are messaging, texting, Facebook FOMO, Instafame, unfriending, likes, and retweets transmitted to-and-from ever-sophisticated devices. Technologies inspire new vocabularies, self-presentations, practices, and connections that we participate in by co-creating technocultures (Kozinets, 2022) within our infoscapes.

National vs. Organizational Cultures

Generally, academics and other subject matter experts argue that culture is systemically difficult to change. However, through evolution of time, technology, leadership, business units, products and services, employees, customers, geography, economics, etc., organizational culture may slowly change when a clear mission, shared values and practices, and a united behavior is communicated to all stakeholders.

Hofstede (1996; 1998) clearly established a conceptualization of culture by identifying salient differences between national culture (nation, region, ethnic group) and organizational culture (type of business or company). Hofstede (1994, p. 12) described nationality as an attribute that we did not choose, "We are born within a family within a nation and are subject to the mental programming of its culture from birth." Schein (2009, p. 61) argued that "Organizational cultures ultimately are embedded in the national cultures in which an organization operates. Thus, the deeper assumptions of the national culture are reflected in the organization through the cultural backgrounds of its founders, leaders, and members."

Hofstede, Hofstede, and Minkov (2010, pp. 344 - 345) later defined organizational culture as "the collective programming of the mind that distinguishes the members of one organization from another. An organization's culture is maintained not only in the minds of its members but also in the minds of its other stakeholders, everybody who interacts with the organization."

Lin and Ha (2009, pp. 72 - 73) suggested that "Organizational culture is a system of artifacts, values, and assumptions, among which artifacts are most observable and directly related to organizational behavior. One such artifact is norms, an agreement about what people should do and not do in a given situation." Similarly, organizational culture is developed within the work environment and is based upon business plans, mission statements, managerial concepts, compensation systems, economic competition, technology integration and implementation, and workplace mores (Hampden-Turner & Trompenaars, 2000). Marsh (1998, p. 94) asserted that, "Organizational culture is socialized at the beginning of employment."

Occupational Culture

Hofstede, Hofstede, and Minkov (2010) described their concept of occupational culture as a cultural level midway between national and organizational culture suggesting that "entering an occupational field means the acquisition of both values and practices; the place of socialization is the school, apprenticeship, or university; and the time is entering work" (pp. 368 - 369). We expanded upon the authors' definition of

occupational culture with our own interpretation based upon our collective years of work experience in the corporate and academic arenas as follows:

> *People become socialized to an organization's culture upon entry into the workplace, and unlike national culture, an individual's encounter with business culture is subject to change each time an employee voluntarily or involuntarily departs one position and commences a new one. The same applies to a chosen occupation and its associated hybrid culture based not only upon the organization's overall culture, but also upon education, training, professional associations and certifications, artifacts, values, vocabulary, communities of practice, experience, and the influence of matrixed sub-cultures.*

Cyberculture vs. Technology

May (2018) coined the term "human firewall" stating that the collective behavior of the people in our lives is both the biggest threat and the best line of defense when it comes to cybersecurity. Relihan (2019) argued that cybersecurity is the responsibility of everyone in the organization, not just the ICT Department. It takes only one keystroke to set off an organization-wide cybersecurity crisis and most executives do not have the deep technical background required to address this problem when the responsibility lands on their shoulders.

Hanspal (2021) agreed that digital security is becoming the key challenge affecting the world; and it is not just a technical problem. Nord, et al. (2022) addressed the controversies surrounding ISP compliance, including leadership, cultural, engagement, and specific role implications. The aggregate research of various subject matter experts supports the need for empathy, trust, awareness, communication, and collaboration. *We refer to this phenomenon as a positive healthy cyberculture.*

Cybersecurity Culture Reports and Surveys

According to ISACA/CMMI's Cybersecurity Culture Gap Report (2018), 95% of global senior technology respondents identified a substantial gap between their current and desired organizational culture of cybersecurity. Organizations face multiple challenges with engaging business units and executives at the strategic level with shifting the business toward a healthier security culture. Ineffective communication styles and lack of awareness can exacerbate these challenges.

