

# Human-Centered Cybersecurity: Integrating Artificial Intelligence, Zero Trust and Security Awareness to Defend U.S. Institutions

**Abdoulie Sowe**

Independent Researcher, USA

Submitted: September 04, 2026

Accepted: September 12, 2026

Published: September 20, 2026

**Citation:** Abdoulie Sowe (2026) Human-Centered Cybersecurity: Integrating Artificial Intelligence, Zero Trust and Security Awareness to Defend U.S. Institutions. *Epistora J. Artif. Intell. & Intell. Syst.* 1(1), 1-17. Article EJAIS-111

## Abstract

The increasing sophistication of cyber threats presents significant challenges for U.S. institutions responsible for protecting sensitive information, critical infrastructure, and essential services. Traditional cybersecurity approaches that rely primarily on technical controls may be insufficient against threats that exploit human behavior, compromised identities, and rapidly evolving attack techniques. This paper examines a human-centered approach to cybersecurity that integrates Artificial Intelligence (AI), Zero Trust Architecture (ZTA), and continuous cybersecurity awareness. Through a qualitative review of cybersecurity research, government guidance, and industry practices, the study examines how these three capabilities can complement one another to improve organizational cyber resilience. AI can enhance threat detection, behavioral analysis, automation, and incident response; Zero Trust can reduce unauthorized access and limit attacker movement through continuous verification and least-privilege principles; and cybersecurity awareness can strengthen employee preparedness and reduce human-related security risks. Based on this analysis, the paper proposes a Human-Centered Cybersecurity Framework that integrates technology, governance, and people into a unified defensive strategy. The framework emphasizes continuous monitoring, adaptive defense, risk reduction, and workforce participation as interconnected components of cyber resilience. The study concludes that U.S. institutions can strengthen their cybersecurity posture by treating technological innovation, security governance, and human awareness as mutually reinforcing rather than independent security functions. The proposed framework provides a foundation for future empirical research examining the effectiveness of integrated cybersecurity strategies across different organizational and critical infrastructure environments.

**Keywords:** Cybersecurity, Artificial Intelligence, Zero Trust Architecture, Cybersecurity Awareness, Insider Threats, Cyber Resilience, Critical Infrastructure, Human-Centered Security, U.S. Institutions, Cybersecurity Governance

## Introduction

As the United States continues to digitize critical services and infrastructure, cyber threats have grown in sophistication, frequency, and impact. Federal agencies, healthcare organizations, financial institutions, educational systems, and critical infrastructure operators increasingly rely on interconnected technologies to deliver essential services. While advances in cloud computing, artificial intelligence (AI), and automation have improved operational efficiency, they have also expanded the cyberattack surface, creating new opportunities for malicious actors to exploit technical vulnerabilities and human behavior.

Recent cyber incidents demonstrate that many successful attacks are not solely the result of software flaws or inadequate technical controls. Instead, they frequently originate from compromised user credentials, phishing campaigns, insider threats, social engineering, and human error. These incidents highlight an important reality: cybersecurity is not only a technical challenge but also a human challenge. Organizations that invest exclusively in technological defenses without strengthening the human element often remain vulnerable to sophisticated adversaries. Artificial intelligence has emerged as a transformative capability in modern cybersecurity. AI-powered security platforms can rapidly analyze large volumes of network traffic, identify anomalous behavior, automate threat detection, and support incident response. At the same time, cybercriminals increasingly leverage AI to generate convincing phishing campaigns, evade detection, automate malware development, and conduct more sophisticated attacks. This evolving landscape creates an ongoing technological competition between defenders and attackers, requiring continuous innovation in defensive strategies.

Similarly, Zero Trust Architecture (ZTA) has become a foundational cybersecurity framework for protecting modern enterprise environments. Rather than assuming that users or devices within a network are trustworthy, Zero Trust requires continuous verification of identities, devices, applications, and access requests. The adoption of Zero Trust principles across U.S. federal agencies reflects a broader shift toward identity-centric security models that reduce organizational risk by enforcing least-privilege access and continuous monitoring. Despite these technological advances, cybersecurity ultimately depends on the decisions and behaviors of individuals. Employees remain primary targets for phishing, business email compromise, credential theft, and social engineering attacks. Insider threats—whether malicious, negligent, or accidental—continue to account for a significant proportion of organizational security incidents. Consequently, security awareness, cybersecurity education, and a culture of shared responsibility have become essential components of effective cyber defense.

This paper argues that resilient cybersecurity requires a comprehensive, human-centered approach that integrates Artificial Intelligence, Zero Trust Architecture, and continuous security awareness programs. Rather than treating these capabilities as independent security measures, organizations should implement them as complementary components of a unified cybersecurity strategy. AI enhances the speed and accuracy of threat detection, Zero Trust limits attacker movement through continuous verification and least-privilege access, and security awareness empowers individuals to recognize and respond appropriately to cyber threats before they escalate into significant security incidents. The objective of this study is to examine how these three pillars can collectively strengthen cybersecurity resilience within U.S. institutions. Drawing upon current cybersecurity research, government guidance, and emerging best practices, this paper evaluates the benefits, implementation challenges, and policy implications of integrating AI-driven defense mechanisms, Zero Trust principles, and human-centered cybersecurity initiatives. The findings contribute to ongoing discussions regarding national cybersecurity resilience and provide practical recommendations for organizations seeking to reduce cyber risk while protecting critical infrastructure, sensitive information, and public trust.

## **Literature Review**

### **The Human Dimension of Cybersecurity**

Traditional cybersecurity strategies have historically focused on technological solutions such as firewalls, intrusion detection systems, antivirus software, and endpoint protection. While these technologies remain essential, research consistently demonstrates that human behavior continues to represent one of the most significant vulnerabilities within organizational security environments. Social engineering, phishing attacks, credential theft, and insider threats frequently bypass sophisticated technical defenses by exploiting human decision-making rather than software vulnerabilities. Insider threats encompass malicious insiders, negligent employees, contractors, and trusted third parties whose actions intentionally or unintentionally compromise organizational assets. Studies indicate that insider incidents often result in substantial financial losses, operational disruption, and reputational damage because insiders typically possess legitimate access to sensitive systems and information. Recent research has emphasized socio-technical approaches that combine technical controls with organizational policies, behavioral analytics, employee education, and continuous monitoring. Such approaches recognize that cybersecurity resilience depends not only on technology but also on organizational culture, leadership commitment, and workforce preparedness.

