Scientific Research Publishing

E-Health Telecommunication Systems and Networks, 2025, 14(3), 31-38
https://www.scirp.org/journal/etsn
ISSN Online: 2167-9525
ISSN Print: 2167-9517

C4 Framework for Healthcare Cybersecurity Defense: A Human-Centric, Socio-Technical Approach

Mostafa Rahmany, Arunmozhi Selvi

Department of Data and Cybersecurity, British University College, Ajman, UAE
Email: GlobalMostafa@gmail.com

How to cite this paper: Rahmany, M. and Selvi, A. (2025) C4 Framework for Healthcare Cybersecurity Defense: A Human-Centric, Socio-Technical Approach. *E-Health Telecommunication Systems and Networks*, **14**, 31-38.
https://doi.org/10.4236/etsn.2025.143004

Received: June 8, 2025
Accepted: July 14, 2025
Published: July 17, 2025

Abstract

Cybersecurity attacks represent a significant threat to healthcare organizations, jeopardizing patient data, clinical operations, and institutional trust. The human element—healthcare workers themselves—continues to be a primary and persistent vulnerability that technological controls alone cannot mitigate. This paper argues that traditional, compliance-oriented security approaches are insufficient to tackle the inherent human factors leveraged by modern cyber attackers. Recognizing that most security incidents stem from human error and social engineering, a new paradigm is needed. This paper presents the C4 Framework, a novel human-centric cybersecurity model tailored to the unique constraints of the healthcare sector. The framework is built on four interdependent pillars: Comprehensive Assessment & Risk Profiling, Customized Education & Training, Cultural Reinforcement & Communication, and Continuous Measurement & Adaptation. By emphasizing a shift in security culture, personalized education, and perpetual evolution, the framework provides a roadmap for transforming an organization's human element from its greatest vulnerability into a resilient defense asset.

Keywords

Security Culture, Healthcare, Human Factor, Insider Threat, C4 Framework, Social Engineering, Human-Computer Interaction, Cybersecurity, Socio-Technical Systems, Change Management

1. Introduction

Healthcare sits at a critical inflection point where technological advancement intersects with high-risk exposure. The digitization of electronic health records

(EHR), the proliferation of the Internet of Medical Things (IoMT), and the rise of telehealth have redefined care delivery but have also dangerously expanded the attack surface for adversaries. As a result, the sector is under constant siege from cybercriminals, leading to ransomware attacks that cripple critical systems and data breaches that compromise sensitive Personal Health Information (PHI) [1]. A comprehensive review of recent trends confirms that the healthcare sector faces numerous, evolving cybersecurity threats owing to this increasing digitization and the considerable value of its data [2]. The traditional approach to security is often insufficient against modern threats, necessitating a shift towards greater cyber resilience and the capacity to adapt in real-time to new attack vectors.

Despite significant investments in technological safeguards, the human element remains the primary vector for such breaches, a reality that exposes the limitations of technology-only security strategies [3]. This challenge is particularly acute in healthcare due to a confluence of environmental factors, including high-stress workloads, and alert fatigue, all of which erode situational awareness and increase susceptibility to deception. Cognitive Load Theory suggests that the high intrinsic cognitive load of clinical tasks leaves fewer mental resources available to process the extraneous load imposed by complex security procedures, making simple, intuitive security design paramount [4]. Recent research underscores that a significant percentage of healthcare-related cyber breaches are initiated via phishing attacks, demonstrating that attackers find it easier to exploit human psychology than to breach technical defenses [3].

While the problem is widely acknowledged, existing solutions often gravitate towards generic, compliance-based training that fails to address the motivational and psychological drivers of human error. The literature reveals a gap for a structured, practical framework designed not merely to raise awareness, but to fundamentally reshape security culture within the specific operational constraints of healthcare. This paper aims to fill this gap by introducing the C4 Framework, a conceptual model that moves beyond compliance to build genuine cybersecurity resilience by placing the human at the center of the defense strategy.