The MediaPro Survey (2018) reported that business executives overall had a relatively low awareness of basic computer (and mobile devices) protection, privacy, and physical security. Generalized survey scores revealed that 41% were putting themselves and their corporations at risk, compared to a general population that scored only 29% at risk. As culture becomes more important to business leaders, the significance of culture on business performance is critical. For example, the cost of US turnover due to culture over 5 years is $223 billion; and millennials who experience a culture of respect, fairness, pride, and camaraderie are 50 times more likely to stay (SHRM Report, 2021).

The annual KnowBe4 Security Culture Report (2022) performed scientific research into the relative cybersecurity culture-related strengths and weaknesses of individuals, organizations, industry sectors, and regions. It surveyed over 530,000 employees across 2,910 organizations worldwide asking questions about knowledge of risk, attitude, behavior, cognition, communication, compliance, norms, and responsibilities. Survey results reported that small business cybersecurity programs were outperforming large corporations in risk assessment, mitigation, and training. However, 37.9% of untrained users would fail a phishing test.

The US CEO Report (KPMG, 2022) identified cybersecurity as threats to growth by 33% of CEOs; but only 41% considered their companies were able to deal with the threats. Interestingly, 92% of the CEOs responded that they were aware of new cyber threats due to news reports, but not due to their interactions and communications with their Security Leaders and ICT Departments. Survey data from executive activities showed that a lack of cultural fit is responsible for up to 68% of new-hire failures at the senior leadership level evidencing that cultural fit is as important as capabilities and experience for individual leaders.

The Conscious Culture Group (Elliot, 2022) reviewed a Harvard Business Review (HBR) Survey that reported employee attitudes can make or break a business; and expressed a simple definition of culture as the employee experience. The HBR report used two dimensions: 1) people interactions and 2) response to change; and these led to eight culture styles: caring, purpose, learning, enjoyment, results, authority, safety, and order. Results showed a that companies had a strong tendency to two prevailing styles: 89% of the companies ranked "results," while 63% ranked "caring" in their top two. From there the ranking was: "order" (15%), "purpose" (9%), "safety" (8%), "learning" (7%), "authority" (4%) and "enjoyment" (2%).

Vasudevan, Piazza and Carr (2022) studied non-technical organizational factors that contributed to better cyber resilience. Cyber resilience moves organizations away from efforts to guarantee security of all systems, toward an approach that acknowledges systems are bound to fail with a focus instead on the impact of that failure on business objectives. Adopting a qualitative approach of analyzing factors of organizational resilience, their research used data collected from 25 IEEE interviews at senior leadership or corporate board-level to point out the extent to which these factors facilitated or impeded cyber resilience. They discovered that cyber strategy and skilled people played a key role in adoption of cyberculture at the management level, while communication between boards and security leadership as well as a clear reporting structure were signals for building cyber resilience. While the work on cyber resilience is evolving, there remains a lack of studies using qualitative data for investigating the concepts and themes pertaining to cyberculture in organizations.

None of the above reports surveyed evidence of any specific organizational cyberculture as relevant to their business; nor was there any evidence of the question being asked. We further noted that Executives and Senior Leadership were often surveyed, but the organizational employees and line workers were rarely questioned. Drucker (1954) argued that "culture eats business strategy for breakfast," but one may conclude that negative cyberculture eats business strategy for lunch and dinner, as well.

Interpretive Discussion

Our review of the literature revealed that it takes only one keystroke to set off an organization-wide cybersecurity crisis and most executives do not have the deep technical background required to address this problem. The human firewall (May, 2018), known as the collective behavior of the people in our lives, is both the biggest threat and the best line of defense when it comes to cybersecurity. It is the responsibility of everyone in the organization, not just the ICT Department (Relihan, 2019; Hanspal, 2021). Our research, and that of many others, supports the need for organizational empathy, trust, awareness, communication, and collaboration to achieve a positive healthy cyberculture. The following narrative describes our interpretative theory of the current and future state of cybercultures in organizations.

