Scientific Research Publishing

E-Health Telecommunication Systems and Networks, 2025, 14(2), 23-30
https://www.scirp.org/journal/etsn
ISSN Online: 2167-9525
ISSN Print: 2167-9517

CARE Framework for Healthcare Cybersecurity Defense: A Human-Centric Approach

Mostafa Rahmany, Arunmozhi Selvi

Department of Data and Cybersecurity, British University College, Ajman, United Arab Emirates
Email: GlobalMostafa@Gmail.Com

How to cite this paper: Rahmany, M, and Selvi, A. (2025) CARE Framework for Healthcare Cybersecurity Defense: A Human-Centric Approach. *E-Health Telecommunication Systems and Networks*, **14**, 23-30.
https://doi.org/10.4236/etsn.2025.142003

Received: June 8, 2025
Accepted: June 27, 2025
Published: June 30, 2025

Abstract

The health sector remains a key target for cyberattacks due to the sensitive information and critical services it manages. Technical safety measures alone are insufficient when the human factor, frequently the weakest link in the security chain, is not addressed. This paper develops a new human-centric conceptual model, the **CARE** model, which proposes a structured route to creating a robust Cyber Defense Capability within healthcare. CARE is an acronym for **Culture, Awareness, Responsibility**, and **Engagement**. The framework posits that a secure organization must be part of a broader culture of safety, where security education is role-based and context-aware. Within this model, Security Awareness underpins a non-negotiable, shared Responsibility for cybersecurity across all roles, which in turn fosters active Engagement. The CARE framework aims to instigate a paradigm shift, anchoring resilient healthcare controls not only in technology, but across the entire socio-technical stack of people, processes, and technology.

Keywords

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

1. Introduction

The increasing digitization of the healthcare industry, from Electronic Health Records (EHR) to the Internet of Medical Things (IoMT), has significantly enhanced patient care but has also broadened the attack surface for malicious actors. Healthcare institutions are particularly attractive targets due to the high value of their data, the critical need for 24/7 operational status, and the frequent use of legacy equipment [1]. Data breaches can lead to severe consequences, including

significant financial penalties, reputational damage, loss of public trust, and, most critically, risks to patient safety [2].

Traditionally, healthcare risk management has been driven by compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA), focusing primarily on implementing technology-based controls. However, even with clear technical and administrative guidance from standards bodies, such as the National Institute of Standards and Technology (NIST) [3] and the International Organization for Standardization (ISO) [4], the human element remains a persistent and critical vulnerability. The continued success of phishing and social engineering attacks, which remain a top threat action in the healthcare sector [5], highlights a systemic failure to comprehend and effectively address human behavior in high-pressure clinical contexts.

Although security culture and awareness are common topics in cybersecurity literature, the components are often addressed in isolation. The unique contribution of the CARE framework is its innovative structure, which integrates four pillars into a self-reinforcing sequence tailored for a healthcare audience. It argues that a strong security posture cannot be achieved by focusing on these facets independently. Rather, it is the four-step cycle of Culture, Awareness, Responsibility, and Engagement that enables holistic defenses against human-targeted attacks. This paper presents this detailed, actionable model as a bridge between high-level security theory and the operational realities of healthcare.

2. Literature Review

2.1. The Changing Shape of the Risk Spectrum in Healthcare

The healthcare risk landscape is exceptionally demanding. For the 15th consecutive year, healthcare has reported the highest average cost per data breach of any industry [1]. Personal Health Information (PHI) is of extreme value on the black market, making healthcare data a prime target. Furthermore, the life-or-death nature of healthcare services makes organizations acutely vulnerable to ransomware attacks that can halt operations. The attack surface is both wide and deep, ranging from sophisticated social engineering to vulnerabilities in unpatched medical devices [2]. While compliance drivers such as HIPAA provide a baseline for security, mere adherence to a framework is insufficient to protect against a dynamic and aggressive threat landscape.