### **Artificial Intelligence in Modern Cyber Defense**

Artificial Intelligence has significantly transformed cybersecurity operations by enabling automated threat detection, anomaly identification, behavioral analysis, malware classification, and rapid incident response. Machine learning algorithms can process vast quantities of security telemetry far more efficiently than traditional rule-based systems, allowing organizations to identify emerging threats in real time.

However, AI introduces new security challenges. Adversaries increasingly employ AI to automate phishing campaigns, evade detection mechanisms, generate malicious code, and identify exploitable vulnerabilities. Consequently, AI functions as both a defensive capability and an offensive tool, creating an evolving cybersecurity arms race.

Researchers emphasize that effective AI governance requires transparency, explainability, human oversight, and responsible deployment to ensure trustworthy cybersecurity applications.

### **Zero Trust Architecture**

Zero Trust Architecture (ZTA) has emerged as one of the most influential cybersecurity frameworks adopted by governments and private organizations. Unlike traditional perimeterbased security models, Zero Trust assumes that no user, device, or application should be inherently trusted, regardless of its location within the network.

Core Zero Trust principles include continuous authentication, least-privilege access, microsegmentation, identity verification, and continuous monitoring. These principles reduce opportunities for lateral movement after an attacker compromises initial access.

The U.S. federal government's adoption of Zero Trust reflects recognition that identitycentric security is essential for defending increasingly distributed computing environments characterized by cloud services, remote work, and hybrid infrastructures.

### **Security Awareness as a Critical Security Control**

Numerous cybersecurity incidents begin with successful phishing attacks or other forms of social engineering targeting employees. Consequently, security awareness programs have become a fundamental component of organizational cybersecurity strategies.

Effective awareness initiatives extend beyond annual compliance training. Contemporary programs emphasize continuous education, phishing simulations, executive engagement, role-specific training, and measurement of behavioral outcomes. Organizations that foster strong security cultures generally demonstrate improved resilience against human-focused cyber threats.

Security awareness is particularly effective when integrated with technical safeguards such as multifactor authentication, endpoint detection, identity management, and Zero Trust controls. This integrated approach recognizes that human vigilance complements technological defenses rather than replacing them.

### **Integrating AI, Zero Trust, and Human-Centered Security**

Although AI, Zero Trust, and security awareness have each received considerable attention individually, relatively few studies examine how these approaches can be integrated into a unified cybersecurity strategy. Emerging research suggests that cybersecurity resilience is strongest when organizations simultaneously invest in advanced detection technologies, identity-based access controls, and workforce education.

Artificial Intelligence enhances visibility and automates threat detection. Zero Trust reduces the likelihood that compromised credentials will result in widespread system compromise. Security awareness decreases the probability of successful phishing, credential theft, and insider incidents by strengthening employee preparedness. Together, these complementary capabilities create multiple layers of defense that improve organizational resilience against evolving cyber threats.

This integrated, human-centered perspective forms the conceptual foundation of this study and supports the argument that cybersecurity resilience requires balanced investment in technology, governance, and people.

## **Methodology**

### **Research Design**

This study employs a qualitative, literature-based research design to examine how Artificial Intelligence (AI), Zero Trust Architecture (ZTA), and cybersecurity awareness programs can be integrated into a human-centered cybersecurity framework for U.S. institutions. Rather than conducting primary data collection through surveys or experiments, the research synthesizes existing academic literature, government publications, industry reports, and cybersecurity frameworks to identify best practices, emerging trends, and implementation challenges.

A qualitative approach is appropriate because the study seeks to evaluate relationships among technological, organizational, and human factors influencing cybersecurity resilience. The methodology emphasizes analytical interpretation of existing knowledge to develop practical recommendations for organizations responsible for protecting critical infrastructure and sensitive information.

### **Data Sources**

- The analysis draws upon multiple categories of authoritative sources to ensure a balanced and comprehensive perspective:
- Peer-reviewed cybersecurity journals and conference publications.
- U.S. government cybersecurity guidance, including publications from the National Institute of Standards and Technology (NIST), the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Office of Management and Budget (OMB).
- Industry reports published by leading cybersecurity organizations.
- Existing literature on Artificial Intelligence, Zero Trust Architecture, insider threats, ransomware, cloud security, and cybersecurity awareness.
- The author's previously published cybersecurity research where directly relevant to the topics under discussion.

## **Analytical Framework**

### **Technological Dimension**

The technological dimension examines how organizations deploy cybersecurity technologies to prevent, detect, contain, and recover from cyber threats. Modern cybersecurity increasingly relies on integrated technologies capable of collecting security information, identifying abnormal behavior, enforcing access controls, and responding to threats in real time.

Key components include AI-powered threat detection, security information and event management (SIEM), endpoint detection and response (EDR), behavioral analytics, identity and access management (IAM), automated incident response, network monitoring, vulnerability management, and Zero Trust controls.

AI-enabled security technologies can analyze large volumes of security events and identify patterns that may be difficult to detect through manual monitoring. Behavioral analytics can establish baselines for normal user and system activity and identify deviations that may indicate compromised accounts, insider threats, or malicious activity.

Identity and access management provides another important layer by ensuring that users and devices receive appropriate access to organizational resources. Zero Trust extends this approach by emphasizing continuous assessment, least-privilege access, and risk-based policy enforcement. CISA's Zero Trust Maturity Model describes increasingly advanced approaches involving automated controls, centralized identity and policy enforcement, riskbased changes to least privilege, and continuous monitoring.

