CLASSICALLIBRARY : Pages:1–17

Original Research

Developing a Culture of Security in the Workplace: The Role of Training, Policy, and Management in Maintaining Information Assurance

Cemre Kaya[1] and Burak Ergin[2]

[1]Munzur University, Department of Computer Engineering, Vali Tuncay Sonel Street No:58, Tunceli, Turkey.
[2]İzmir Katip Çelebi University, Department of Software Engineering, Havaalanı Şosesi No:33, İzmir, Turkey.

Abstract

Information security breaches continue to pose significant threats to organizations worldwide, with human factors being identified as the weakest link in cybersecurity defense systems. This research examines the critical role of organizational culture in establishing and maintaining robust information security practices within workplace environments. The study investigates how comprehensive training programs, well-defined security policies, and committed management leadership contribute to developing a sustainable culture of security awareness among employees. Through analysis of security incident patterns, employee behavior modification strategies, and organizational change management principles, this paper presents a framework for cultivating security-conscious workplace cultures. The research demonstrates that organizations implementing integrated approaches combining regular security training, clear policy frameworks, and visible management commitment achieve significantly higher levels of security compliance and reduced incident rates. Key findings indicate that security culture development requires sustained effort across multiple organizational levels, with particular emphasis on continuous education, policy reinforcement, and behavioral change mechanisms. The study concludes that successful information assurance depends not merely on technological solutions but fundamentally on creating organizational environments where security consciousness becomes embedded in daily work practices and decision-making processes.

1. Introduction

The digital transformation of modern workplaces has fundamentally altered the landscape of information security challenges facing organizations today [1]. As businesses increasingly rely on interconnected systems, cloud-based services, and remote work arrangements, the traditional perimeter-based security models have proven inadequate in addressing contemporary threats. The human element within organizational security frameworks has emerged as both the greatest vulnerability and the most promising avenue for strengthening overall security posture. [2, 3]

Information security incidents continue to escalate in frequency and sophistication, with studies indicating that over 85% of successful cyberattacks involve some form of human error or social engineering component. This statistic underscores the fundamental reality that technology alone cannot provide comprehensive security protection [4]. Instead, organizations must recognize that their employees represent the first and most critical line of defense against security threats.

The concept of security culture encompasses the shared values, beliefs, attitudes, and behaviors that characterize how an organization and its members approach information security responsibilities [5]. Unlike traditional security measures that focus primarily on technical controls and compliance requirements, security culture addresses the psychological and social dimensions of security behavior. This cultural approach recognizes that sustainable security improvements require fundamental changes

in how employees think about, prioritize, and execute security-related activities in their daily work routines [6] [7].

Contemporary workplace environments present unique challenges for security culture development. The proliferation of bring-your-own-device policies, remote work arrangements, and collaborative technologies has blurred traditional organizational boundaries and created new vectors for security vulnerabilities [8]. Employees often operate in environments where convenience and productivity pressures compete directly with security requirements, necessitating cultural approaches that align security practices with business objectives rather than positioning them as impediments to operational efficiency.

The economic impact of security breaches further emphasizes the importance of cultural approaches to information assurance [9]. Organizations experiencing significant security incidents face not only immediate financial losses but also long-term reputational damage, regulatory penalties, and loss of competitive advantage. The average cost of a data breach has risen to approximately $4.45 million globally, with costs varying significantly based on industry sector and organizational size [10]. These financial implications demonstrate that investments in security culture development represent strategic business imperatives rather than optional compliance activities.

Research in organizational behavior and change management provides valuable insights into the mechanisms through which security cultures develop and evolve [11]. Cultural transformation requires sustained effort across multiple organizational levels, involving leadership commitment, structural changes, and individual behavior modification. The process typically involves several stages, including awareness creation, skill development, attitude adjustment, and behavior reinforcement [12]. Each stage presents distinct challenges and requires specific interventions to ensure successful progression toward desired cultural outcomes.

The role of training in security culture development extends beyond traditional awareness programs to encompass comprehensive education strategies that address both technical competencies and behavioral change objectives. Effective security training programs must account for diverse learning styles, varying levels of technical expertise, and different risk perceptions among employee populations [13]. Moreover, training initiatives must be designed to create lasting behavioral changes rather than temporary compliance responses.

Policy frameworks provide the structural foundation for security culture development by establishing clear expectations, procedures, and accountability mechanisms [14]. However, the effectiveness of security policies depends significantly on how they are communicated, implemented, and reinforced within organizational contexts. Policies that are perceived as overly restrictive, impractical, or disconnected from actual work requirements often generate resistance and non-compliance behaviors that undermine overall security objectives. [15]

Management leadership represents perhaps the most critical factor in successful security culture development. Leaders at all organizational levels must demonstrate visible commitment to security principles through their decisions, resource allocations, and personal behaviors [16]. The concept of security leadership extends beyond formal authority positions to include informal influencers who shape organizational norms and expectations regarding security practices.

2. Theoretical Framework for Security Culture Development

The theoretical foundation for understanding security culture development draws from multiple disciplinary perspectives, including organizational psychology, information systems theory, risk management principles, and behavioral economics [17]. These diverse theoretical lenses provide complementary insights into the complex processes through which organizations develop and maintain security-conscious cultures.

Social cognitive theory offers valuable frameworks for understanding how security behaviors develop and persist within organizational contexts [18]. According to this theoretical perspective, behavior change occurs through the interaction of personal factors, environmental influences, and behavioral

consequences. In security culture contexts, personal factors include individual knowledge, skills, attitudes, and risk perceptions related to information security [19]. Environmental influences encompass organizational policies, social norms, physical security controls, and technological systems that shape security-related decision-making. Behavioral consequences include both positive and negative outcomes that result from security-related actions or inactions. [20]

The theory of planned behavior provides another important theoretical lens for analyzing security culture development processes. This theory suggests that behavioral intentions are the primary predictors of actual behavior, with intentions being influenced by attitudes toward the behavior, subjective norms regarding the behavior, and perceived behavioral control [21]. In security contexts, employees' intentions to follow security procedures are influenced by their attitudes toward security practices, their perceptions of organizational and peer expectations regarding security behavior, and their confidence in their ability to execute security procedures effectively.

Organizational culture theory contributes essential insights into the mechanisms through which shared values, beliefs, and assumptions develop and influence behavior within organizational settings [22]. Culture operates at multiple levels, including observable artifacts such as policies and procedures, espoused values that guide decision-making, and underlying assumptions that represent deeply held beliefs about organizational reality. Security culture development requires attention to all three levels, ensuring alignment between formal security requirements, stated organizational values, and fundamental assumptions about security importance and responsibility.

Risk perception theory helps explain why individuals and organizations often fail to adopt appropriate security behaviors despite awareness of potential threats [23]. Psychological research demonstrates that human risk assessment processes are subject to various cognitive biases and heuristics that can lead to systematic underestimation or overestimation of security risks. For example, the availability heuristic causes people to judge the likelihood of security incidents based on how easily they can recall examples of such incidents, potentially leading to overreaction to highly publicized but statistically rare events while underestimating more common but less visible threats. [24]

Protection motivation theory provides a framework for understanding the psychological processes that motivate individuals to adopt protective behaviors in response to perceived threats. According to this theory, protection motivation results from the evaluation of threat severity, threat vulnerability, response efficacy, and self-efficacy [25]. In security contexts, employees are more likely to adopt security behaviors when they perceive security threats as serious and personally relevant, believe that recommended security measures will effectively mitigate threats, and feel confident in their ability to implement security procedures successfully.