Culture: Context, Conditions, and Convergence

Cyber literature showed that high levels of employee engagement with ICT, management, and customers closely aligned views regarding which cultural characteristics are salient in the company. This convergence of constructs applies to employees at all levels of the corporate hierarchy. Therefore, context matters when assessing a culture's strategic effectiveness.

Leaders must simultaneously consider culture styles and key organizational and market conditions if they want their culture to help drive performance (Hofstede, 2018). External factors are geographic regions and industries; and critical internal considerations include alignment with business strategy, leadership, and organizational frames (Groysberg, et al., 2018).

Communication Challenges: Senior Leadership vs. ICT Department vs. Employees

Typically, ICT Departments and Security Managers are on-board with cyberculture and want to encourage partnership and engagement throughout the organization. But often they are perceived negatively by executives and employees alike, having a corrosive effect on cyberculture. The concept that employee attitudes can make or break a business is directly related to organizational culture; therefore, the attitudes toward cybersecurity are directly related to cyberculture.

The employee experience positively related to caring, purpose, learning, enjoyment, results, authority, safety, and order are all paramount to a successful cybersecurity program (Elliot, 2022). We also assert that occupational sub-cultures play a role in the acceptance of a positive cyberculture. Employees will be more receptive to cybersecurity if they know the ICT folks are also interested in their roles and responsibilities within the corporation, too.

Executives are often confounded by culture, because much of it is anchored in unspoken behaviors, mindsets, and social patterns. Many leaders either disregard culture or relegate it to HR, where it becomes a secondary concern for the business. However, when properly managed, culture can help achieve change and build organizations that will thrive in even the most trying cybersecurity times. Following our literature review, we learned that through our own observations, and practical experiences the elements of trust, respect, structure, and shared norms are required at all levels of an organization.

For example, when aligned with strategy and leadership, a strong culture drives positive organizational outcomes. In a merger or acquisition, designing a new or hybrid culture on complementary strengths can speed up integration and create more value over time. And in a dynamic, uncertain environment, in which organizations must be more agile, *learning* gains importance (Blum, 2020). Our fundamental assessment is that a strong cyberculture can be a significant liability when it is misaligned with business strategy.

Organizational culture and cyberculture often work at cross-purposes, due to misunderstanding corporate objectives. Disruptive changes to ICT and immaturity of security governance programs and training contribute to these entanglements. New or updated policies and procedures and revised training programs may be required to emphasize change in knowledge, practices, awareness, and attitude. Table 1 lists a sample of systemic obstructive employee attitudes about the ICT personnel, as evidenced in the collective Cyber Surveys. Coincidentally, leadership and management also exhibit their own negative cyber attitudes about the ICT Department (Table 2), and several align with the employees' comments, too.

Table 1: Negative Employee Cyber Attitudes	Table 2: Negative Management Cyber Attitudes
ICT doesn't provide timely solutions to my issues	ICT doesn't provide timely solutions to my issues
ICT only gives me bad news	ICT only gives me bad news
ICT people have no personalities; they never smile	ICT people have no personalities; they never smile
ICT people only say 'NO' to want I want	ICT always has a 'NO' attitude when I want something
ICT won't let me use my thumb drive to take work home	ICT won't let me use my thumb drive to take work home
ICT won't let me use my home PC for work	ICT won't let me use my home PC for work
ICT training is boring and too long	ICT always tells me I can't do something due to regs.
ICT people can't communicate and won't explain	ICT speaks in jargon, can't understand, no time to ask
ICT spies on my laptop, business and personal	ICT rarely provides reasonable low-cost solutions
ICT people are disinterested in my feedback	ICT always asking for $$s for upgrades, equipmt, people
ICT protocols are too difficult to follow, I do it my way	ICT does not contribute to the business revenue
ICT tries to scare me, not sympathetic to my issues	ICT generates fear, does not understand business issues

It is widely accepted by ICT professionals that people are the greatest vulnerabilities to a secure cyber system. However, without employee trust and collaboration with the ICT Department, human cyber security improvements are unlikely to occur. We offer that positive targeted communication from the ICT personnel and proactive awareness from the employee population could help to mitigate these vulnerabilities.