The technological dimension can therefore be evaluated through indicators such as:

| Area                 | Example indicators                                                      |
|----------------------|-------------------------------------------------------------------------|
| AI threat detection  | Automated detection, anomaly detection, threat classification           |
| SIEM                 | Log collection, event correlation, alert generation                     |
| EDR                  | Endpoint visibility, suspicious activity detection, response capability |
| Behavioral analytics | User/entity behavior monitoring, anomaly identification                 |
| IAM                  | Authentication, authorization, access reviews                           |
| Zero Trust           | Least privilege, continuous verification, risk-based access             |
| Automation           | Automated alerts, containment, remediation                              |
| Monitoring           | Network, endpoint, identity, and cloud monitoring                       |

### Human Dimension

The human dimension recognizes that cybersecurity resilience depends not only on technical controls but also on the people who use, manage, and govern information systems.

Employees interact with organizational systems every day and can either strengthen or weaken security. Human-related risks can include phishing susceptibility, weak password practices, inappropriate data handling, social engineering, accidental disclosure, and misuse of legitimate access.

Consequently, organizations should develop continuous cybersecurity awareness and education programs that teach employees how to identify threats, follow security policies, report suspicious activity, and respond appropriately to cybersecurity incidents.

NIST research specifically examines federal cybersecurity awareness programs and identifies training, awareness, usability, and the competencies of security-awareness personnel as important areas of organizational cybersecurity.

The human dimension should also consider organizational culture and leadership commitment. Security awareness is more effective when leadership establishes cybersecurity as an organizational responsibility rather than treating it solely as an IT function.

This dimension can therefore be evaluated using indicators such as:

| Area               | Example indicators                             |
|--------------------|------------------------------------------------|
| Security awareness | Training frequency and participation           |
| Employee behavior  | Phishing awareness, reporting behavior         |
| Insider threat     | Access monitoring, behavioral indicators       |
| Security culture   | Employee security practices and attitudes      |
| Leadership         | Executive support and cybersecurity investment |
| Education          | Continuous training and skills development     |
| Incident reporting | Speed and frequency of employee reporting      |
| Human error        | Policy violations and preventable incidents    |

### **Governance Dimension**

The governance dimension addresses the policies, leadership structures, risk-management processes, regulatory requirements, and strategic decisions that determine how cybersecurity is managed throughout an organization. Governance establishes who is responsible for cybersecurity, what risks are acceptable, how security investments are prioritized, and how technological and human controls are integrated into organizational operations.

This dimension includes:

- Cybersecurity policies and standards
- Risk assessment and risk management
- Regulatory and legal compliance
- Security leadership and accountability
- Incident-response policies
- Third-party and supply-chain risk management
- Data protection policies
- Security architecture standards
- Cybersecurity performance measurement
- Strategic cybersecurity planning

This is particularly consistent with NIST CSF 2.0, which added Govern as a sixth core function. NIST explains that the Govern function establishes and monitors the organization's cybersecurity risk-management strategy, expectations, and policy.

| Area              | Example indicators                                      |
|-------------------|---------------------------------------------------------|
| Policies          | Existence and effectiveness of cybersecurity policies   |
| Risk management   | Risk assessments and risk registers                     |
| Compliance        | Regulatory and standards compliance                     |
| Leadership        | Executive accountability and oversight                  |
| Strategy          | Alignment between cybersecurity and business objectives |
| Incident response | Documented response and recovery procedures             |
| Third-party risk  | Vendor/security assessments                             |
| Performance       | Cybersecurity metrics and KPIs                          |
| Investment        | Allocation of resources to cybersecurity                |

### **How the Three Dimensions Interact**

The three dimensions should not be presented as independent categories. They are interdependent components of cybersecurity resilience.

For example: Technology without trained employees can fail because users may ignore security warnings or mishandle credentials.

Trained employees without technology may recognize threats but lack the technical controls necessary to prevent or contain attacks.

Technology and trained employees without governance may result in inconsistent security practices because there are no clearly defined policies, responsibilities, risk thresholds, or accountability mechanisms.

Therefore:

| Technological Capability                                      | Human Capability                                            | Governance Capability                           |
|---------------------------------------------------------------|-------------------------------------------------------------|-------------------------------------------------|
| AI & AutomationEndpoint Security (EDR)SIEM & Threat Detection | Training & AwarenessBehavioral AnalyticsPhishing Resilience | Security PoliciesRisk ManagementAccess Controls |

### Cybersecurity Resilience

The three capabilities-Technological Capability, Human Capability, and Governance Capability, together to strengthen Cybersecurity Resilience.

### Scope of the Study

This research focuses primarily on cybersecurity within United States institutions, including federal agencies, healthcare organizations, financial institutions, educational institutions, and operators of critical infrastructure. These sectors are particularly important because they manage sensitive information, provide essential services, and increasingly depend on interconnected digital systems.

The study examines cybersecurity resilience from a technological, human, and governance perspective. From the technological perspective, the research considers cybersecurity technologies and architectures such as artificial intelligence (AI)-enabled threat detection, security analytics, behavioral analysis, endpoint detection and response (EDR), security information and event management (SIEM), identity and access management (IAM), cloud security, continuous monitoring, and Zero Trust architecture.

From the human perspective, the research considers cybersecurity awareness, employee behavior, social engineering risks, insider threats, security training, organizational culture, and leadership commitment. This human-centered focus recognizes that employees and other authorized users interact continuously with organizational information systems and can influence an organization's ability to prevent, detect, and respond to cyber incidents.

The governance component examines cybersecurity policies, risk-management practices, regulatory and compliance requirements, organizational accountability, security standards, and strategic decision-making. Particular attention is given to how organizations can align technological security measures and human-centered practices with established cybersecurity frameworks and national cybersecurity priorities.

The research considers a range of cyber threats, including ransomware, phishing, credential compromise, insider threats, malware, data breaches, unauthorized access, social engineering, and emerging AI-enabled attacks. The analysis recognizes that modern cyberattacks frequently exploit the interaction between technical vulnerabilities and human behavior rather than relying exclusively on weaknesses in technology.

The study also considers the increasing use of artificial intelligence in both cyber defense and cyberattacks. AI can support threat detection, behavioral analysis, security automation, and incident response, while simultaneously creating new challenges involving adversarial attacks, automated exploitation, privacy, reliability, and governance. This dual-use nature of AI makes responsible implementation and appropriate oversight an important component of cybersecurity resilience.