The concept of security climate represents the shared perceptions that employees hold regarding the priority, support, and implementation of security within their organization [26]. Security climate differs from security culture in that climate represents more surface-level perceptions that can change relatively quickly, while culture represents deeper-level assumptions and values that change more slowly. However, security climate and culture are closely related, with climate often serving as a leading indicator of cultural development and change.

Behavioral economics principles illuminate the role of incentives, cognitive biases, and decision-making contexts in shaping security-related behaviors. Traditional economic models assume that individuals make rational decisions based on complete information and consistent preferences [27]. However, behavioral economics research demonstrates that actual decision-making processes are influenced by various psychological factors that can lead to seemingly irrational choices. In security contexts, these insights help explain why employees sometimes choose convenient but risky behaviors even when they understand the potential consequences. [28]

The diffusion of innovations theory provides insights into how new security practices and technologies spread throughout organizations. This theory identifies several factors that influence the rate and extent of innovation adoption, including the perceived relative advantage of the innovation, its compatibility with existing practices and values, its complexity or ease of use, its trialability or ability to be tested on

a limited basis, and its observability or visibility of results [29]. Understanding these factors can help organizations design implementation strategies that facilitate the adoption of new security practices.

Systems theory perspectives emphasize the interconnected nature of organizational elements and the importance of considering security culture development as a systemic change process rather than a series of isolated interventions [30]. From this perspective, security culture development requires attention to the relationships and interactions between various organizational components, including formal structures, informal networks, technological systems, and external environments.

3. Training and Education Strategies

The development of effective security training and education programs requires a sophisticated understanding of adult learning principles, behavioral change mechanisms, and the specific challenges associated with security knowledge transfer [31]. Traditional approaches to security training often fall short of their intended objectives because they fail to account for the complex cognitive and motivational factors that influence learning and behavior change in organizational contexts.

Adult learning theory provides essential guidance for designing security education programs that resonate with working professionals. Adult learners bring significant prior experience, established mental models, and specific motivational orientations to learning environments [32]. They tend to be most engaged when training content is directly relevant to their immediate work responsibilities, builds upon their existing knowledge and skills, and provides opportunities for active participation and problem-solving. Security training programs that ignore these principles often result in passive compliance rather than genuine understanding and commitment. [33]

Experiential learning approaches have shown particular promise in security education contexts. These approaches emphasize learning through direct experience, reflection, abstract conceptualization, and active experimentation [34]. In security training, experiential learning might involve simulated phishing exercises, tabletop incident response scenarios, or hands-on activities with security technologies. Such approaches help participants develop both declarative knowledge about security principles and procedural knowledge about how to apply security practices in realistic work situations. [35]

The concept of situated learning emphasizes the importance of learning within authentic contexts that closely resemble actual work environments. Security training that occurs in artificial or overly simplified settings may fail to transfer effectively to real-world situations where employees face competing priorities, time pressures, and ambiguous circumstances [36]. Situated learning approaches might involve training activities that are embedded within actual work processes, case studies based on realistic organizational scenarios, or peer-to-peer learning opportunities that leverage the expertise of experienced employees.

Microlearning strategies have gained popularity in security education due to their alignment with contemporary work patterns and attention spans [37]. Rather than delivering security training through lengthy, infrequent sessions, microlearning approaches provide brief, focused learning experiences that can be integrated into daily work routines. These might include short video modules, interactive quizzes, security tips delivered through email or messaging systems, or just-in-time learning resources that are accessible when employees encounter specific security challenges. [38]

Personalization and adaptive learning technologies offer opportunities to customize security training experiences based on individual learning preferences, job roles, risk exposures, and performance history. Advanced learning management systems can track learner progress, identify knowledge gaps, and automatically adjust content delivery to optimize learning outcomes for each participant [39]. Personalized learning approaches recognize that employees have different baseline knowledge levels, learning styles, and security responsibilities that require tailored educational interventions.

Gamification strategies can enhance engagement and motivation in security training programs by incorporating game-like elements such as points, badges, leaderboards, and challenges [40]. Well-designed gamification approaches tap into intrinsic motivators such as autonomy, mastery, and purpose while providing immediate feedback and recognition for learning achievements. However, gamification

must be implemented thoughtfully to avoid trivializing serious security topics or creating competitive dynamics that undermine collaborative security objectives.

Social learning approaches recognize that much security knowledge is acquired through observation, interaction, and collaboration with colleagues rather than through formal instruction [41]. Organizations can leverage social learning by creating communities of practice around security topics, implementing peer mentoring programs, encouraging informal knowledge sharing, and providing platforms for employees to share security experiences and lessons learned. Social learning approaches can be particularly effective for addressing the cultural and behavioral dimensions of security that are difficult to convey through traditional training methods. [42]

Simulation-based training provides opportunities for employees to practice security responses in realistic but safe environments. Advanced simulation platforms can replicate complex security scenarios, allowing participants to experience the consequences of their decisions without risking actual organizational assets [43]. Simulation-based training is particularly valuable for developing incident response capabilities, testing emergency procedures, and building confidence in security-related decision-making under pressure.

Continuous learning models recognize that security knowledge and skills require ongoing development rather than one-time acquisition [44]. The rapidly evolving threat landscape, changing technologies, and emerging regulations require security education programs that provide regular updates, refresher training, and opportunities for skill advancement. Continuous learning approaches might involve subscription-based content delivery, regular security briefings, participation in professional development activities, or ongoing assessment and feedback mechanisms. [45]

The integration of security training with performance management systems helps reinforce the importance of security competencies and provides accountability mechanisms for learning outcomes. This integration might involve incorporating security knowledge and skills into job descriptions, performance evaluation criteria, promotion requirements, and compensation decisions [46]. When security competencies are formally recognized and rewarded, employees are more likely to prioritize security learning and apply their knowledge consistently in their work activities.

Measurement and evaluation strategies are essential for assessing the effectiveness of security training programs and identifying opportunities for improvement [47]. Traditional approaches to training evaluation often focus on participant satisfaction and knowledge acquisition rather than behavioral change and business impact. More sophisticated evaluation approaches might involve behavioral observation, incident analysis, simulated assessments, and longitudinal studies that track the relationship between training participation and security performance over time. [48]

4. Policy Development and Implementation

The creation and implementation of security policies represents a critical component of organizational security culture development, serving as the formal mechanism through which security expectations, procedures, and accountability structures are established and communicated. Effective security policies must balance the need for comprehensive coverage of security requirements with practical considerations related to usability, enforceability, and organizational integration. [49]

Policy development processes must begin with thorough risk assessments that identify the specific threats, vulnerabilities, and potential impacts that the organization faces. These assessments should consider both technical and human factors, examining how different types of security incidents might occur and what their consequences would be for organizational operations, reputation, and strategic objectives [50]. Risk-based policy development ensures that security requirements are proportionate to actual threats and aligned with business priorities rather than representing generic or overly conservative approaches that may generate unnecessary compliance burdens.