When ICT Department communication skills are lacking or sub-par, cyberculture has no influence over the organization's population. And if their communication style is out of line with the rest of the organization, the cyberculture will not be embraced by the leaders and employees. If cybersecurity isn't considered strategic or business units are disengaged, leaders are less likely to support the cyberculture. Even without the cultural dissonance, security leaders tend to find communicating with executives or peer business partners challenging and difficult. Since ICT or cybersecurity is a non-revenue generating department, the ICT leaders are often too low in the management hierarchy to have regular access to senior leadership. Therefore, when communications take place, they are typically perceived as the bearers of bad news about incidents, vulnerabilities, deficiencies, and unwelcome regulatory requirements (Blum, 2020, p. 96). When ICT Managers need funding for new software, hardware, cloud-support, upgrades, maintenance, enhancements, and training, they may lack strong communication skills, resulting in the perception of loss of credibility. ICT must learn to communicate in the language and vocabulary of its intended audience.

Social Engineering, Routine Cyber Training, and Influencers

Human error or misconduct of one kind or another is typically the direct cause or a contributing factor to almost every security breach or outage. Whether it is the user clicking a phishing link, an operator accidentally deleting the corporate directory, a manager approving excessive privileges, a receptionist letting a thief or spy into the building; or an incident responder hitting the snooze button on the wrong malware alarm, the examples are legion (Blum, 2020, p. 91).

Social engineering refers to techniques aimed at a target into revealing specific information or performing a specific action for illegitimate reasons. In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information (Borkovich & Skovira, 2019). Security leaders can improve security-related behavior through user awareness and training programs. Formally adopted policies, procedures, well-defined governance, and clear security-related roles in the business are prerequisites for a successful cyber program. But in the background behind the visible machinations is the organization's security culture. A positive cyberculture can provide the best opportunity to achieve business security; a negative one can be its greatest vulnerability (Gehl & Lawson, 2022).

Security professionals know that end-user behavior is still one of the biggest risks. But with the right approach, end-users can be the best security advocates. Educating users about security threats and best practices is a full-time responsibility, not just when a crisis emerges. Social distractions have long been a primary threat and cyberattacks are more successful when user attention is diverted elsewhere.

Influencers

In the Age of Social Media, the term "Influencer" is a popular moniker. It denotes a person or organization with perceived expert knowledge about a subject and the ability to influence a social, marketing, economic, political, and other type of decision. Shau and Gilly (2003) recognized the seismic changes that Internet culture was having on social interaction, presaging the global rise of a culture that turned customers into social media content consumers and creators, forecasting the rise of a self-branding culture by predicting the sudden emergence of Influencers. More recently, Kozinets (2019) offered new technocultural effects of cybercultures and consumer experiences with his research on Influencers.

Historically, self-presentation as conceptualized builds on Goffman's (1959) theories of identity and social performance. Social actors engage in complex intra-self-impressions maintained through consistently performing coherent and complementary behaviors (Schlenker, 1975). Similar to *Influencers*, Goffman termed this process *Impression Management.*

We recommend that ICT and Cybersecurity Departments appoint and train good communicators as Cyberculture Influencers to engage with the user communities and management. Akin to train-the-trainer techniques, these Influencers can also recruit and reward other users as new Influencers, as well. These include the development of policies that can be understood, adhered to, and enforced; change management efforts that improve practices; implement incentives for desired behaviors that also identify and enforce compliance; and introduce new efforts that emphasize change in knowledge/awareness and in attitude.

Security leaders can use awareness programs accompanied by good communication to gradually enhance cybersecurity culture throughout an organization, as well as improve specific user behavior. Over time, security teams can cultivate a network of Influencers throughout the business to create a healthier cybersecurity culture and good stewards of the intellectual property, both corporate and personal. But first, cybersecurity leaders must look inward, at their organizations, themselves, and their communication styles. Table 3 offers our recommendations for ICT Groups to foster, implement, and communicate positive healthy cyberculture to executives and employees.