The research is primarily concerned with the United States cybersecurity environment, including federal cybersecurity policies, national cybersecurity strategies, and frameworks developed or adopted by U.S. government organizations. Relevant frameworks and guidance from organizations such as the National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and other U.S. government entities are considered where applicable.

Although examples from international cybersecurity practices and standards may be referenced where they provide useful comparative perspectives, the central analysis remains focused on cybersecurity policies, frameworks, technologies, organizational practices, and challenges that are most relevant to institutions operating within the United States.

The study does not attempt to provide an exhaustive technical analysis of every cybersecurity technology or every type of cyber threat. Instead, it focuses on the integration of technological capabilities, human factors, and governance mechanisms as interconnected elements of organizational cyber resilience.

### **Limitations**

Several limitations should be acknowledged in interpreting the findings of this study. First, the research relies primarily on secondary sources, including peer-reviewed academic literature, government publications, cybersecurity frameworks, industry reports, and publicly available research. Consequently, the study does not include original empirical data collected through surveys, interviews, experiments, or longitudinal observations. The findings should therefore be interpreted as a synthesis and analysis of existing evidence rather than as the results of a controlled empirical investigation.

Second, the rapidly evolving nature of cybersecurity presents a temporal limitation. Cyber threats, attack techniques, artificial intelligence capabilities, security technologies, and defensive strategies continue to develop rapidly. Consequently, technologies and threat patterns discussed in this study may evolve after publication. This limitation is particularly relevant to AI-enabled cybersecurity, where both defensive applications and adversarial uses of AI are developing quickly.

Third, differences among organizations may affect the applicability of the recommendations. Organizations vary considerably in size, financial resources, technical capabilities, workforce expertise, infrastructure, risk tolerance, and regulatory obligations. A cybersecurity strategy that is practical for a large federal agency or financial institution may not be equally feasible for a small educational institution, healthcare organization, or other resource-constrained organization.

Fourth, the effectiveness of cybersecurity controls may depend on organizational implementation rather than technology alone. The presence of AI-powered security tools, Zero Trust Architecture, or other technical controls does not automatically guarantee improved cybersecurity resilience. Their effectiveness may depend on appropriate configuration, integration, employee adoption, continuous monitoring, governance, and organizational leadership.

Fifth, the study does not attempt to evaluate every cybersecurity technology, threat category, or regulatory framework. The analysis concentrates primarily on the relationship between AI-enabled cybersecurity, Zero Trust Architecture, human-centered security practices, and organizational governance. Other technologies and approaches may provide additional benefits but fall outside the primary scope of this research.

Finally, reliance on publicly available information may introduce limitations in assessing the actual effectiveness of organizational cybersecurity programs. Organizations may not publicly disclose cybersecurity incidents, internal security weaknesses, security architecture, or the outcomes of particular security investments. Therefore, publicly available evidence may not fully represent the cybersecurity conditions of individual organizations.

Despite these limitations, the study provides a comprehensive synthesis of existing research, government guidance, cybersecurity frameworks, and industry knowledge. By examining cybersecurity resilience through technological, human, and governance dimensions, the study provides an integrated perspective on how organizations can strengthen their ability to prevent, detect, respond to, and recover from cyber threats. In particular, the integration of AI-enabled security technologies, Zero Trust Architecture, continuous monitoring, cybersecurity awareness, and human-centered security practices provides a practical framework for addressing both technical and human sources of cyber risk.

The study therefore provides a foundation for future empirical research, including quantitative studies, organizational surveys, interviews with cybersecurity professionals, controlled experiments, and longitudinal evaluations of AI and Zero Trust implementations. Such research could further validate the relationships identified in this study and determine how cybersecurity resilience strategies perform across different organizational environments.

### **Results and Discussion**

The analysis indicates that organizational cybersecurity resilience is strongest when technological controls, human-centered security practices, and governance mechanisms operate as an integrated system. The reviewed literature and cybersecurity frameworks suggest that AI can improve the speed and scale of threat detection, Zero Trust can reduce opportunities for unauthorized access and lateral movement, and security awareness can reduce human-related risks. However, none of these components is sufficient in isolation. Their effectiveness depends on appropriate governance, continuous monitoring, skilled personnel, and organizational commitment.

### **Artificial Intelligence as a Force Multiplier in Cyber Defense**

Artificial Intelligence (AI) has increasingly become a force multiplier in modern cyber defense because it enables organizations to analyze security information at a scale and speed that would be difficult to achieve through manual analysis alone. Machine learning and related AI techniques can process network traffic, endpoint activity, authentication events, system logs, and user behavior to identify patterns and anomalies that may indicate malicious activity.

Within Security Operations Centers (SOCs), AI can assist analysts by correlating security events, prioritizing alerts, identifying anomalous behavior, and automating repetitive investigative tasks. This can help security teams concentrate their limited human resources on incidents requiring contextual judgment and more complex investigation.

AI can also strengthen threat intelligence by correlating information from multiple sources. For example, indicators associated with suspicious IP addresses, domains, user accounts, endpoint activity, and known attack techniques can be analyzed together to identify relationships that might otherwise remain isolated. AI-supported security platforms can consequently contribute to faster detection and potentially reduce the time between initial compromise and organizational response.

However, the analysis also indicates that AI should be considered a force multiplier rather than a replacement for cybersecurity professionals. AI systems depend on the quality, relevance, and representativeness of the data used to train and operate them. Poor-quality data, inappropriate model configurations, changing attack patterns, and inadequate validation can produce false positives or false negatives.

Another important concern is the adversarial use of AI. The same technologies that can support defensive cybersecurity operations can potentially be used by threat actors to improve social engineering, automate malicious activity, identify vulnerabilities, or adapt attacks more quickly. This creates an ongoing technological competition between defenders and attackers.

Consequently, organizations should implement AI security capabilities within a broader governance framework that includes human oversight, model evaluation, access controls, data protection, continuous monitoring, and periodic reassessment. NIST's AI Risk Management Framework provides a useful foundation for managing risks associated with AI systems while promoting trustworthy and responsible deployment.