Stakeholder engagement throughout the policy development process is essential for creating policies that are both technically sound and practically implementable. Key stakeholders typically include security professionals, information technology personnel, legal and compliance teams, human resources

representatives, and operational managers from various business units [51]. Each stakeholder group brings different perspectives, expertise, and concerns that must be considered and balanced in policy design. Meaningful stakeholder engagement helps ensure that policies address real-world challenges and constraints while building buy-in for implementation efforts. [52]

The language and structure of security policies significantly influence their effectiveness and adoption rates. Policies written in highly technical language or complex legal terminology may be difficult for general employees to understand and apply consistently [53]. Conversely, policies that are overly simplified may fail to provide adequate guidance for complex situations or may not meet regulatory requirements. Effective policy writing requires careful attention to audience needs, using clear and accessible language while maintaining necessary precision and comprehensiveness. [54]

Policy hierarchies and relationships must be clearly defined to avoid confusion and conflicts between different policy documents. Organizations typically maintain multiple levels of policy documents, including high-level governance policies that establish general principles and authorities, detailed procedural documents that specify implementation requirements, and technical standards that provide specific configuration or operational guidelines [55]. The relationships between these different policy levels must be clearly articulated, with appropriate cross-references and escalation procedures for situations where policies may conflict or provide inadequate guidance.

Implementation planning represents a critical phase in the policy lifecycle that is often inadequately addressed in organizational practice [56]. Effective implementation requires careful consideration of change management principles, resource requirements, training needs, communication strategies, and timeline considerations. Implementation planning should identify potential barriers to adoption, develop strategies for addressing resistance or confusion, and establish mechanisms for monitoring and supporting the transition to new policy requirements. [57]

Communication strategies for policy implementation must account for the diverse information needs, communication preferences, and organizational positions of different employee groups. Generic policy announcements or mass email distributions are typically insufficient for ensuring adequate understanding and adoption of new security requirements [58]. More effective communication approaches might involve targeted briefings for different functional groups, interactive training sessions that allow for questions and discussion, visual aids or infographics that summarize key requirements, and ongoing reinforcement through multiple communication channels.

Policy enforcement mechanisms are essential for ensuring that security policies translate into actual behavioral change rather than merely representing aspirational statements [59]. Enforcement approaches can range from automated technical controls that prevent policy violations to disciplinary procedures that address non-compliance behaviors. The most effective enforcement strategies combine multiple approaches, using technical controls where feasible while maintaining clear consequences for intentional violations and providing support and additional training for employees who struggle with compliance due to knowledge or skill gaps. [60]

Policy review and update processes ensure that security policies remain current and relevant as organizational circumstances, threat landscapes, and regulatory requirements evolve. Regular policy reviews should examine both the content and effectiveness of existing policies, gathering feedback from users, analyzing compliance data, and assessing whether policies are achieving their intended objectives. Update processes should be systematic and well-documented, with clear procedures for proposing, evaluating, approving, and implementing policy changes. [61]

Exception handling procedures provide mechanisms for addressing situations where standard policy requirements may not be appropriate or feasible. Well-designed exception processes balance the need for flexibility with the importance of maintaining security standards, typically involving risk assessment, alternative control measures, approval authorities, and time-limited approvals with review requirements [62]. Exception processes should be clearly documented and consistently applied to avoid creating precedents that undermine overall policy effectiveness.

Integration with broader organizational governance structures helps ensure that security policies are aligned with other organizational policies, procedures, and objectives [63]. This integration might involve

coordination with human resources policies related to acceptable use and disciplinary procedures, financial policies related to procurement and vendor management, and operational policies related to business continuity and incident management. Alignment with organizational governance structures also helps establish appropriate authority and accountability for security policy implementation and enforcement. [64]

Training and awareness programs must be closely coordinated with policy implementation to ensure that employees have the knowledge and skills necessary to comply with security requirements. Policy-related training should go beyond simply communicating policy content to help employees understand the rationale for requirements, develop practical skills for implementation, and build confidence in their ability to make appropriate security decisions in ambiguous situations [65]. Training programs should also address common misconceptions or resistance points that may interfere with policy adoption.

Metrics and measurement approaches are necessary for assessing policy effectiveness and identifying opportunities for improvement [66]. Policy metrics might include compliance rates measured through technical monitoring or audit activities, incident rates related to specific policy areas, employee feedback on policy clarity and practicality, and business impact measures related to security performance. Effective measurement programs use multiple indicators to provide comprehensive views of policy performance while avoiding over-reliance on easily quantified but potentially misleading metrics. [67]

5. Mathematical Modeling of Security Culture Dynamics

The quantitative analysis of security culture development and maintenance requires sophisticated mathematical frameworks that can capture the complex interactions between individual behaviors, organizational structures, and environmental factors that influence security outcomes. This section presents advanced mathematical models that provide insights into the dynamics of security culture formation, the optimization of intervention strategies, and the prediction of long-term cultural evolution patterns. [68]

Let us define the organizational security culture state as a multidimensional vector $\mathbf{C}(t) = [C_1(t), C_2(t), \ldots, C_n(t)]^T$ where each component $C_i(t)$ represents a specific cultural dimension at time t. These dimensions might include security awareness levels, policy compliance rates, incident reporting behaviors, risk perception accuracy, and collaborative security practices. The evolution of this cultural state can be modeled using a system of differential equations that captures both internal dynamics and external influences. [69]

The fundamental dynamical system governing security culture evolution takes the form:

$$\frac{d\mathbf{C}}{dt} = \mathbf{F}(\mathbf{C}, \mathbf{I}, \mathbf{E}, t)$$

where $\mathbf{F}$ represents the vector field describing cultural change rates, $\mathbf{I}(t)$ represents intervention vectors including training programs and policy changes, and $\mathbf{E}(t)$ represents environmental factors such as threat levels and regulatory requirements.

For individual cultural dimensions, we can express the evolution as: [70]

$$\frac{dC_i}{dt} = \alpha_i(C_{max,i} - C_i) - \beta_i C_i + \gamma_i \sum_{j \neq i} w_{ij} C_j + \delta_i I_i(t) + \epsilon_i E_i(t)$$

This formulation captures several key mechanisms: the first term represents natural improvement toward a maximum cultural state with rate α_i, the second term represents cultural decay with rate β_i, the third term captures interdependencies between cultural dimensions with weights w_{ij}, the fourth term represents the direct impact of interventions with effectiveness δ_i, and the final term captures environmental influences with sensitivity ϵ_i.

The steady-state analysis of this system yields equilibrium conditions where $\frac{d\mathbf{C}}{dt} = \mathbf{0}$. For the single-dimension case without interventions or environmental changes, the equilibrium state is:

$$C_i^* = \frac{\alpha_i C_{max,i} + \gamma_i \sum_{j \neq i} w_{ij} C_j^*}{\alpha_i + \beta_i}$$

The stability of these equilibria can be analyzed through the Jacobian matrix $\mathbf{J}$ of the system:

$$J_{ij} = \frac{\partial F_i}{\partial C_j} = \begin{cases} -(\alpha_i + \beta_i) + \gamma_i w_{ii} & \text{if } i = j \\ \gamma_i w_{ij} & \text{if } i \neq j \end{cases}$$

The system is stable if all eigenvalues of $\mathbf{J}$ have negative real parts, which provides conditions for sustainable security culture development.