Table 3: ICT Personnel Can Be Influencers, too.
Make Communication Skills a Top ICT/Security Team Priority; Speak the Language/Vocabulary of the Audience
Understand Security Culture and Awareness Concepts
Use Awareness Programs to Improve User Behaviors and Practices
Commence Cybersecurity Campaign: Incentives, Awards, Prizes, Recognition
Issue Cyberculture Security Newsletter with Tips, Advice, and Cyber Games
Reward Positive Cyber Behavior with Company Swag, Totes, T-Shirts, Caps, Mugs, & Buttons
Secure Executive Management Support; Identify a Senior Sponsor or Champion for Cybersecurity
Develop Influencers (Relevant Communicators and Users in All Organizational Roles and Levels)
Commit to Improving Security for On-site and Remote Employees and Executive Leadership
Measure Results; Update Policies, Procedures, and Training Programs; Focus on User-Friendly Outreach; SMILE

Measuring Cyberculture. Blum (2020, p. 96) argues that measuring cyberculture is challenging, unless one is only concerned with quantitative results, such as counting the number of employees at training sessions, how many times per year training is offered, number of cyber incidents reported per quarter, etc.

These types of metrics may not prove useful, except for audit and governance purposes, unless the employees show visible and observable improvement in their cultural actions and behaviors (Roer, 2018). For example, measuring incidents can be confusing, as leadership may inquire if more people are making cyber errors or are more people just coming forward to report? Incident metrics alone will not resolve cyberculture issues. Observations and conversations are equally important.

A security cyberculture is the part of a business culture's self-sustaining patterns of behavior and perception that determine how (or if) the organization pursues cybersecurity. It is an amalgamation of perceptions about and behavior toward the business' own ICT and security systems, policies, and operational practices and projects. Security culture is not fixed, it is constantly evolving based on people's experiences and social interactions.

Collins (2009, p. 103) analyzed CISO soft skills using system theory. In the author's model, the negative inputs degrade the system, producing negative outputs and a vicious circle that degrades the culture. Positive inputs and outputs do the opposite. Since all security cultures have a mix of positive and negative flows, systems theory plays a role in organizational culture, and cyberculture is just one of the component parts; therefore, the business and cyber strategies must align with all the sub-cultures, as well.

A security strategy is a conscious effort by ICT and business leaders to transform their cyberculture into one that's more conducive to information protection and risk management; and sustain the security culture at the desired state as the business changes over time (Collins, et al., 2021). Security cyberculture can impact an organization's risk levels, compliance posture, and costs or benefits in both positive and negative ways. Business and security leaders ignore it at their own risk, or they can leverage it to get better outcomes.

Black Swans. We also identified that Black Swans occasionally surfaced within the cyberculture, whereas organizational members appeared to understand and commit to good cybersecurity practices, but in fact implemented workarounds or shadow ICT (Vaibhav, 2021) to return to previous cyber habits and vulnerable practices. The Black Swan process describes the falsifiability of research induction by identifying an instance of uncertainty when discovering a gap in what we thought we knew to be completely different from what we previously understood, or thought we knew (Taleb, 2007). These rule exceptions are critical contributions to the analysis of positive healthy cybercultures vs. negative unhealthy ones (Jensen, 1993).

Cyberculture Plans for Strategy, Leadership, Trust, Data, Remote Workers, & Empowerment

In many cases, organizational structure and systems follow culture. Most culture models are overly simplistic because they help an organization to assert a mission or values statement. But culture is more complex than simple, more unique than common, and more evolving than static (Collette, et al., 2009). For example, companies that prioritize teamwork and collaboration can design incentive systems that include shared team and company goals along with rewards that recognize collective effort.

Strategy and Leadership. It is hard to overestimate the importance of aligning cyberculture and leadership. The character and behavior of a CEO and top executives have a profound effect on the organization. Conversely, culture serves to either constrain or enhance the performance of leaders. Survey data from executive recruiting activities shows that a lack of cultural fit is responsible for up to 68% of new-hire failures at the senior leadership level (Doughtie, 2022). For individual leaders, cultural fit is as important as capabilities and experience. And for its full benefit to be realized, a cyberculture must support the strategic goals and plans of the business.