The key finding is therefore not that AI independently solves cybersecurity problems, but that properly governed AI can expand the analytical capacity, speed, and scalability of cybersecurity teams.

### **Zero Trust Architecture Strengthens Organizational Resilience**

The analysis further indicates that Zero Trust Architecture (ZTA) provides an important complementary layer of organizational defense. Traditional perimeter-based security models were largely designed around the assumption that systems and users inside an organizational network could be trusted. The expansion of cloud computing, remote work, mobile devices, third-party services, and distributed applications has made this assumption increasingly difficult to maintain.

Zero Trust replaces implicit trust with a model in which access is continuously evaluated according to factors such as identity, device security, resource sensitivity, behavioral context, and organizational policy.

A central principle of Zero Trust is least-privilege access. Users and systems should receive only the permissions necessary to perform authorized tasks. This reduces the potential consequences of compromised credentials because an attacker who obtains access to one account does not automatically gain unrestricted access to organizational resources.

Micro-segmentation provides another important mechanism. By separating networks, applications, workloads, or sensitive resources into controlled segments, organizations can limit an attacker's ability to move laterally following an initial compromise.

Zero Trust can therefore be particularly valuable when combined with AI-enabled monitoring. AI can identify unusual access behavior, while Zero Trust controls can restrict or require additional verification when that behavior presents an elevated risk.

For example:

| Security event                 | AI capability                              | Zero Trust response               |
|--------------------------------|--------------------------------------------|-----------------------------------|
| Unusual login location         | Detects anomalous behavior                 | Require additional verification   |
| Abnormal file access           | Identifies deviation from baseline         | Restrict access                   |
| Compromised credentials        | Detects suspicious authentication patterns | Revoke or limit session           |
| Unusual administrator activity | Behavioral analytics                       | Apply additional controls         |
| Suspicious device              | Identifies device-risk indicators          | Deny or limit access              |
| Lateral movement attempt       | Detects abnormal network behavior          | Segment or restrict communication |

However, Zero Trust implementation also presents challenges. Organizations may need to modernize legacy infrastructure, improve identity management, establish device management capabilities, integrate security telemetry, and develop appropriate policies. Implementation can therefore require significant technical and organizational investment.

The analysis suggests that the value of Zero Trust should not be measured simply by whether an organization has deployed a particular security product. Instead, effectiveness should be evaluated according to how consistently identity, device, application, network, and data controls are integrated into organizational risk management.

### Security Awareness Remains the First Line of Defense

The technological findings are complemented by the human dimension of cybersecurity. Even sophisticated security technologies cannot completely eliminate risks arising from human behavior. Employees interact with email, applications, cloud services, authentication systems, websites, and organizational data every day. Their decisions can therefore directly affect an organization's security posture.

Common human-related risks include:

- Phishing and social engineering
- Weak or reused passwords
- Improper handling of sensitive information
- Unauthorized software installation
- Unsafe use of removable media
- Failure to report suspicious activity
- Accidental disclosure of information
- Misuse of authorized privileges

For this reason, cybersecurity awareness should be treated as an ongoing organizational capability rather than a one-time compliance requirement.

Effective programs can combine:

| Awareness Practice            | Purpose                                        |
|-------------------------------|------------------------------------------------|
| Continuous security education | Reinforce secure behaviors                     |
| Phishing simulations          | Improve recognition of social engineering      |
| Role-based training           | Address risks specific to job responsibilities |
| Interactive workshops         | Encourage practical learning                   |
| Incident-reporting education  | Increase early reporting                       |
| Executive engagement          | Demonstrate organizational commitment          |
| Security assessments          | Measure changes in behavior                    |
| Regular communications        | Maintain awareness of emerging threats         |

The analysis suggests that organizations should also move away from viewing employees solely as a cybersecurity vulnerability. Employees can become an important human detection and response capability when they understand organizational risks and have simple mechanisms for reporting suspicious activity.

For example, an employee who recognizes a suspicious email and reports it quickly may enable the security team to investigate the message and prevent other employees from interacting with it. Human awareness can therefore complement automated detection technologies.

Leadership commitment is particularly important. Cybersecurity awareness programs are more likely to become embedded in organizational culture when senior leadership provides resources, communicates expectations, participates in security initiatives, and treats cybersecurity as an organizational responsibility rather than exclusively an IT responsibility.

### **A Human-Centered Cybersecurity Framework**

This study proposes a Human-Centered Cybersecurity Framework (HCCF) that integrates three complementary dimensions of cybersecurity: technology, governance, and people. The framework is designed to address a central limitation of technology-focused cybersecurity strategies: the assumption that increasingly sophisticated technical controls alone can provide sufficient protection against modern cyber threats.

In practice, organizational cybersecurity is influenced by the interaction of technological capabilities, organizational policies, and human behavior. A technically sophisticated security environment may still be vulnerable when employees lack adequate security awareness, when access privileges are poorly managed, or when organizational leadership does not establish effective cybersecurity policies and accountability mechanisms. Conversely, well-trained employees may be unable to adequately protect organizational systems when appropriate technical controls or governance mechanisms are absent.

The proposed HCCF therefore positions cyber resilience within U.S. institutions as its primary objective. The framework combines Artificial Intelligence (AI), Zero Trust Architecture (ZTA), cybersecurity awareness, and governance into an integrated security model in which each component reinforces the others.