To model the impact of training interventions, we introduce a learning function that describes how training effectiveness varies with frequency, intensity, and individual characteristics. Let $T(t)$ represent the cumulative training exposure at time t, with training events occurring at times t_k with intensities I_k: [71]

$$T(t) = \sum_{t_k \leq t} I_k e^{-\lambda(t - t_k)}$$

The exponential decay factor λ accounts for forgetting and skill degradation over time. The impact of training on cultural dimension C_i can then be modeled as: [72]

$$\frac{\partial C_i}{\partial T} = \eta_i \frac{T^\alpha}{T^\alpha + \theta_i^\alpha}$$

This Hill function formulation captures saturation effects where additional training provides diminishing returns beyond certain thresholds.

For policy implementation effects, we model the transition between compliance states using a two-state Markov process where employees can be in compliant (S_C) or non-compliant (S_N) states [73]. The transition rates depend on policy clarity P_c, enforcement probability P_e, and cultural influence C:

$$\lambda_{NC} = k_1 P_c P_e + k_2 C$$

$$\lambda_{CN} = k_3 e^{-k_4 P_e} + k_5 e^{-k_6 C}$$

The steady-state compliance probability is: [74]

$$\pi_C = \frac{\lambda_{NC}}{\lambda_{NC} + \lambda_{CN}}$$

To optimize intervention strategies, we formulate a control problem that maximizes security culture improvement while minimizing intervention costs. The objective function is: [75]

$$J = \int_0^T \left[\sum_{i=1}^{n} w_i C_i(t) - \sum_{j=1}^{m} c_j I_j^2(t) \right] dt$$

subject to the constraint of the cultural evolution dynamics. Using optimal control theory with Lagrange multipliers $\boldsymbol{\lambda}(t)$, the Hamiltonian becomes:

$$H = \sum_{i=1}^{n} w_i C_i - \sum_{j=1}^{m} c_j I_j^2 + \boldsymbol{\lambda}^T \mathbf{F}(\mathbf{C}, \mathbf{I}, \mathbf{E}, t)$$

The optimal control conditions require: [76]

$$\frac{\partial H}{\partial I_j} = -2c_j I_j + \sum_{i=1}^{n} \lambda_i \frac{\partial F_i}{\partial I_j} = 0$$

yielding the optimal intervention intensity:

$$I_j^* = \frac{1}{2c_j} \sum_{i=1}^{n} \lambda_i \delta_{ij}$$

For stochastic modeling of security incidents and their cultural impacts, we employ a marked Poisson process where incidents arrive with rate $\nu(C)$ that depends on the current cultural state [77]. Each incident has an associated severity mark S drawn from distribution $G(s|C)$. The expected incident rate becomes: [78]

$$\mathbb{E}[\text{incidents}] = \int_0^\infty \nu(C(t))dt$$

The cultural impact of incidents can be modeled as sudden state transitions:

$$\mathbf{C}(t^+) = \mathbf{C}(t^-) + \boldsymbol{\phi}(S, \mathbf{C}(t^-))$$

where $\boldsymbol{\phi}$ represents the incident impact function that may include both negative effects from security failures and positive effects from increased awareness.

Network effects in organizational security culture can be modeled using graph-theoretic approaches where employees are nodes connected by influence relationships [79]. Let $\mathbf{A}$ be the adjacency matrix of the influence network and $\mathbf{c}(t)$ be the vector of individual security culture levels. The network evolution follows:

$$\frac{d\mathbf{c}}{dt} = -\mathbf{L}\mathbf{c} + \mathbf{f}(\mathbf{c}) + \mathbf{u}(t)$$

where $\mathbf{L} = \mathbf{D} - \mathbf{A}$ is the graph Laplacian, $\mathbf{f}(\mathbf{c})$ represents nonlinear individual dynamics, and $\mathbf{u}(t)$ represents external interventions.

The convergence properties of this system depend on the network structure, with faster convergence typically occurring in well-connected networks with influential nodes targeted by interventions. The optimal intervention allocation problem becomes: [80]

$$\min_{\mathbf{u}} \int_0^T \left[\|\mathbf{c}(t) - \mathbf{c}^*\|^2 + \rho \|\mathbf{u}(t)\|^2 \right] dt$$

This optimization balances the desire for rapid cultural improvement against intervention costs, with solutions depending on network topology and individual influence patterns.

6. Management Leadership and Organizational Commitment

The role of management leadership in security culture development extends far beyond traditional command-and-control approaches to encompass authentic commitment, visible modeling of security behaviors, strategic resource allocation, and the creation of organizational environments that naturally reinforce security-conscious decision-making [81]. Leadership effectiveness in security contexts requires a sophisticated understanding of how formal authority, informal influence, and organizational systems interact to shape employee attitudes and behaviors regarding information security [82].

Transformational leadership theory provides valuable insights into the mechanisms through which leaders can inspire and motivate employees to embrace security responsibilities as integral components of their professional identities [83]. Transformational leaders in security contexts demonstrate idealized influence by consistently modeling exemplary security behaviors, provide inspirational motivation by articulating compelling visions of organizational security excellence, offer intellectual stimulation by encouraging creative problem-solving approaches to security challenges, and show individualized consideration by recognizing and supporting employees' security-related efforts and achievements.

The concept of security leadership authenticity encompasses the degree to which leaders genuinely believe in and personally commit to the security principles they espouse publicly [84]. Authentic security leaders demonstrate consistency between their stated values and their actual behaviors, willingness to invest personal time and attention in security initiatives, and openness about their own security learning processes and occasional mistakes. This authenticity is particularly important in security contexts because employees are highly sensitive to perceived hypocrisy or inconsistency between leadership rhetoric and actual priorities. [85]

Strategic communication by security leaders involves more than simply disseminating security policies or incident notifications. Effective security communication requires leaders to connect security objectives with broader organizational missions, explain the business rationale for security investments and requirements, share relevant threat intelligence in ways that increase awareness without creating unnecessary anxiety, and provide regular updates on security performance and improvement initiatives [86]. Leaders must also demonstrate skill in crisis communication during security incidents, maintaining employee confidence while acknowledging problems and outlining response plans.

Resource allocation decisions represent perhaps the most visible indicators of genuine leadership commitment to security culture development [87]. These decisions encompass not only financial investments in security technologies and training programs but also the allocation of leadership time and attention, personnel assignments to security roles, and the prioritization of security initiatives relative to other organizational objectives. Employees closely observe these allocation patterns and draw conclusions about the actual importance of security based on resource commitment rather than stated priorities. [88]

Performance management integration requires leaders to establish clear connections between security responsibilities and individual performance expectations, career advancement opportunities, and recognition programs. This integration might involve incorporating security competencies into job descriptions and performance evaluation criteria, creating career development paths that include security-related roles and responsibilities, and ensuring that security contributions are recognized and rewarded alongside other professional achievements [89]. Leaders must also address performance issues related to security non-compliance in ways that are consistent with stated organizational values and expectations.

Governance structure design represents a critical leadership responsibility that determines how security decisions are made, communicated, and implemented throughout the organization [90]. Effective security governance structures balance centralized coordination with distributed responsibility, provide clear escalation procedures for security issues, and establish appropriate oversight and accountability mechanisms. Leaders must also ensure that security governance structures are integrated with broader organizational governance rather than operating in isolation from other business functions.