2. Methodology of Framework Development

The C4 Framework is a conceptual model derived from a systematic synthesis of interdisciplinary research and industry best practices. Its development involved three stages:

Literature Review: A comprehensive review of peer-reviewed literature in cybersecurity, human-computer interaction, organizational psychology, and behavioral science was conducted. This included an analysis of established theories such as Schein's Model of Organizational Culture [5], Bandura's Social Learning Theory [6], and Protection Motivation Theory [7] to ground the framework in robust academic principles.

Best-Practice Analysis: An analysis of existing industry frameworks (e.g., NIST [8], ISO 27001 [9]) and compliance mandates (e.g., HIPAA [10]) was performed

to identify gaps related to human-centric controls and cultural integration.

Framework Synthesis: The four pillars of the C4 framework were synthesized from the thematic analysis of the above sources. Each pillar was designed to address a specific weakness in traditional security approaches and to function as part of an integrated, cyclical system.

3. The C4 Human-Centric Awareness Framework

The C4 framework is composed of four interdependent pillars designed to transform the human element from a liability into a defensive asset. Each pillar's focus has been sharpened to reduce overlap and improve clarity, per reviewer suggestions.

3.1. Pillar 1: Comprehensive Assessment & Risk Profiling (The Diagnosis)

This foundational pillar focuses on developing a deep, data-driven understanding of an organization's specific human risks. It moves beyond simple knowledge tests to create a detailed "human vulnerability map". This is achieved through:

Behavioral Risk Surveys: Using qualitative interviews and surveys to understand why risky behaviors occur, identifying friction points in workflows and sources of cognitive load.

Realistic Threat Simulations: Deploying phishing and social engineering campaigns tailored to healthcare scenarios to measure baseline vulnerabilities across different roles and departments.

Insider Threat Profiling: Monitoring data access patterns to identify anomalies that may indicate compromised accounts or inadvertent misuse, recognizing that most insider threats are non-malicious.

3.2. Pillar 2: Customized & Personalized Education (The Education)

Armed with insights from Pillar 1, this pillar rejects one-size-fits-all training in favor of targeted, engaging, and relevant security education that is designed to overcome the Ebbinghaus Forgetting Curve, which shows that individuals forget most new information shortly after learning it without reinforcement [11]. Key principles include:

Role-Based Micro-Learning: Delivering short (5-10 minute), on-demand training modules specific to the risks faced by different roles (e.g., a nurse, a billing administrator) to respect the time constraints of clinical staff. This approach manages cognitive load effectively.

Contextual, Just-in-Time Reminders: Using pop-up prompts and login screen tips to reinforce secure behaviors directly within the workflow, such as a reminder to encrypt an email when PHI is detected.

Interactive and Gamified Learning: Employing formats like competitive quizzes and virtual reality simulations to move beyond passive learning and allow staff to practice secure behaviors in a safe environment.

3.3. Pillar 3: Cultural Reinforcement & Communication (The Environment)

This pillar focuses on embedding security principles into the organization's daily life, making security a shared value rather than an IT mandate. This cultural shift is guided by Lewin's 3-Stage Model of Change (Unfreeze, Change, Refreeze) [12].

Leadership Engagement (Unfreezing): Requiring active, visible sponsorship from senior leadership, who must allocate resources and consistently communicate that security is integral to patient safety. This aligns with Transformational Leadership theory, where leaders inspire a shared vision [13].

Positive Reinforcement and Security Champions (Changing): Implementing recognition programs that reward proactive security behaviors and cultivating a network of motivated "Security Champions" from various departments who act as peer influencers and normalize secure practices through social learning.

No-Blame Reporting (Refreezing): Establishing a psychologically safe system for staff to report incidents or errors without fear of reprisal. This fosters Organizational Justice, as employees who perceive policies as fair are more likely to comply [14].

3.4. Pillar 4: Continuous Measurement & Adaptation (The Evolution)

This final pillar ensures the program remains effective and relevant by creating a data-driven feedback loop. It utilizes the Kirkpatrick Model for training evaluation to assess effectiveness on multiple levels [15].

Behavioral KPIs (Level 3: Behavior): Tracking a decline in phishing simulation click-through rates, an increase in staff-reported suspicious events, and wider adoption of security tools like MFA.

Cultural Metrics (Level 4: Results): Measuring long-term cultural shifts through annual security culture surveys, sentiment analysis of internal communications, and feedback from focus groups.