2.2. The Human Factors, The Frontliners

A majority of significant security incidents—approximately 73%—involve a human element, which includes everything from simple errors to social engineering and privilege misuse [6]. Many current security training programs are ineffective because they do not account for the diverse roles, work habits, and situational contexts of employees, often leading to apathy rather than fostering a strong "human firewall" [7]. This is compounded by issues like alert fatigue, where the sheer volume of system warnings causes clinicians to ignore critical security alerts, a

well-documented issue in high-pressure environments that can lead to increased medical errors [8].

2.3. The Emergence of a Security Culture

The recognition of the inadequacy of traditional training has led to an emphasis on fostering a "security culture". A strong security culture, as defined by organizational theorists like Edgar Schein, is one where security is a shared value, actively supported by leadership, and integrated into the organization's daily operations and priorities [9]. When security is viewed as a collective responsibility rather than just an "IT problem", individuals are more likely to take ownership and adopt secure practices.

3. Methodology of Framework Development

This paper puts forward a conceptual framework and is not an empirical study. Its methodology is based on a systematic integration of three core areas:

- **Literature Review:** A comprehensive review of academic and industry literature in cybersecurity, human factors, and organizational behavior.
- **Best-Practice Analysis:** An analysis of existing industry frameworks (e.g., NIST, ISO) and compliance mandates (e.g., HIPAA) to identify gaps related to human-centric controls.
- **Theoretical Synthesis:** A review of established theories of organizational culture change, behavioral psychology, and employee engagement to provide a robust theoretical foundation for the framework's pillars.

The CARE framework was distilled from a thematic analysis of this synthesized information, designed as a pragmatic, theoretically-grounded model for practical application.

4. The Proposed CARE Framework

The CARE-model is a sociotechnical model for containing cybersecurity in a healthcare organization. It is built on four guiding principles that are interdependent and generate a cycle of continuous enhancement. Below is the CRAE Framework Cycle (Figure 1).

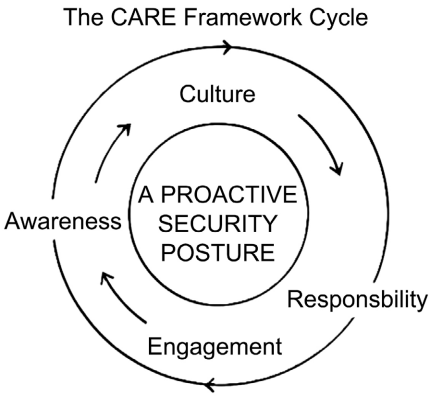

Figure 1. The CARE framework cycle.

This figure is a conceptual diagram illustrating the interdependent and cyclical nature of the framework's four pillars and is not based on quantitative data.

To help organizations operationalize the framework, the following maturity model (Table 1) outlines concrete stages of implementation.

Table 1. CARE framework maturity model.

Pillar	Initial/Ad-Hoc (Level 1)	Developing (Level 2)	Mature (Level 3)	Optimized (Level 4)
Culture	Security is seen as an IT problem. Leadership involvement is minimal and reactive.	Leadership begins to message the importance of security. Security is discussed as a compliance requirement.	Security is explicitly linked to patient safety in communications. Annual security culture surveys are conducted.	Security is a core organizational value. Leadership consistently models secure behaviours. Security is integrated into strategic planning.
Awareness	Generic, annual, check-the-box training. Phishing simulations are rare or non-existent.	Some role-based training is introduced. Phishing simulations are conducted quarterly.	Training is fully role-based and context-aware, using healthcare scenarios. Phishing simulation results are used to tailor training.	Training is continuous, adaptive, and integrated into workflows. Near-misses are used as real-time learning opportunities.
Responsibility	Security responsibility is not defined outside of the IT department.	Security tasks are assigned but not formalized in job descriptions.	Security duties are explicitly included in all job descriptions and performance reviews. A shared responsibility model is officially adopted.	Individuals proactively take ownership of security within their roles. Cross-departmental security champions are established and empowered.
Engagement	Reporting is punitive and discouraged. Staff are passive recipients of policy.	A formal, non-punitive channel for reporting security concerns is created.	Staff are actively invited to participate in policy review and tool selection. A security recognition program is in place.	Staff actively collaborate with IT to co-create security solutions. Security is a regular topic in team meetings, driven by staff.