Trust. Trust is all about people and the effective way to enhance trust is to acknowledge that it will always be a work-in-progress. Typically, the most effective way to build trust is to listen, learn, and lead with empathy. We propose that when users tell ICT that security protocols are difficult to follow, they aren't lectured or ignored. ICT should seek to understand and find adoptable solutions. Encourage users to speak up about mistakes, and reward proactive behavior. Trust within an organization multiplies when it is generously and wisely given, and when people feel heard (Parenty & Domet, 2021). Remote and on-site employees need to trust that there are systems in place to support them, too. Companies need to weave trust throughout their entire ecosystem of cyberculture.

Employees Education and Empowerment. Unfortunately, some aspects of security practice have earned a bad reputation over the years, as well-meaning ICT teams implemented security solutions that placed barriers between people and the information they need to do their jobs. People will always find a way to workaround security measures that don't align with business needs. If end-users see security as something that gets in the way, organizations will always face unnecessary risks. Effective security comes from having tools and solutions that are easy to implement and follow, such as user awareness and training programs. When employees practice a strong cyberculture, they are empowered to make good decisions.

Organizations need strong education programs and ICT Departments should look at leadership to support them in ways that organically mesh into the culture of learning within an organization. It matters because it creates a work environment full of empowered people who feel invested in the company's success, which is a trust-based security posture that money can't buy. Salesforce, Southwest, and CISCO are a few examples of organizations that have created conscious intentional cultures. They are purpose driven, list professional growth as a value, are profitable, donate 1% of employee's time to causes, and consistently make Fortune's Best Places to Work list (Fortune, 2022). These corporations proudly display and post their well-earned recognitions on the Internet and in their offices.

Once cyberculture is defined, the next key step is to identify and eliminate gaps between that vision and the employee experience. Organizations that have a true purpose, value learning, care about employees, and create fun at work, will achieve good results. Ultimately cybersecurity is everybody's business according to their role and companies need to make cybersecurity part of every job description to ensure the longevity of a positive healthy cyberculture.

Conclusion

This limited curation of literature provided a sample of the current cyberculture research performed. As we studied and analyzed the work products, we were able to establish cyberculture patterns, trends, and anomalies of complex behaviors and practices. And as we consider the future work that this review may elicit, it is important to realize that cyber infoscapes and technocultures are composed not merely human physical and tangible objects, but rather behavioral flows of tacit and explicit information.

Digital security is a key challenge affecting the world and accepting that cybersecurity is not (just) a technical problem is a positive path forward. Ultimately companies need to make security part of every job description. Trust, awareness, communication, influencers, and accountability are paramount, specifically generated from the top-down. Incorporating these elements will elicit and frame a positive healthy cyberculture between the groups, comprising a cybersystem inextricably linked and integral to each other.

Numerous studies point out that cybersecurity stems primarily from the persistent sources of human behavior and vulnerability. And the question before us remains, what is the role of culture (or lack of cultural philosophy), and in particular, the role of cyberculture as reflected in the attitude and behavior of

organizational employees? But we need more research to combine embedded observations of organizations and their collective behaviors, operationalized by technology's ability to connect each other through social awareness and effective communication. Our work began with the literature review exploration of technological changes in the cybercultures of digital organizations; but our research will continue as we apply and test our theory through future ethnographic field observations and case study conversations applied to workplace practical experiences.

Cyberculture and cybersecurity are more than awareness; they are social sciences and social phenomena (Blum, 2020, p. 96). To paraphrase Schein (1996), if you don't manage business culture, it manages you, and you may not even be aware to the extent to which this is happening. Likewise, lacking a positive healthy cyberculture could break a security program. More work is needed to understand how cyberculture impacts the business strategies of organizations. Every day, the world confronts us with new and unprecedented levels of machine development and adoption. It follows that the human dimension is a significant source of cyber vulnerability; therefore, we submit that creating a cyberculture by which a pattern of shared basic assumptions that support both the aspects of information security, business strategy, and trust as a daily behavioral practice is a major step toward a positive cyber solution.