Programmatic Review: Conducting regular, rigorous reviews of all data to assess impact, identify areas for improvement, and update educational content with the latest threat intelligence.

C4 framework is composed of four interdependent pillars designed to transform the human element from a liability into a defensive asset. Each pillar's focus has been sharpened to reduce overlap and improve clarity, per reviewer suggestions.

4. Application of the Framework: Real-World Case Analyses

4.1. Case Analysis 1: The 2015 Anthem Inc. Phishing Breach

Context: Anthem Inc. is one of the largest health insurance providers in the United States.

Incident: In February 2015, Anthem disclosed a breach that exposed the personal information of nearly 79 million people. The investigation revealed that attackers initiated the breach via a targeted phishing email sent to an Anthem sub-

sidiary, which allowed them to steal administrative credentials and move through Anthem's systems for weeks before detection [16].

Contributing Human Factors: The root cause was a social engineering attack that deceived an employee. A lack of immediate reporting allowed the attackers extended dwell time within the network.

C4 Framework Application:

Pillar 1: An assessment would have identified the high-risk status of system administrators for spear-phishing.

Pillar 2: Customized micro-learning on credential-harvesting attacks would have been delivered to this group.

Pillar 3: A "no-blame" culture would have encouraged immediate reporting of the mistake, drastically reducing attacker dwell time.

Pillar 4: KPIs like mean-time-to-report would be tracked for this user group to refine training.

Projected Outcome: The probability of the initial phishing email succeeding would be lower. More importantly, the cultural mechanisms would be in place to detect and report the intrusion far more quickly, mitigating the scale of the breach.

4.2. Case Analysis 2: The 2011 TRICARE Management Activity Data Breach

Context: TRICARE is the healthcare program for the U.S. Department of Defense Military Health System. The breach involved a business associate, SAIC.

Incident: In September 2011, it was discovered that unencrypted computer backup tapes containing the records of approximately 4.9 million TRICARE patients had been stolen from an SAIC employee's car [17]. The breach was a failure of physical security protocols.

Contributing Human Factors: The primary human error was the employee's violation of data handling policies by removing unencrypted backup media from a secure facility.

C4 Framework Application:

Pillar 1: A risk assessment would have audited physical security practices and data handling workflows.

Pillar 2: Customized training for IT staff would include rigorous modules on physical security and data lifecycle management.

Pillar 3: A strong security culture would reinforce that protecting patient data is critical, regardless of its format.

Pillar 4: Measurement would include regular physical security audits and spot-checks of data handling procedures.

Projected Outcome: An employee embedded in a C4-driven culture would be far less likely to violate a critical data handling policy, averting the breach entirely.

5. Discussion: Benefits, Implications, and Scalability

Adopting the C4 framework shifts an organization from a reactive, compliance-focused posture to a proactive, resilient one. By directly addressing the human

factor the root cause of most organizations breaches and security weakness which can significantly reduce the likelihood of costly data loss, unauthorize access or breaches, thereby safeguarding patient data, building trust, and ensuing continuity of care.

5.1. Scalability and Adaptation for Varied Contexts

The C4 framework is designed to be scalable to address concerns about organizational capacity. Smaller or under-resourced organizations can begin with a phased implementation, focusing on low-cost, high-impact initiatives first:

Phase 1 (Foundational): Start Pillar 1 with simple surveys and free phishing simulation tools. Launch a volunteer-based "Security Champions" network (Pillar 3).

Phase 2 (Developing): Introduce role-based micro-learning (Pillar 2) using internal expertise. Formalize the no-blame reporting process.

Phase 3 (Mature): Invest in more advanced simulation tools and automated "just-in-time" training systems as resources allow.

5.2. Cost-Benefit Considerations

While a full cost-benefit analysis for implementing the C4 Framework is organization-specific, its value proposition can be clearly framed in terms of cost avoidance. The investment in a human-centric program pales in comparison to the catastrophic costs of a major healthcare breach. According to industry reports, the healthcare sector consistently suffers the highest average data breach costs [2]. To illustrate with a specific case, the 2015 Anthem breach resulted in a record $16 million HIPAA settlement [18] and over $115 million to settle related class-action lawsuits [19]. More recently, the 2024 Change Healthcare ransomware attack caused massive disruptions, with the parent company reporting over $872 million in unfavorable effects in a single quarter due to the attack [20]. The return on investment for a C4-style program is measured by the reduction of this risk.