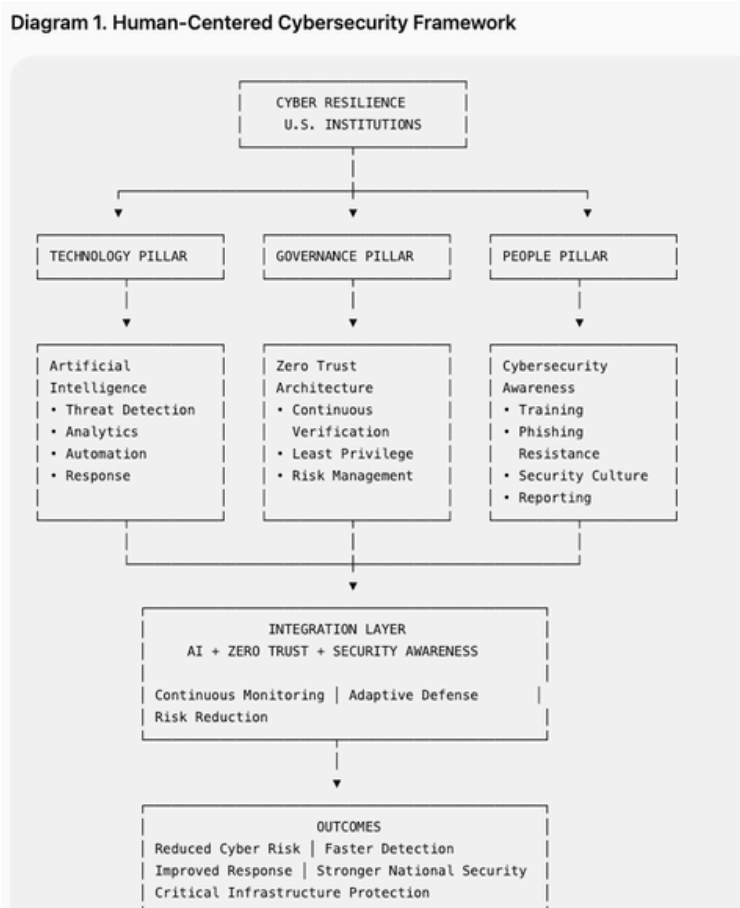


Diagram 1. Human-Centered Cybersecurity Framework: Integrating Artificial Intelligence, Zero Trust Architecture, and Cybersecurity Awareness

As illustrated in Diagram1, the proposed framework integrates three complementary cybersecurity pillars technology, governance, and people to strengthen cyber resilience within U.S. institutions. The Technology Pillar uses artificial intelligence to enhance threat detection, analytics, automation, and response. The Governance Pillar applies Zero Trust principles, including continuous verification, least-privilege access, and risk management. The People Pillar emphasizes cybersecurity awareness, training, phishing resistance, security culture, and incident reporting. The integration of these pillars creates a multilayered defense model designed to support continuous monitoring, adaptive defense, and risk reduction.

#### Technology Pillar

The Technology Pillar focuses on the use of advanced technological capabilities to identify, analyze, prevent, and respond to cyber threats. Artificial Intelligence serves as a central component because of its ability to process large volumes of security data, identify abnormal behavior, prioritize threats, and support automated or semi-automated incident response.

| Component                                               | Key Capabilities                                                                       | Primary Security Function                                    |
|---------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------|
| <b>Artificial Intelligence (AI)</b>                     | AI-powered threat detection and response; anomaly detection; predictive analytics      | Identifies and prioritizes emerging threats                  |
| <b>Security Analytics &amp; Behavioral Analysis</b>     | User and entity behavior analytics; anomaly detection; threat intelligence correlation | Detects unusual activities and potential compromises         |
| <b>Endpoint Detection and Response (EDR)</b>            | Endpoint monitoring; threat detection; automated containment; investigation            | Protects endpoints and responds to endpoint-based threats    |
| <b>Security Information and Event Management (SIEM)</b> | Log collection; event correlation; centralized monitoring; alerting                    | Provides centralized visibility across security environments |

|                                             |                                                                               |                                                  |
|---------------------------------------------|-------------------------------------------------------------------------------|--------------------------------------------------|
| <b>Automated Threat Response</b>            | Automated alert prioritization; containment; response workflows               | Accelerates response to detected threats         |
| <b>Identity and Access Management (IAM)</b> | Authentication; authorization; identity lifecycle management; access controls | Controls access to systems and resources         |
| <b>Continuous Security Monitoring</b>       | Network, endpoint, application, and cloud monitoring                          | Provides ongoing visibility into security events |
| <b>Endpoint and Network Protection</b>      | Endpoint security; network monitoring; intrusion prevention; segmentation     | Prevents and limits unauthorized activity        |

The objective is not to replace cybersecurity professionals with AI but to provide security teams with capabilities that improve speed, visibility, and decision-making. This approach builds upon the growing role of AI in cyber defense while recognizing the need for human oversight and responsible governance.

### Governance Pillar

The Governance Pillar establishes the policies, controls, and organizational processes necessary to manage cybersecurity risk. Zero Trust Architecture serves as the principal security model within this pillar.

Zero Trust operates on the principle that access should not be automatically trusted based solely on a user's location or previous authentication. Instead, access decisions should incorporate continuous verification, least-privilege principles, device and identity security, and ongoing risk assessment.

| Component                                          | Key Capabilities                                                        | Primary Security Function                              |
|----------------------------------------------------|-------------------------------------------------------------------------|--------------------------------------------------------|
| <b>Zero Trust Architecture (ZTA)</b>               | Continuous verification; least privilege; explicit trust decisions      | Prevents implicit trust and limits unauthorized access |
| <b>Continuous Identity and Access Verification</b> | Identity validation; device verification; contextual access decisions   | Ensures access remains appropriate over time           |
| <b>Least-Privilege Access</b>                      | Minimum necessary permissions; role-based access                        | Limits damage from compromised accounts                |
| <b>Risk-Based Access Decisions</b>                 | User, device, location, behavior, and threat-risk evaluation            | Adjusts access according to security risk              |
| <b>Cybersecurity Policies and Standards</b>        | Security policies; procedures; technical standards                      | Establishes organizational security requirements       |
| <b>Risk Management Processes</b>                   | Risk identification; assessment; mitigation; monitoring                 | Reduces and manages organizational cyber risk          |
| <b>Regulatory Compliance</b>                       | Applicable laws, regulations, and cybersecurity requirements            | Supports legal and regulatory obligations              |
| <b>Executive Oversight and Strategic Planning</b>  | Leadership accountability; cybersecurity investment; strategic planning | Aligns cybersecurity with organizational objectives    |
| <b>Continuous Governance and Monitoring</b>        | Policy review; control assessment; security metrics                     | Ensures security controls remain effective             |

The governance pillar ensures that technological capabilities are deployed within a structured security environment. AI may identify suspicious behavior, for example, but governance policies determine how access should be restricted, how incidents should be escalated, and who is responsible for responding.

