International Journal of Cybersecurity and Risk Assessment
Volume 1 • Issue 1 • January-December 2025

Toward Human-Centric Cybersecurity:
Case Study Insights and the HuCRAF Model

Olumide O Malomo
https://orcid.org/0000-0003-2592-6953
Virginia State University, USA

Shanzhen Gao
https://orcid.org/0000-0002-3856-2530
Virginia State University, USA

Adeyemi A. Adekoya
Virginia State University, USA

Aurelia M. Donald
https://orcid.org/0009-0008-8058-5657
Virginia State University, USA

Theodore Andrews Jr.
https://orcid.org/0009-0007-4883-7968
Virginia State University, USA

Julian D. Allagan
https://orcid.org/0000-0003-0275-4239
Elizabeth City State University, USA

Weizheng Gao
https://orcid.org/0009-0003-5078-6283
Elizabeth City State University, USA

Jianning Su
https://orcid.org/0000-0002-7443-8940
Perimeter College, Georgia State University, USA

Ephrem Eyob
https://orcid.org/0000-0003-3590-0028
Virginia State University, USA

Received: July 9th, 2025 | **Accepted:** September 3rd, 2025

ABSTRACT

Human vulnerabilities contribute to organizational data breaches across various sectors. Between 2013 and 2024, despite emerging technology and innovations in cybersecurity defenses, recurring patterns such as poor communication, leadership lapses, and decision-making under pressure remain central to the causation of cybersecurity breaches. Using the Dirty Dozen human error framework, the study identifies systemic behavioral risks often overlooked in cybersecurity governance. The authors propose the Human-Centric Risk Assessment Framework (HuCRAF) to fill this void. HuCRAF offers six thematic pillars and six assessment stages to embed behavioral risk into cybersecurity governance. The findings support a shift toward a behavior-informed cybersecurity strategy and a platform for future studies to enhance HuCRAF through decision modeling and algorithmic risk discovery. The recommendations include adopting HuCRAF, measuring security culture, conducting breach simulations, and managing legacy systems.

KEYWORDS

Human Factors, Data Breaches, Cybersecurity, Risk Assessment, Behavioral Risk, Organizational Vulnerabilities, Governance, Incident Response, HuCRAF, Case Study Analysis

INTRODUCTION

Today, data breaches have become increasingly alarming, impacting millions of individuals and compromising the critical infrastructure of both small businesses and large organizations worldwide (Purplesec, 2024). While technical vulnerabilities are often blamed as the root cause of many cybersecurity incidents, growing evidence suggests that human and organizational decisions

DOI: 10.4018/IJCRA.389592

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

are often the underlying cause (Cybernews, 2022; Desolda et al., 2021; Malomo et al., 2024). This study's cross-sectoral observations—including airlines and transportation, healthcare, finance, social media, gaming, and digital retail platforms—reveal an unsettling problem: from health insurance providers to online fitness apps, and from government regulatory bodies to e-commerce giants, the exposure of sensitive personal, financial, and medical data has occurred with regularity (Cybernews, 2022; Purplesec, 2024).

One of the essential insights emerging from this study's analysis is the consistent role of unintentional human error, often characterized in the aviation and safety industries as the Dirty Dozen. These factors include lack of communication, complacency, distraction, lack of knowledge, fatigue, pressure, lack of teamwork, stress, poor norms, lack of resources, lack of assertiveness, and lack of awareness (Malomo et al., 2024; Mellema, 2018). These human factors have manifested in several breach scenarios, including cloud misconfigurations, insecure application programming interfaces (APIs, which allow software systems to communicate), credential stuffing, and legacy system exploitation. Notably, these are not isolated behaviors, but systemic issues embedded within organizational culture and operational workflows (Cybernews, 2022; Jeimy & Cano, 2019; Malomo et al., 2024; Purplesec, 2024).