4.1. Pillar 1: Culture

Implanting and implementing the CARE Framework begins with a "security-first" culture. This starts with leadership demonstrating an unwavering commitment to security, ensuring it is a non-negotiable aspect of the organization's operations. The organizational narrative must clearly link cybersecurity to the core mission of patient safety.

- **Suggested Metrics (KPIs)**: Scores from an annual security culture survey; frequency of security mentions in leadership communications; employee perceptions of security's role in patient safety.

4.2. Pillar 2: Awareness

While culture sets the environment, awareness provides the knowledge and skills for safe behavior. The CARE framework advocates for role-based and context-

aware training programs. This means tailoring training to the specific threats faced by different roles (e.g., medical staff vs. IT administrators) and using real-world healthcare scenarios that address regulations like HIPAA.

- **Suggested Metrics (KPIs):** Click-through and reporting rates in simulated phishing attacks; post-training knowledge assessments; completion rates for role-based training modules.

4.3. Pillar 3: Responsibility

A common failure is viewing information security as solely the IT department's responsibility. The CARE model promotes a culture of collective ownership. This shared responsibility model clarifies that while IT manages the infrastructure, every employee is responsible for its secure use. These responsibilities should be formally defined in job descriptions and performance evaluations.

- **Suggested Metrics (KPIs):** Percentage of job descriptions with explicit security duties; number of security incidents per department; rate of staff-reported security concerns.

4.4. Pillar 4: Engagement

Beyond mere compliance, active engagement is crucial. The framework encourages involving staff in the development of security policies to foster a sense of ownership. It also emphasizes the need for open and non-punitive channels for reporting security issues and mistakes. Simulating incidents with both clinical and administrative staff can provide practical experience in responding to security events.

- **Suggested Metrics (KPIs):** Participation rates in policy review sessions; number of submissions to feedback channels; nominations for proactive security behavior recognition.

5. Discussion and Implications

Adopting the CARE framework signifies a shift from a compliance-driven to a culture-driven, continuous security program. A primary implication is enhanced organizational resilience, where the "human firewall" becomes an active network for threat detection and response. By distributing security ownership, the organization reduces its reliance on the central IT team.

However, implementation requires long-term commitment from leadership, dedicated resources for customized training, and a willingness to redefine roles. Overcoming institutional inertia and moving from a culture of blame to one of transparent, non-punitive error reporting is a significant challenge. It is crucial to remember that the CARE framework complements, rather than replaces, essential technical safeguards.

6. Real-World Case Analyses: Applying the CARE Framework

To demonstrate the framework's practical application, this section analyses two

significant, real-world healthcare breaches through the lens of the CARE pillars.

6.1. Case Analysis 1: The 2024 Change Healthcare Ransomware Attack

- **Incident:** In February 2024, a catastrophic ransomware attack on Change Healthcare, a subsidiary of UnitedHealth Group, paralyzed large parts of the U.S. healthcare system. The attack halted prescription processing, medical billing, and insurance claims for weeks. The root cause was identified as compromised credentials used on a remote access server that lacked multi-factor authentication (MFA) [10]. The financial impact on the parent company was reported to be approximately $872 million in the first quarter alone [11].
- **Human Factor Failure:** The incident highlights a critical intersection of human and policy failure. While the initial entry point was compromised credentials (a common human-centric vulnerability), the core failure was the organizational oversight of not enforcing a basic, mandatory security control (MFA) on a critical, internet-facing system.
- **CARE Intervention:**
  - **Culture:** A security-first culture would mandate that critical infrastructure never be left without fundamental security controls like MFA, viewing it as a non-negotiable standard of care.
  - **Awareness:** Role-based training for IT administrators and all employees would emphasize the critical importance of strong, unique passwords and the role of MFA as a primary defense against credential theft.
  - **Responsibility:** An IT administrator's responsibilities would explicitly include conducting regular audits to ensure all remote access points comply with security baselines. There would be clear accountability for such a significant security gap.
  - **Engagement:** An engaged security team, empowered by leadership, would proactively identify and remediate such critical vulnerabilities rather than letting them persist.