### People Pillar

The People Pillar recognizes employees, administrators, security professionals, and organizational leadership as essential components of cybersecurity defense. Even highly advanced technical controls can be undermined when individuals are unaware of security risks or fail to follow established security practices.

The People Pillar therefore emphasizes continuous cybersecurity awareness and the development of a strong organizational security culture. Key components include:

| Component                                          | Key Capabilities                                                                    | Primary Security Function                               |
|----------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------|
| <b>Continuous Cybersecurity Awareness Training</b> | Ongoing security education; threat awareness; safe computing practices              | Improves employee cybersecurity knowledge               |
| <b>Phishing Awareness and Resistance</b>           | Phishing education; simulations; recognition and reporting                          | Reduces susceptibility to social engineering            |
| <b>Insider-Threat Awareness and Mitigation</b>     | Recognition of insider-risk indicators; reporting mechanisms; behavioral safeguards | Reduces malicious and unintentional insider risk        |
| <b>Security-Conscious Organizational Culture</b>   | Leadership involvement; shared responsibility; security-minded behavior             | Makes cybersecurity part of organizational culture      |
| <b>Role-Specific Cybersecurity Education</b>       | Training tailored to employees, administrators, executives, and security teams      | Addresses security risks specific to different roles    |
| <b>Incident Reporting and Communication</b>        | Reporting procedures; escalation; communication channels                            | Enables faster identification and response to incidents |
| <b>Security Behavior Development</b>               | Secure password practices; access protection; responsible data handling             | Converts security knowledge into everyday behavior      |

Rather than treating employees solely as potential security vulnerabilities, the framework considers them an important defensive capability. Well-trained employees can recognize suspicious activity, report potential incidents, protect credentials, and support organizational security policies.

### Integration of the Three Pillars

The principal contribution of the framework is not the individual pillars themselves but their integration. AI provides advanced detection and analytical capabilities; Zero Trust establishes adaptive access and governance controls; and cybersecurity awareness strengthens the human component of defense.

When these capabilities operate together, weaknesses in one layer can potentially be compensated for by protections in another. For example, if an employee's credentials are compromised through phishing, Zero Trust controls can limit unauthorized access, while AI-based behavioral analytics may identify anomalous activity associated with the compromised account. At the same time, effective security awareness training can increase the likelihood that the employee recognizes and reports the phishing attempt.

The integration of these three pillars therefore creates a multilayered and adaptive cybersecurity model designed to improve an organization's ability to prevent, detect, respond to, and recover from cyber threats.

Diagram 1 presents the proposed Human-Centered Cybersecurity Framework and illustrates how the Technology, Governance, and People pillars converge through an integration layer to support continuous monitoring, adaptive defense, risk reduction, and ultimately stronger cyber resilience for U.S. institutions.

Rather than operating independently, these pillars reinforce one another. AI provides visibility into emerging threats, Zero Trust limits attacker movement within networks, and informed employees reduce opportunities for attackers to gain initial access. Organizations implementing all three pillars simultaneously are better positioned to detect, prevent, respond to, and recover from cyber incidents.

### Policy Implications for U.S. Institutions

The increasing sophistication of cyber threats requires organizations to move beyond technology-only security strategies. Policymakers should encourage integrated cybersecurity approaches that recognize the interconnected roles of technology, governance, and human behavior.

Federal agencies should continue promoting Zero Trust implementation while supporting responsible AI adoption through clear governance standards. Public-private partnerships can facilitate information sharing, workforce development, and cybersecurity research that benefits both government and industry.

Educational institutions should expand cybersecurity education programs to address not only technical skills but also human-centered security practices. Similarly, organizations across critical infrastructure sectors should prioritize continuous workforce training as an essential component of national cybersecurity resilience.

By integrating AI capabilities, Zero Trust principles, and comprehensive security awareness programs, U.S. institutions can significantly strengthen their ability to defend against evolving cyber threats while supporting broader national security objectives.

## **Conclusion and Future Research Directions**

### **Conclusion**

The cybersecurity landscape facing U.S. institutions continues to evolve as organizations adopt increasingly complex digital technologies and adversaries develop more sophisticated attack methods. While technological advancements such as Artificial Intelligence and Zero Trust Architecture have significantly improved defensive capabilities, cybersecurity resilience cannot be achieved through technology alone. The human element remains a critical factor in determining whether organizations can successfully prevent, detect, and respond to cyber threats.

This study examined the importance of integrating Artificial Intelligence, Zero Trust Architecture, and cybersecurity awareness into a human-centered cybersecurity strategy. Artificial Intelligence enhances cybersecurity operations by improving threat detection, automating security processes, and enabling faster response to emerging attacks. Zero Trust Architecture strengthens organizational defenses by eliminating implicit trust, enforcing continuous verification, and reducing the potential impact of compromised identities. Cybersecurity awareness programs address the behavioral component of security by empowering employees to recognize threats and make informed security decisions.

The findings demonstrate that these capabilities should not be viewed as separate security initiatives. Instead, organizations should adopt an integrated approach where advanced technologies, governance frameworks, and human-centered practices work together to create multiple layers of defense. Such an approach is particularly important for U.S. institutions responsible for protecting critical infrastructure, sensitive data, and essential public services.

The proposed Human-Centered Cybersecurity Framework provides a strategic model for organizations seeking to improve cybersecurity resilience. By combining AI-driven defense mechanisms, Zero Trust security principles, and continuous workforce education, institutions can reduce cyber risk while developing a stronger security culture.

As cyber threats continue to evolve, cybersecurity strategies must also evolve beyond traditional technical defenses. The future of cybersecurity will depend on the ability of organizations to successfully combine technological innovation with human awareness, responsible governance, and proactive risk management.