The prevalence of these factors is even more troubling when examined in conjunction with the nature and sensitivity of the compromised data. Across multiple incidents, organizations have failed to adequately safeguard highly sensitive data, including complete payment card information, Social Security numbers, passport details, health insurance data, and sensitive behavioral profiles. In the airline, healthcare, and credit reporting sectors, for example, breaches have frequently exposed passengers' travel itineraries, confidential medical records, and complete financial profiles. These types of data are highly valuable to threat actors and can be devastating to affected individuals when compromised (Card-Connect, 2023; CUInsight, 2024; European Data Protection Board, 2021; Forbes, 2012; Strategic Risk, 2019; StrongDM, 2025; The HIPAA Journal, 2019; UK Tech News, 2021). Additionally, the digital transformation and rapid expansion of services in sectors such as app-based platforms, mobile services, and cloud storage have exacerbated the problem. As organizations rush to deploy new features and expand their reach to broader audiences, security often becomes an afterthought. The use of third-party APIs, under-tested backend environments, and poorly configured cloud platforms has caused many vulnerabilities. Cases of unauthorized access due to poor authentication, insecure database storage, and inadequate internal controls are recurrent themes (Cascio & Montealegre, 2016; Li et al., 2016; Malomo et al., 2018).

In parallel, internal governance and organizational culture within risk management programs have not evolved in line with the expanding threat landscape. Many small and large business enterprises still operate in silos, where information technology departments remain disconnected from executive leadership and legal teams. Under tremendous pressure to deliver results, decision-makers may ignore security warnings, delay critical updates, or underfund cybersecurity training. This pressure-driven environment often normalizes risk, leading to a lower prioritization of known vulnerabilities until they are inevitably exploited (Hubbard, 2020). Human mistakes do not just happen before a breach; they also shape how the situation is handled afterward. Delays in detection and public disclosure, as usually seen in multiple high-profile cases, are caused by unclear roles, fear of reputational damage, or indecisiveness within the legal community. The lack of communication during these critical windows can exacerbate the impact of a breach, erode public confidence and trust, and result in regulatory fines or litigation (Cybernews, 2022; Desolda et al., 2021; Malomo et al., 2024). Even as cyber threats grow more sophisticated in terms of tactics, techniques, and procedures, such as advanced persistent threats, human behavior tends to be the most vulnerable point of entry for cybercriminals to attack. The findings in this study suggest a growing need to approach cybersecurity through a socio-technical lens, acknowledging the interaction between technology, human cognition, organizational dynamics, and leadership accountability. Building on these observations, this study examines representative breaches through the lens of human factor theory, demonstrating that cybersecurity failures are not

59 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/toward-human-centric-cybersecurity/389592

Related Content

A Proposed Framework for Environmental Risk Assessment (ERA) in Airports

Elen Paraskevi Paraschi (2025). *Cases on Security, Safety, and Risk Management (pp. 227-250).*
www.irma-international.org/chapter/a-proposed-framework-for-environmental-risk-assessment-era-in-airports/358739

Measuring and Analysing Credit Risk

(2019). *Six Sigma Improvements for Basel III and Solvency II in Financial Risk Management: Emerging Research and Opportunities (pp. 37-112).*
www.irma-international.org/chapter/measuring-and-analysing-credit-risk/213277

Managing the Current Risks of Companies: The Applicability of Tax Risk Management

Feride Bakar Türegünand Adnan Gerçek (2022). *Handbook of Research on New Challenges and Global Outlooks in Financial Risk Management (pp. 250-269).*
www.irma-international.org/chapter/managing-the-current-risks-of-companies/296056

Analyzing Online Customer Satisfaction: The Impacts of Perceived Benefits, Perceived Risks, and Trust

Jennifer H. Gao (2019). *International Journal of Risk and Contingency Management (pp. 1-12).*
www.irma-international.org/article/analyzing-online-customer-satisfaction/216866

Proposed Isomorphic Graph Model for Risk Assessment on a Unix Operating System

Prashant Kumar Patraand Padma Lochan Pradhan (2013). *International Journal of Risk and Contingency Management (pp. 49-62).*
www.irma-international.org/article/proposed-isomorphic-graph-model-for-risk-assessment-on-a-unix-operating-system/80020