References

Appadurai, A. (1990). Disjuncture & difference in the global cultural economy, IN *Media & Cultural Studies* (Chapter 33), Durham, M., & Kellner, D., Eds. Blackwell Publishing, 584-603.

Blum, D. (2020). *Rational cybersecurity for business*. Apress Open.

Borkovich, D. J., & Skovira, R. J. (2019). Cybersecurity & Social Engineering: Who's worse, employees or hackers? *Issues in Information Systems*, *20*(3), 139-150.

Collette, R., Gentile, M., & Gentile, S. (2009). *CISO soft skills: Securing organizations.* CRC Press.

Collins, J., Schneider, M., & Shoard, P. (2021). Security Culture Framework (CLTRe). *Gartner KnowBe4*. https://securityculturefframework.net

Cybersecurity Culture Gap Report. (2018). ISACA/CMMI's Institute Study. https://www.isaca.org/-/media/info/cybersecurity-culture-report/index.html

Doughtie, L. (May, 2022). *US CEO Report*. KPMG US, LLC. https://assets.kpmg/content/dam/kpmg/us/pdf/2022/05/kpmg-ceo-outlook-2022.pdf

Drucker, P. (1954). *The practice of management*. Harper & Row.

Elliot, R. (2022). Culture Factor: Why employee experience is more important than you think. *Conscious Culture Group*. https://consciousculturegroup.com/the-culture-factor-hbr-article-review/

Ellul, J. (1964). *The Technological Society*. Vintage Books.

Firat, F., Dholakia, N., & Venkatesh, A. (1995). Marketing in a postmodern world. *European Journal of Marketing, 29*(1), 40-56.

100 Best Companies (2023). *Fortune Online.* https://fortune.com/ranking/best-companies/2023/search/

Ge, J., & Gretzel, U. (2018). Emoji Rhetoric: A Social Media Influencer Perspective. *Journal of Marketing Management, 34*(15-16), 1272-1295.

Geertz, C. (1973). *The interpretation of cultures*. Basic Books.

Gehl, R., & Lawson, S. (2022). *Social engineering.* The MIT Press.

Goffman, E. (1959). *The presentation of self in everyday life.* Anchor Books.

Groysberg, B., Lee, J., Price, J., & Cheng, J. (Jan.-Feb., 2018). The Culture Factor. *Harvard Business Review, 1*(4), 43-57. https://hbr.org/2018/01/the-culture-factor

Hampden-Turner, C., & Trompenaars, F. (2000). *Building cross-cultural competence: How to create wealth from conflicting values.* Yale University Press.

Hanspal, L. (Jan., 2021). Cybersecurity Is Not (Just) a Tech Problem. Harvard Business Review. https://hbr.org/2021/01/cybersecurity-is-not-just-a-tech-problem

Heidegger, M. (1954). The Question Concerning Technology, IN *Technology and Values: Essential Readings*, Craig Hanks (Ed.). Wiley-Blackwell, 99-113.

Hofstede, G. (1994). Business cultures. *The Unesco Courier, 4*, 12-14. Retrieved June 29, 2010, from Research Library. (Document ID: 8733488).

Hofstede, G. (1996). An American in Paris: The influence of nationality on organization theories. *Organization Studies, 17*(3), 525-537.

Hofstede, G. (1998). Attitudes, values and organizational culture: Disentangling the concepts. *Organizational Studies, 19*(3), 477-493.

Hofstede, G. (2018). Signs your organization culture is not working. *Hofstede Insights.* https://news.hofstede-insights.com/news/2018/06/15/ask-an-expert-when-an-organization-culture-is-not-working

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind*. McGraw-Hill.

Jensen, J. (1993). Computer culture: Meaning of technology and technology of meaning. IN Anderson, P., Holmqvist, B., & Jensen, J. F. (Eds.). *The Computer as Medium* (pp. 292-337). Cambridge Press.

Kozinets, R. V. (2019). Consuming technocultures. *Journal of Consumer Research, 46*(3), 620-627.