6.2. Case Analysis 2: The 2020 Universal Health Services (UHS) Ransomware Attack

- **Incident:** In September 2020, Universal Health Services, a Fortune 500 owner of hundreds of hospitals, was hit by a Ryuk ransomware attack. The attack shut down IT systems across all 250+ of its U.S. facilities, forcing doctors and nurses to revert to pen and paper, cancelling surgeries, and diverting ambulances. The initial entry point was widely reported to be a phishing email that tricked an employee into launching malware [12].
- **Human Factor Failure:** The root cause was a classic phishing attack that successfully deceived an employee. This single click by one individual was enough to cripple a nationwide hospital network, directly impacting patient care and safety.

- **CARE Intervention:**
  - **Culture:** A strong culture would emphasize constant vigilance and a collective sense of duty to protect clinical systems from external threats.
  - **Awareness:** The employee would have undergone regular, realistic phishing simulations and context-aware training, making them more likely to recognize and report the malicious email instead of engaging with it.
  - **Responsibility:** The employee's role would include a clearly defined responsibility to scrutinize and report suspicious electronic communications.
  - **Engagement:** A non-punitive and easy-to-use "report phishing" button and process would empower the employee to immediately alert the security team. This could have enabled containment before the ransomware payload was deployed across the network, turning a potential catastrophe into a managed incident.

7. Conclusion and Future Researches

As the healthcare industry remains a top target for cyberattacks, a new approach to security is imperative. The CARE framework offers a strategic, human-centric solution that moves beyond compliance to address the root organizational causes of security breaches. By systematically fostering a positive Culture, building relevant Awareness, defining clear Responsibility, and promoting active Engagement, healthcare organizations can embed a robust security posture into their operational core.

Future research should focus on validating the CARE framework through case studies and longitudinal studies within healthcare organizations. Developing a standardized maturity model to quantitatively measure the implementation of the framework would be a valuable contribution, along with research to establish a direct causal link between the adoption of the model and a reduction in security incidents and an improvement in the overall safety culture.

Conflicts of Interest

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

References

[1] IBM Security (2025) Cost of a Data Breach Report 2025. Ponemon Institute.

[2] Ponemon Institute (2023) Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care.

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

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

[5] Z-CERT (2025) Cybersecurity Threat Landscape in Healthcare 2025.

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

[7] SANS Institute (2024) The 2024 SANS Security Awareness Report: The Human Risk.

[8] Ancker, J.S., Edwards, A., Nosal, S., Hauser, D., Mauer, E. and Kaushal, R. (2017) Effects of Workload, Work Complexity, and Repeated Alerts on Alert Fatigue in a Clinical Decision Support System. *BMC Medical Informatics and Decision Making*, **17**, Article No. 36. https://doi.org/10.1186/s12911-017-0430-8

[9] Schein, E.H. (2004) Organizational Culture and Leadership. 3rd Editon, Jossey-Bass.

[10] Witty, A. (2024) Testimony before the U.S. Senate Committee on Finance. United Health Group. As Reported by Multiple News Outlets.

[11] United Health Group (2024) United Health Group Reports First Quarter 2024 Results.

[12] Bleeping Computer (2020) UHS Hospitals Hit by Ryuk Ransomware Attack, Systems Shutdown. As Reported by Multiple Cybersecurity News Outlets.