6. Conclusions

As a conceptual model, the C4 Framework has limitations that present opportunities for future research. Its successful implementation depends heavily on sustained leadership support and resource allocation. The primary direction for future work, as can be highlighted, is the empirical validation of the framework. A longitudinal study monitoring the KPIs outlined in Pillar 4 within a healthcare organization would provide invaluable data on its effectiveness. Comparative research studying the impact of customized education modules versus generic training could offer further evidence. Finally, investigating the use of machine learning and AI to further personalize simulations and just-in-time training represents a promising frontier for optimizing the framework's delivery in real-time.

Limitations and Future Directions

As a conceptual model, the C4 Framework has limitations that present opportuni-

ties for future research. Its successful implementation depends heavily on sustained leadership support and resource allocation. The primary direction for future work, as highlighted by the reviewers, is the empirical validation of the framework. A longitudinal study monitoring the KPIs outlined in Pillar 4 within a healthcare organization would provide invaluable data on its effectiveness. Comparative research studying the impact of customized education modules versus generic training could offer further evidence. Finally, investigating the use of machine learning and AI to further personalize simulations and just-in-time training represents a promising frontier for optimizing the framework's delivery in real-time.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] HIMSS (2024) 2024 HIMSS Cybersecurity Survey. Healthcare Information and Management Systems Society.

[2] IBM Security (2024) Cost of a Data Breach Report 2024. Ponemon Institute.

[3] Verizon (2025) 2025 Data Breach Investigations Report. Verizon Enterprise Solutions.

[4] Sweller, J. (1988) Cognitive Load during Problem Solving: Effects on Learning. *Cognitive Science*, **12**, 257-285. https://doi.org/10.1207/s15516709cog1202_4

[5] Schein, E.H. (2010) Organizational Culture and Leadership. 4th Edition, Jossey-Bass.

[6] Bandura, A. (1977) Social Learning Theory. Prentice Hall.

[7] Rogers, R.W. (1975) A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, **91**, 93-114. https://doi.org/10.1080/00223980.1975.9915803

[8] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29.

[9] International Organization for Standardization (2022) ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements.

[10] U.S. Department of Health & Human Services (1996) Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191.

[11] Murre, J.M.J. and Dros, J. (2015) Replication and Analysis of Ebbinghaus' Forgetting Curve. *PLOS ONE*, **10**, e0120644. https://doi.org/10.1371/journal.pone.0120644

[12] Lewin, K. (1947) Frontiers in Group Dynamics: Concept, Method and Reality in Social Science; Social Equilibria and Social Change. *Human Relations*, **1**, 5-41. https://doi.org/10.1177/001872674700100103

[13] Bass, B.M. (1990) From Transactional to Transformational Leadership: Learning to Share the Vision. *Organizational Dynamics*, **18**, 19-31. https://doi.org/10.1016/0090-2616(90)90061-s

[14] Colquitt, J.A. (2001) On the Dimensionality of Organizational Justice: A Construct Validation of a Measure. *Journal of Applied Psychology*, **86**, 386-400. https://doi.org/10.1037/0021-9010.86.3.386

[15] Kirkpatrick, D.L. (1996) Evaluating Training Programs: The Four Levels. Berrett-Koeh-

ler Publishers.

[16] Krebs, B. (2015) Anthem Breach Exposes 80 Million Patient, Employee Records. Krebs on Security.

[17] U.S. Department of Health & Human Services (2011) Breach Report Details Theft of Backup Tapes Affecting 4.9M. Official HHS Breach Portal Report and Subsequent News Coverage.

[18] U.S. Department of Health & Human Services (2017) Anthem Pays HHS $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History. HHS Press Release.

[19] Stempel, J. (2018) Anthem Agrees to Pay $115 Million to Settle U.S. Data Breach Litigation. Reuters.

[20] UnitedHealth Group (2024) UnitedHealth Group Reports First Quarter 2024 Results.