KnowBe4 Security Culture Report. (2022). *KnowBe4*. https://www.knowbe4.com/organizational-cyber-security-culture-research-report

Lin, C., & Ha, L. (2010). Subculture, critical mass, and technology use. *Journal of Computer Information Systems, 50*(3), 72-80.

Marsh, W. M. (1998). *The impact of context on team process and performance: Cross cultural examination of globalized teams*. ProQuest Dissertations Database. (UMI No. 9915897)

May, R. (2018). *The human firewall: Cybersecurity is not just an IT problem*. Independently published.

Meadows, D. H. (2008). *Thinking in systems: A primer*. Chelsea Green Publishing Company.

Mick, D., & Fournier, S. (1998). Paradoxes of Technology: Consumer Cognizance, Emotions, & Coping Strategies, *Journal of Consumer Research*, *25*(2), 123-143.

Mumford, L. (1967). *The Myth of the Machine: Technics & Human Development*. Secker & Warburg.

Nord, J. N., Sargent, C. S., Koohang, A., & Marotta, A. (2022). Predictors of success in information security
policy compliance. *Journal of Computer Information Systems, 62*(4), 863-873.

Nye, D. E. (2006). *Technology Matters: Questions to Live With*. MIT Press.

Parenty, T., & Domet, J. (2020). *A leader's guide to cybersecurity*. Harvard Business Review.

Paul, I., & Porche, I. (2011). Toward a US Army Cyber Security Culture. *International Journal of Cyber Warfare and Terrorism, 1*(3), 1-11. DOI: 10.4018/ijcwt.2011070105

Penley, C., & Ross, R., (1991). *Technoculture*. University of Minnesota Press.

Postman, N. (1992). *Technopoly: The Surrender of Culture to Technology.* Vintage Books.

Relihan, T. (Jan, 2019). Cybersecurity isn't just for tech people anymore. MIT Sloan Management. https://mitsloan.mit.edu/ideas-made-to-matter/cybersecurity-isnt-just-tech-people-anymore-heres-why

Roer, K. (2018). Security culture: Measure to improve. *CLTRe.* https://get.clt.re/report

Schau, H., & Gilly, M. (2003). We are what we post: Self-presentation in personal web space. *Journal of Consumer Research, 30*(3), 385-404.

Schein, E. H. (1996). Culture: The missing concept in organization studies. *Administrative Science Quarterly, 41*(2), 229-240. Retrieved May 25, 2011, from ABI/INFORM Global. ID: 9820938.

Schein, E. H. (2009). *The corporate culture survival guide* (2nd ed.). Jossey-Bass.

Schein, E. H. (2010). *Organizational culture and leadership* (4th ed.). Jossey-Bass.

Schlenker, B. (1975). Self-presentation. *Journal of Personality & Social Psychology, 32*, 1030-1037.

Self, D. (July, 2018). *State of executive cybersecurity awareness*. MediaPro. www.mediapro.com/blog/infographic-executive-cybersecurity/

Semaw, S., Rogers, M., Quade, J., Renne, P., Butler, R., Dominguez-Rodrigo, M., Stout, D., Hart, W., et al. (2003). 2.6-Million-Year-Old Stone Tools, *Journal of Human Evolution, 45*(2), 169-77.

SHRM Employee Engagement Survey. (2021). *Society for HR Management (SHRM).* https://www.shrm.org/resourcesandtools/business-solutions/pages/employee-engagement-survey-service.aspx

Skovira, R. J. (2010). Toward a theory of informing objects. *Issues in Informing Science and Information Technology, 7*, 369-374.

Taleb, N. (2007). *Black swan: Impact of the highly improbable*. Random House, USA.

Vaibhav, G. (2021). *The art of cybersecurity management*. New Haven: Independently Published.

Vasudevan, S., Piazza, A., & Carr, M. (2022). Qualitative organizational cyber resilience, *2022 Int'l. Conf. on Cyber Resilience (ICCR)*, Dubai, UAE, pp. 1-5. doi: 10.1109/ICCR56254.2022.9995762