Change management expertise becomes essential when leaders must guide organizations through significant security culture transformations [91]. These transformations typically involve multiple phases, including creating urgency around security needs, building coalitions of security champions, developing and communicating security vision and strategy, empowering employees to act on security priorities, generating short-term wins that demonstrate progress, consolidating gains and producing additional changes, and anchoring new security behaviors in organizational culture. Each phase requires different leadership approaches and presents distinct challenges that must be addressed thoughtfully. [92]

Risk leadership involves helping organizations develop mature approaches to security risk assessment, communication, and decision-making. Leaders must demonstrate comfort with uncertainty and

ambiguity while making reasonable risk-based decisions with incomplete information [93]. They must also help employees develop appropriate risk perception and decision-making capabilities, avoiding both excessive risk aversion that impedes business operations and inadequate risk consideration that exposes organizations to unnecessary threats.

Cross-functional collaboration leadership requires security leaders to work effectively with colleagues from various organizational functions who may have different priorities, expertise, and perspectives on security issues [94]. This collaboration is essential because security culture development requires integration across human resources, information technology, legal and compliance, operations, and other functional areas. Leaders must demonstrate skill in building consensus, managing conflicts, and finding win-win solutions that address both security and business requirements. [95]

Innovation leadership in security contexts involves encouraging creativity and experimentation in security approaches while maintaining appropriate risk management practices. This might include supporting pilot programs for new security technologies or practices, encouraging employee suggestions for security improvements, creating safe environments for discussing security challenges and failures, and balancing the benefits of innovation with the need for proven and reliable security measures. [96]

Measurement and accountability leadership involves establishing appropriate metrics for security culture development, regularly reviewing progress against security objectives, and taking corrective action when performance falls short of expectations. Leaders must balance quantitative measures that can be easily tracked and compared with qualitative indicators that capture the less tangible aspects of cultural development [97]. They must also demonstrate personal accountability for security outcomes while avoiding blame-oriented approaches that discourage incident reporting and learning.

Stakeholder engagement leadership requires security leaders to build and maintain relationships with various internal and external stakeholders who influence or are affected by organizational security culture [98]. Internal stakeholders might include board members, senior executives, middle managers, front-line employees, and union representatives. External stakeholders might include customers, suppliers, regulatory authorities, industry associations, and community organizations [99]. Effective stakeholder engagement requires understanding different stakeholder perspectives, communication preferences, and influence patterns.

Succession planning and leadership development ensure that security culture development efforts can be sustained over time despite inevitable leadership transitions [100]. This involves identifying and developing future security leaders, documenting and transferring security culture knowledge and practices, and creating organizational structures and systems that support security culture maintenance regardless of specific individual leaders. Succession planning should address both formal leadership positions and informal influence roles that contribute to security culture development.

7. Implementation Challenges and Solutions

The translation of security culture development concepts into practical organizational implementations presents numerous challenges that require sophisticated problem-solving approaches and adaptive management strategies [101]. These challenges span technical, organizational, psychological, and resource-related domains, often requiring coordinated interventions across multiple organizational levels and timeframes [102].

Resistance to change represents one of the most pervasive challenges in security culture implementation [103]. This resistance can manifest at individual, group, and organizational levels, with different underlying causes requiring different intervention approaches. Individual resistance might stem from fear of increased workload, skepticism about security threats, previous negative experiences with security measures, or simple preference for familiar routines [104]. Group resistance might emerge from established social norms, collective skepticism about management motives, or concern about impacts on group productivity or autonomy. Organizational resistance might result from competing priorities, resource constraints, or institutional inertia that favors existing practices over new security requirements. [105]

Addressing resistance requires careful diagnosis of underlying causes combined with targeted intervention strategies. Communication-based approaches might involve providing additional rationale for security changes, addressing specific concerns and misconceptions, and creating opportunities for dialogue between security leaders and skeptical employees [106]. Participation-based approaches might involve including resistant individuals or groups in security planning processes, soliciting input on implementation approaches, and providing opportunities for employees to shape security initiatives rather than simply receiving mandated changes. Support-based approaches might involve providing additional training, resources, or assistance to help employees succeed with new security requirements. [107]

Resource constraints present ongoing challenges for security culture implementation, particularly in organizations facing competitive pressures or economic difficulties. Security culture development requires sustained investments in training, communication, technology, and personnel that may compete with other organizational priorities [108]. These resource challenges are often compounded by the difficulty of quantifying the return on investment for security culture initiatives, making it challenging to justify expenditures relative to more tangible business investments.

Effective resource management for security culture development requires creative approaches to maximizing impact while minimizing costs [109]. This might involve leveraging existing organizational communication channels and training programs to deliver security content, utilizing peer-to-peer learning approaches that reduce formal training requirements, implementing phased implementation approaches that spread costs over time, and seeking external funding or support through industry partnerships or regulatory programs. Organizations might also explore shared service approaches where security culture resources are developed collaboratively across multiple organizations or industry sectors. [110]

Measurement and evaluation challenges arise from the inherently complex and multifaceted nature of organizational culture. Traditional metrics such as compliance rates or incident frequencies provide important but incomplete pictures of security culture development. More comprehensive measurement approaches require combining quantitative indicators with qualitative assessments, longitudinal studies that track changes over time, and multi-perspective evaluations that gather feedback from various stakeholder groups. [111]

References

[1] V. Shapo, "Cybersecurity implementation aspects at shipping 4.0 and industry 4.0 concepts realization," *HEALTH SCIENCES QUARTERLY*, vol. 2, pp. 1–12, 10 2018.

[2] D. Cerdeiro, M. Dziubiiski, and S. Goyal, "Contagion risk and network design," *SSRN Electronic Journal*, 1 2015.

[3] S. Khanna and S. Srivastava, "Patient-centric ethical frameworks for privacy, transparency, and bias awareness in deep learning-based medical systems," *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 3, no. 1, pp. 16–35, 2020.

[4] B. S. Rawal, G. Eberhardt, and J. Lee, "Cybersecurity snapshot: Google, twitter, and other online databases," *Journal of Advanced Computer Science & Technology*, vol. 5, pp. 14–22, 5 2016.

[5] V. K. Aggarwal and A. W. Reddie, "Comparative industrial policy and cybersecurity: a framework for analysis," *Journal of Cyber Policy*, vol. 3, pp. 291–305, 9 2018.

[6] H. Baik and J. Valenzuela, "Unmanned aircraft system path planning for visually inspecting electric transmission towers," *Journal of Intelligent & Robotic Systems*, vol. 95, pp. 1097–1111, 10 2018.

[7] I. Ahmed, R. Mia, and N. A. F. Shakil, "Mapping blockchain and data science to the cyber threat intelligence lifecycle: Collection, processing, analysis, and dissemination," *Journal of Applied Cybersecurity Analytics, Intelligence, and Decision-Making Systems*, vol. 13, no. 3, pp. 1–37, 2023.

[8] E. T. Gilmore, P. D. Frazier, I. J. Collins, W. Reid, and M. F. Chouikha, "Infrared analysis for counterfeit electronic parts detection and supply chain validation," *Environment Systems and Decisions*, vol. 33, pp. 477–485, 11 2013.

[9] L. Slusky, R. S. Hayes, and R. Lau, "Information security risks and countermeasures in cpa practices," *Accounting and Finance Research*, vol. 2, pp. 123–, 8 2013.

[10] N. Lau, R. Pastel, P. M. R. Chapman, J. Minarik, J. Petit, and D. Hale, "Human factors in cybersecurity – perspectives from industries:," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 62, pp. 139–143, 9 2018.

[11] J. Dawson and R. Thomson, "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance.," *Frontiers in psychology*, vol. 9, pp. 744–744, 6 2018.