### **Future Research Directions**

Future research should further examine how integrated cybersecurity approaches can be implemented and measured across different organizational environments. Several areas require additional investigation:

#### **1. Measuring the Effectiveness of Human-Centered Cybersecurity Programs**

Future studies should develop quantitative methods to evaluate how cybersecurity awareness programs influence employee behavior, phishing resistance, incident reporting, and overall organizational risk reduction.

#### **2. Improving Trustworthy Artificial Intelligence for Cyber Defense**

As organizations increasingly rely on AI-driven security solutions, additional research is needed to address challenges related to explainability, privacy, adversarial attacks against AI models, and human oversight of automated cybersecurity decisions.

#### **3. Integrating Zero Trust with Emerging Technologies**

Future research should explore how Zero Trust principles can be adapted for emerging environments, including cloud-native systems, Internet of Things (IoT) networks, operational technology (OT), and artificial intelligence infrastructure.

#### **4. Developing Cybersecurity Workforce Resilience**

The cybersecurity workforce shortage remains a significant challenge. Research should examine methods for improving cybersecurity education, professional development, and practical training programs to prepare future cybersecurity professionals.

## 5. Strengthening Public-Private Cybersecurity Collaboration

Because many critical infrastructure systems are operated by private organizations, future studies should explore improved collaboration models between government agencies, industry stakeholders, academic institutions, and cybersecurity researchers.

## Final Remarks

Cybersecurity is increasingly recognized as a critical component of national security, economic stability, public safety, and institutional resilience in the United States. As federal agencies, healthcare organizations, financial institutions, educational institutions, and critical infrastructure operators become increasingly dependent on interconnected digital technologies, the consequences of successful cyberattacks can extend beyond individual systems and affect essential services, sensitive information, and public trust.

The findings of this study demonstrate that cybersecurity resilience cannot be achieved through technological investment alone. Although advanced technologies such as Artificial Intelligence (AI), behavioral analytics, Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Zero Trust Architecture (ZTA) can significantly strengthen an organization's defensive capabilities, their effectiveness depends on how they are implemented, governed, and used by people.

The study therefore emphasizes the importance of integrating people, processes, technology, and governance into a unified cybersecurity strategy. AI can expand an organization's ability to identify and analyze threats at scale, while Zero Trust can limit unauthorized access and reduce opportunities for attackers to move through compromised environments. At the same time, cybersecurity awareness, continuous workforce education, leadership commitment, and security-conscious organizational culture can address risks associated with human behavior.

The proposed Human-Centered Cybersecurity Framework (HCCF) brings these elements together through three interconnected pillars: technological security, human-centered security, and governance. Rather than treating employees as merely a potential vulnerability, the framework recognizes them as active participants in organizational defense. Similarly, rather than treating AI and Zero Trust as standalone technologies, the framework places them within a broader governance structure that emphasizes continuous monitoring, risk management, accountability, and improvement.

A key implication of this research is that cybersecurity resilience should be viewed as a continuous organizational capability rather than a one-time technical implementation. Threats evolve, technologies change, and organizational environments continually introduce new risks. Organizations must therefore continuously evaluate their security controls, educate their workforce, reassess risks, and adapt their cybersecurity strategies. For U.S. institutions, this integrated approach is particularly important because cybersecurity vulnerabilities can have consequences extending beyond individual organizations. Weaknesses affecting critical infrastructure, healthcare systems, financial institutions, government agencies, and other essential services can create broader economic, operational, and national-security risks. Strengthening organizational cyber resilience therefore contributes to the broader objective of protecting the United States' increasingly interconnected digital environment.

Ultimately, this research concludes that AI innovation, Zero Trust Architecture, workforce preparedness, and effective governance should operate as complementary components of a human-centered cybersecurity strategy. The integration of these capabilities provides a more comprehensive approach to preventing, detecting, responding to, and recovering from cyber threats. The HCCF offers a conceptual foundation for organizations seeking to move beyond technology-centric security toward a more adaptive, resilient, and human-centered cybersecurity model.

Future research should empirically evaluate the proposed framework across different U.S. sectors and organizational environments. Surveys, interviews, case studies, controlled experiments, and longitudinal studies could be used to assess how the integration of AI, Zero Trust, workforce preparedness, and governance affects measurable cybersecurity outcomes. Such research could further refine the HCCF and contribute to the development of more effective strategies for strengthening cybersecurity resilience in the United States.

## References

- Sowe, Abdoulie, Cloud Security and Data Sovereignty: Balancing Efficiency with National Security Concerns: (November 20, 2024).
- Sowe, Abdoulie, The Evolution of Ransomware: Legal, Technical, and Policy Responses in the United States (June 04, 2025).
- Sowe, Abdoulie, Insider Threat Detection: Socio-Technical Approaches to Preventing Cyber Breaches in U.S. Institutions (December 12, 2025).
- Sowe, Abdoulie, Artificial Intelligence in Cyber Defense: Opportunities, Risks, and Governance Challenges for U.S. Critical Infrastructure (March 03, 2025).
- Sowe, Abdoulie, Zero-Trust Architecture in Federal Agencies: Effectiveness and Challenges of Implementation (May 24, 2024).
- Sowe, Abdoulie, The Role of Artificial Intelligence in Enhancing Cybersecurity: A Semi-Systematic Literature Review (June 05, 2024).
- National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce.
- Federal Bureau of Investigation Internet Crime Complaint Center. (2024). 2023 Internet Crime Report.
- Cybersecurity and Infrastructure Security Agency. (2023). Zero Trust Maturity Model (Version 2.0). U.S. Department of Homeland Security.
- National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce.
- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce.
- Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology.
- Cybersecurity and Infrastructure Security Agency. (2023). Zero Trust Maturity Model, Version 2.0.
- Haney, J., Jacobs, J., & Furman, S. (2022). Federal Cybersecurity Awareness Programs: A Mixed Methods Research Study. NISTIR 8420.
- Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework). NIST SP 800-181 Rev. 1.
- Rangarajan, A., et al. (2026). Advancing Human-Centered Cybersecurity: Challenges and Pathways Forward. IEEE Security & Privacy.