[12] J. Q. Chen, "A framework for cybersecurity strategy formation," *International Journal of Cyber Warfare and Terrorism*, vol. 4, pp. 1–10, 7 2014.

[13] K. Littlejohn, V. Rajabian-Schwart, N. S. Kovach, and C. P. Satterthwaite, "Mission systems open architecture science and technology (moast) program," *SPIE Proceedings*, vol. 10205, pp. 1020504–, 4 2017.

[14] J. G. Ronquillo, J. E. Winterholler, K. Cwikla, R. Szymanski, and C. Levy, "Health it, hacking, and cybersecurity: national trends in data breaches of protected health information.," *JAMIA open*, vol. 1, pp. 15–19, 6 2018.

[15] C. Lewin, K. W. Lai, H. van Bergen, A. Charania, J. G. Ntebutse, B. Quinn, R. Sherman, and D. Smith, "Integrating academic and everyday learning through technology: Issues and challenges for researchers, policy makers and practitioners," *Technology, Knowledge and Learning*, vol. 23, pp. 391–407, 8 2018.

[16] A. Nagurney, P. Daniele, and S. Shukla, "A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints," *Annals of Operations Research*, vol. 248, pp. 405–427, 4 2016.

[17] E. K. Hawthorne, "Creating 2+2 education pathways in cybersecurity," *ACM Inroads*, vol. 6, pp. 33–35, 5 2015.

[18] T. Chen, Y. Wang, P. Liu, Q. Zhou, and C. Zhang, "Using im-visor to stop untrusted ime apps from stealing sensitive keystrokes," *Cybersecurity*, vol. 1, pp. 1–17, 6 2018.

[19] F. Chen, J. H. Yu, and N. Gupta, "Obfuscation of embedded codes in additive manufactured components for product authentication.," *Advanced engineering materials*, vol. 21, pp. 1900146–, 4 2019.

[20] D. M. Schaeffer and P. C. Olson, "Securing confidence with data escrow," *International Journal of Management & Information Systems (IJMIS)*, vol. 22, pp. 1–6, 12 2018.

[21] K. X. Bancroft, "Regulating information security in the government contracting industry: Will the rising tide lift all the boats?," *The American University law review*, vol. 62, pp. 3–, 5 2013.

[22] W. J. Gordon, A. Wright, R. Aiyagari, L. Corbo, R. J. Glynn, J. Kadakia, J. Kufahl, C. Mazzone, J. Noga, M. A. Parkulo, B. Sanford, P. Scheib, and A. B. Landman, "Assessment of employee susceptibility to phishing attacks at us health care institutions.," *JAMA network open*, vol. 2, pp. e190393–, 3 2019.

[23] R. E. Hebner, F. M. Uriarte, A. Kwasinski, A. L. Gattozzi, H. B. Estes, A. Anwar, P. Cairoli, R. A. Dougal, X. Feng, H.-M. Chou, L. J. Thomas, M. Pipattanasomporn, S. Rahman, F. Katiraei, M. Steurer, M. O. Faruque, M. A. Rios, G. Ramos, M. J. Mousavi, and T. McCoy, "Technical cross-fertilization between terrestrial microgrids and ship power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 4, pp. 161–179, 5 2015.

[24] M. S. Jalali, M. Bruckes, D. Westmattelmann, and G. Schewe, "Why employees (still) click on phishing links: Investigation in hospitals.," *Journal of medical Internet research*, vol. 22, pp. e16775–, 1 2020.

[25] B. Ransford, D. B. Kramer, D. F. Kune, C. Yan, W. Xu, T. Crawford, and K. Fu, "Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists.," *Pacing and clinical electrophysiology : PACE*, vol. 40, pp. 913–917, 7 2017.

[26] W. Ren, X. Lian, and K. Ghazinour, "Skyline queries over incomplete data streams," *The VLDB Journal*, vol. 28, pp. 961–985, 10 2019.

[27] M. M. Mello, J. Adler-Milstein, K. L. Ding, and L. Savage, "Legal barriers to the growth of health information exchange-boulders or pebbles?," *The Milbank quarterly*, vol. 96, pp. 110–143, 3 2018.

[28] B. Kim and S.-B. Cho, "3d tsv-based inductor design for a secure internet of things," *International Symposium on Microelectronics*, vol. 2016, pp. 000364–000367, 10 2016.

[29] I. Ahmed, R. Mia, and N. A. F. Shakil, "An adaptive hybrid ensemble intrusion detection system (ahe-ids) using lstm and isolation forest," *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 3, no. 1, pp. 52–65, 2020.

[30] N. Baracaldo, B. Palanisamy, and J. Joshi, "G-sir: An insider attack resilient geo-social access control framework," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, pp. 84–98, 1 2019.

[31] W. H. Maisel, J. E. Paulsen, M. B. Hazelett, and K. A. Selzman, "Striking the right balance when addressing cybersecurity vulnerabilities.," *Heart rhythm*, vol. 15, pp. e69–e70, 5 2018.

[32] J. L. Servadio and M. Convertino, "Optimal information networks: Application for data-driven integrated health in populations," *Science advances*, vol. 4, pp. e1701088–, 2 2018.

[33] J. Wagner, J. N. Paulson, X. Wang, B. Bhattacharjee, and H. C. Bravo, "Privacy-preserving microbiome analysis using secure computation," *Bioinformatics (Oxford, England)*, vol. 32, pp. 1873–1879, 2 2016.

[34] B. Schooley, S. Walczak, N. Hikmet, and N. Patel, "Impacts of mobile tablet computing on provider productivity, communications, and the process of care," *International journal of medical informatics*, vol. 88, pp. 62–70, 1 2016.

[35] W. He and Z. J. Zhang, "Enterprise cybersecurity training and awareness programs: Recommendations for success," *Journal of Organizational Computing and Electronic Commerce*, vol. 29, pp. 249–257, 7 2019.

[36] B. Croteau and D. Krishnankutty, "Cyber-physical security research at umbc's eclipse lab," *Mechanical Engineering*, vol. 139, pp. S18–S23, 3 2017.

[37] M. E. Shin, T. Kang, and S. Kim, "Blackboard architecture for detecting and notifying failures for component-based unmanned systems," *Journal of Intelligent & Robotic Systems*, vol. 90, pp. 571–585, 10 2017.

[38] V. Chandola and V. Kumar, "Icdm - summarization - compressing data into an informative representation," *Knowledge and Information Systems*, vol. 12, pp. 355–378, 10 2006.

[39] Z. Yang and X. Guo, "Teaching hadoop using role play games," *Decision Sciences Journal of Innovative Education*, vol. 18, pp. 6–21, 2 2020.

[40] G. Jin, M. Tu, T. Kim, J. Heffron, and J. White, "Evaluation of game-based learning in cybersecurity education for high school students," *Journal of Education and Learning (EduLearn)*, vol. 12, pp. 150–158, 2 2018.

[41] B. Bohara, J. N. Bhuyan, F. Wu, and J. Ding, "A survey on the use of data clustering for intrusion detection system in cybersecurity.," *International journal of network security & its applications*, vol. 12, pp. 1–18, 1 2020.

[42] S. J. Blanke and E. McGrady, "When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist.," *Journal of healthcare risk management : the journal of the American Society for Healthcare Risk Management*, vol. 36, pp. 14–24, 7 2016.

[43] L. Nanni, S. Brahnam, and A. Lumini, "Face detection ensemble with methods using depth information to filter false positives.," *Sensors (Basel, Switzerland)*, vol. 19, pp. 5242–, 11 2019.

[44] D. Chatterjee, "Should executives go to jail over cybersecurity breaches," *Journal of Organizational Computing and Electronic Commerce*, vol. 29, pp. 1–3, 1 2019.

[45] S. Li and I. Alon, "China's intellectual property rights provocation: A political economy view," *Journal of International Business Policy*, vol. 3, pp. 60–72, 9 2019.

[46] S. Jain, E. W. Felten, and S. Goldfeder, "Determining an optimal threshold on the online reserves of a bitcoin exchange," *Journal of Cybersecurity*, vol. 4, 1 2018.

[47] B. K. Payne, B. Hawkins, and C. Xin, "Using labeling theory as a guide to examine the patterns, characteristics, and sanctions given to cybercrimes," *American Journal of Criminal Justice*, vol. 44, pp. 230–247, 11 2018.

[48] S. Weber, "Coercion in cybersecurity: What public health models reveal," *Journal of Cybersecurity*, vol. 3, pp. 173–183, 5 2017.

[49] W. A. Wulf and A. K. Jones, "Unlocking the door to better cybersecurity—response," *Science*, vol. 327, pp. 1451–1451, 3 2010.

[50] T. G. Bakker and K. Streff, "Accuracy of self disclosed cybersecurity risks of large u.s. banks," *THE JOURNAL OF APPLIED BUSINESS AND ECONOMICS*, vol. 18, pp. 39–51, 7 2016.

[51] H. Darabian, A. Dehghantanha, S. Hashemi, M. Taheri, A. Azmoodeh, S. Homayoun, K.-K. R. Choo, and R. M. Parizi, "A multiview learning method for malware threat hunting: windows, iot and android as case studies," *World Wide Web*, vol. 23, pp. 1241–1260, 1 2020.

[52] C. Molinaro, V. Moscato, A. Picariello, A. Pugliese, A. Rullo, and V. S. Subrahmanian, "Padua: Parallel architecture to detect unexplained activities," *ACM Transactions on Internet Technology*, vol. 14, pp. 3–28, 7 2014.

[53] Z. M. Bodnar, R. Schuchard, D. Myung, M. E. Tarver, M. S. Blumenkranz, N. A. Afshari, M. S. Humayun, C. L. Morse, K. Nischal, M. X. Repka, D. T. Sprunger, M. T. Trese, and M. B. Eydelman, "Evaluating new ophthalmic digital devices for safety and effectiveness in the context of rapid technological development.," *JAMA ophthalmology*, vol. 137, pp. 939–944, 8 2019.

[54] N. A. F. Shakil, R. Mia, and I. Ahmed, "Applications of ai in cyber threat hunting for advanced persistent threats (apts): Structured, unstructured, and situational approaches," *Journal of Applied Big Data Analytics, Decision-Making, and Predictive Modelling Systems*, vol. 7, no. 12, pp. 19–36, 2023.

[55] M. van Eeten and J. M. Bauer, "Emerging threats to internet security: Incentives, externalities and policy implications," *Journal of Contingencies and Crisis Management*, vol. 17, pp. 221–232, 11 2009.

[56] B. Hamdan, "Teaching case study: introducing data analytics in an advanced cybersecurty course," *Journal of Computing Sciences in Colleges*, vol. 33, pp. 113–120, 12 2017.

[57] M. Hecht and D. Baum, "Use of sysml for the creation of fmeas for reliability, safety, and cybersecurity for critical infrastructure," *INCOSE International Symposium*, vol. 29, pp. 145–158, 9 2019.

[58] M. C. Lacity, S. A. Khan, and A. Yan, "Review of the empirical business services sourcing literature: An update and future directions," *Journal of Information Technology*, vol. 31, pp. 269–328, 9 2016.

[59] J. Healey, "The implications of persistent (and permanent) engagement in cyberspace," *Journal of Cybersecurity*, vol. 5, 1 2019.

[60] C. J. Lesko, "A design case: Assessing the functional needs for a multi-faceted cybersecurity learning space," *Journal of Cybersecurity Education, Research and Practice*, vol. 2019, 6 2019.

[61] T. August, R. August, and H. Shin, "Designing user incentives for cybersecurity," *Communications of the ACM*, vol. 57, pp. 43–46, 10 2014.

[62] Z. Su, W. Wang, L. Li, H. E. Stanley, and L. A. Braunstein, "Optimal community structure for social contagions," *New Journal of Physics*, vol. 20, pp. 053053–, 5 2018.

[63] P. Rajivan, E. Aharonov-Majar, and C. Gonzalez, "Update now or later? effects of experience, cost, and risk preference on update decisions," *Journal of Cybersecurity*, vol. 6, 1 2020.

[64] A. Jones and J. Straub, "Using deep learning to detect network intrusions and malware in autonomous robots," *SPIE Proceedings*, vol. 10185, pp. 1018505–, 5 2017.

[65] K. Salah, M. Hammoud, and S. Zeadally, "Teaching cybersecurity using the cloud," *IEEE Transactions on Learning Technologies*, vol. 8, pp. 383–392, 10 2015.

[66] S. Zeadally, A.-S. K. Pathan, C. Alcaraz, and M. Badra, "Towards privacy protection in smart grid," *Wireless Personal Communications*, vol. 73, pp. 23–50, 12 2012.

[67] S. Walczak and V. Velanovich, "Prediction of perioperative transfusions using an artificial neural network.," *PloS one*, vol. 15, pp. e0229450–, 2 2020.

[68] R. Jorgensen, D. C. Rowe, and N. Wyler, "Competitions and gamification in cybersecurity education and workforce development and evaluation of real world skills," *Journal of Computing Sciences in Colleges*, vol. 33, pp. 155–156, 12 2017.

[69] H. Niu and S. Jagannathan, "Optimal defense and control of dynamic systems modeled as cyber-physical systems," *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, vol. 12, pp. 423–438, 7 2015.

[70] L. Bitomsky, O. Bürger, B. Häckel, and J. Töppel, "Value of data meets it security – assessing it security risks in data-driven value chains," *Electronic Markets*, vol. 30, pp. 589–605, 2 2020.

[71] J. Zheng and A. S. Namin, "A survey on the moving target defense strategies: An architectural perspective," *Journal of Computer Science and Technology*, vol. 34, pp. 207–233, 1 2019.

[72] A. Xiong, R. W. Proctor, W. Yang, and N. Li, "Embedding training within warnings improves skills of identifying phishing webpages.," *Human factors*, vol. 61, pp. 577–595, 12 2018.

[73] S. A. Kusumastuti, J. Blythe, H. Rosoff, and R. S. John, "Behavioral determinants of target shifting and deterrence in an analog cyber-attack game.," *Risk analysis : an official publication of the Society for Risk Analysis*, vol. 40, pp. 476–493, 9 2019.

[74] P. Jungwirth, T. Barnett, and A.-H. A. Badawy, "Rootkits and the os friendly microprocessor architecture," *SPIE Proceedings*, vol. 10185, pp. 1018503–, 5 2017.

[75] Y. Lu, "Cybersecurity research: A review of current research topics," *Journal of Industrial Integration and Management*, vol. 03, pp. 1850014–, 11 2018.

[76] N. Tan, G. Shoemaker, A. Gedi, J. Mache, and R. Weiss, "Applying a framework for creating and analyzing cybersecurity questions for peer instruction," *Journal of Computing Sciences in Colleges*, vol. 33, pp. 102–108, 10 2017.

[77] S. Romanosky, L. Ablon, A. Kuehn, and T. Jones, "Content analysis of cyber insurance policies: how do carriers price cyber risk?," *Journal of Cybersecurity*, vol. 5, 1 2019.

[78] O. Malomo, D. B. Rawat, and M. Garuba, "Security through block vault in a blockchain enabled federated cloud framework," *Applied Network Science*, vol. 5, pp. 1–18, 2 2020.

[79] P. Lawson, C. J. Pearson, A. Crowson, and C. B. Mayhorn, "Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy.," *Applied ergonomics*, vol. 86, pp. 103084–, 3 2020.

[80] D. Frincke, D. Craigen, N. Nadima, A. Low, and M. Thomas, "Tim lecture series – three collaborations enabling cybersecurity," *Technology Innovation Management Review*, vol. 5, pp. 45–48, 6 2015.

[81] M. Tabassum, T. Kosinski, A. Frik, N. Malkin, P. Wijesekera, S. Egelman, and H. R. Lipford, "Investigating users' preferences and expectations for always-listening voice assistants," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, pp. 1–23, 12 2019.

[82] Y. Jani, "Real-time anomaly detection in distributed systems using java and apache flink," *European Journal of Advances in Engineering and Technology*, vol. 8, no. 2, pp. 113–116, 2021.

[83] T. Hu, K.-Y. Wang, W.-H. Chih, and X.-H. Yang, "Trade off cybersecurity concerns for co-created value," *Journal of Computer Information Systems*, vol. 60, pp. 468–483, 11 2018.

[84] C. L. Canonne and T. Gur, "An adaptivity hierarchy theorem for property testing," *computational complexity*, vol. 27, pp. 671–716, 5 2018.

[85] D. C. de Leon, A. Q. Stalick, A. A. Jillepalli, M. Haney, and F. T. Sheldon, "Blockchain: properties and misconceptions," *Asia Pacific Journal of Innovation and Entrepreneurship*, vol. 11, pp. 286–300, 12 2017.

[86] K. R. Fitzpatrick, C. White, and L. M. Bier, "C-suite perspectives on corporate diplomacy as a component of public diplomacy," *Place Branding and Public Diplomacy*, vol. 16, pp. 25–35, 5 2019.

[87] M. Dawson, "National cybersecurity education: Bridging defense to offense," *Land Forces Academy Review*, vol. 25, pp. 68–75, 3 2020.

[88] G. J. McKee and A. Kagan, "Community bank structure an x-efficiency approach," *Review of Quantitative Finance and Accounting*, vol. 51, pp. 19–41, 8 2017.

[89] Y. Z. Chen, Z.-G. Huang, and Y.-C. Lai, "Controlling extreme events on complex networks," *Scientific reports*, vol. 4, pp. 6121–6121, 8 2014.

[90] J. Eckroth, "Teaching cybersecurity and python programming in a 5-day summer camp," *Journal of Computing Sciences in Colleges*, vol. 33, pp. 29–39, 6 2018.

[91] D. N. Burrell, C. Nobles, M. Dawson, T. McDowell, and A. M. Hines, "A public policy discussion of food security and emerging food production management technologies that include drones, robots, and new technologies," *Perspectives of Innovations, Economics and Business*, vol. 18, pp. 71–87, 7 2018.

[92] J. C. Ong, "Limits and luxuries of slow research in radical war: how should we represent perpetrators?," *Digital War*, vol. 1, pp. 111–116, 3 2020.

[93] G. Wang, G. B. Giannakis, J. Chen, and J. Sun, "Distribution system state estimation: an overview of recent developments," *Frontiers of Information Technology & Electronic Engineering*, vol. 20, pp. 4–17, 1 2019.

[94] D. F. Norris, L. Mateczun, A. Joshi, and T. Finin, "Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity," *Public Administration Review*, vol. 79, pp. 895–904, 2 2019.

[95] J. Brown, M. Anwar, and G. Dozier, "An artificial immunity approach to malware detection in a mobile platform," *EURASIP Journal on Information Security*, vol. 2017, pp. 7–, 3 2017.

[96] D. H. Duong, W. Susilo, and H. T. N. Tran, "A multivariate blind ring signature scheme," *The Computer Journal*, vol. 63, pp. 1194–1202, 11 2019.

[97] R. Weiss, J. Ladish, J. Mache, and M. E. Locasto, "Hands-on cybersecurity exercises for introductory classes: tutorial presentation," *Journal of Computing Sciences in Colleges*, vol. 32, pp. 173–175, 10 2016.

[98] Z. Wang, H. Wu, G. W. Burr, C. S. Hwang, K. L. Wang, Q. Xia, and J. Yang, "Resistive switching materials for information processing," *Nature Reviews Materials*, vol. 5, pp. 173–195, 1 2020.

[99] M. F. Grady and F. Parisi, "The law and economics of cybersecurity: An introduction," *SSRN Electronic Journal*, 1 2004.

[100] S. G. Brooks, "Power transitions, then and now: five new structural barriers that will constrain china's rise," *China International Strategy Review*, vol. 1, pp. 65–83, 6 2019.

[101] R. J. Harknett, J. P. Callaghan, and R. D. Kauffman, "Leaving deterrence behind: War-fighting and national cybersecurity," *Journal of Homeland Security and Emergency Management*, vol. 7, 1 2010.

[102] S. Khanna, "Identifying privacy vulnerabilities in key stages of computer vision, natural language processing, and voice processing systems," *International Journal of Business Intelligence and Big Data Analytics (IJBIBDA)*, vol. 4, no. 1, 2021.

[103] L. Weiland and G. Wei, "Evaluating the impact of nextgen's air traffic system on aviation security," *MATEC Web of Conferences*, vol. 189, pp. 10030–, 8 2018.

[104] R. S. Gutzwiller, K. Ferguson-Walter, and S. Fugate, "Are cyber attackers thinking fast and slow? exploratory analysis reveals evidence of decision-making biases in red teamers:," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 63, pp. 427–431, 11 2019.

[105] S. R. Moore, H. Ge, N. Li, and R. W. Proctor, "Cybersecurity for android applications: Permissions in android 5 and 6," *International Journal of Human–Computer Interaction*, vol. 35, pp. 630–640, 7 2018.

[106] L. I. Hadzhidimova and B. K. Payne, "The profile of the international cyber offender in the u.s.," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 2, pp. 40–55, 2 2019.

[107] H. Blauw, P. Keith-Hynes, R. Koops, and J. H. DeVries, "A review of safety and design requirements of the artificial pancreas," *Annals of biomedical engineering*, vol. 44, pp. 3158–3172, 6 2016.

[108] B. Kim and S.-B. Cho, "A secure tunable lna design for internet of things," *International Symposium on Microelectronics*, vol. 2017, pp. 000705–000708, 10 2017.

[109] S. Lawson, "Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the united states," *First Monday*, vol. 17, 6 2012.

[110] A. Root, "Do cells use passwords in cell-state transitions? is cell signaling sometimes encrypted?," *Theory in biosciences = Theorie in den Biowissenschaften*, vol. 139, pp. 87–93, 6 2019.

[111] M. L. Frank, J. H. Grenier, and J. S. Pyzoha, "How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance," *Journal of Information Systems*, vol. 33, pp. 183–200, 1 2019.