The Identity and Access Manager: A Social Science Perspective

Solen Grossman

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Diwakar Yalpi

11/16/2025

Bottom Line Up Front (BLUF):

This essay reflects that the Identity and Access Management (IAM) is a major area in cybersecurity that changes rapidly and cannot be solved only by technical measures but has to be complemented by fundamental social science principles. The argument, which is based on three significant scholarly articles, reveals that an efficient IAM system should be backed up by empirical data and implemented in an ethical manner so as to safeguard the CIA triad, lessen the digital disenfranchisement of vulnerable social groups, and 3) maintain its indispensable function of providing security to the sectors, which are, for instance, finance and healthcare.

Introduction

Cybersecurity is the prevention of damage to, protection of, and restoration of cyber technologies from computers, to communications, to the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (NIST, 2024). In the modern world, everything is highly digitized; according to a 2025 report, 15% of the world's economy happens online (Strukhoff, 2025). This means that cybersecurity is vital to protect our digital world and governments recognize that; the 2025 fiscal year budget for United States cybersecurity funding was $13 billion (Ribeiro, 2024). Within Cybersecurity, one of the most important disciplines is Identity and Access Management (IAM), a discipline tasked with ensuring only the right people can access the right resources at the right time for the right reason (Auth0). This makes an Identity and Access Manager a security gatekeeper primarily concerned with identity management, system access, and permission controls. They ensure unauthorized users cannot access sensitive data or make changes once they are inside systems (IMI, 2025). The role of an Identity and Access Manager is increasingly important in modern cybersecurity, with the market for IAM being expected to grow at around 13% with an estimated value of over $24 billion by the end of 2025 (IMI, 2025). While IAM is a technical discipline, it has an inherent connection to the social sciences. This paper will analyze this connection by examining how social science principles can be integrated into IAM, how social science insights can be used to develop IAM strategies and education, and how IAM connects with marginalization in cybersecurity.

Social science principles

Within the field of cybersecurity, human factors matter as much as technological factors. A 2024 survey showed that 68% of breaches were caused by human factors. and another survey involving over 1000 participants reported that 95% of cybersecurity issues have some human element (Jones, 2024). The study of human factors such as society and relations is social sciences, and like natural sciences, social sciences has the underpinning principles like empiricism (Relying on evidence), skepticism (Questioning assumptions), and ethical neutrality (Adherence to ethical standards). For cybersecurity, such principles order a specialist to rely on evidence on the context and nature of a given situation in cyberspace, question assumptions they may have about the information at hand, and parse through and utilize this information in an ethical manner.

Within the discipline of IAM, one may employ social science principles to their strategy. For example, an IAM specialist can utilize user based analytics, data-driven access reviews, and measurements for policy effectiveness to be empirical; they can be ethically neutral by consistent policy enforcement, unbiased monitoring and investigation, and balancing security and privacy; they can be healthily skeptical by challenging the 'default trust' model and employing a 'zero trust' model and scrutinizing third party integrations.

These strategic behaviors, in turn, will shape cybersecurity education and awareness. IAM professionals will be positioned to instruct users and peers on how to also be empirical by basing decisions on data and not feelings, being skeptical, and ethically neutrally by applying rules consistently and fairly in their cyberspace usage.

Application of Key Concepts

One key concept in cybersecurity is the CIA triad, which is confidentiality (Making sure user access is regulated), integrity (Making sure data remains accurate and reliable), and availability (Making sure data is accessible when it's needed). An IAM has a major role in upholding the CIA triad. They implement multi-factor authentication (MFA) to ensure confidentiality, implement Role-Based Access Controls (RBAC) to protect data integrity from unauthorized data alteration, and they design resilient access systems to prevent attacks like denial

of service to protect availability. They also need to discern which data is vital for confidentiality (Like customer personal identifiable information), integrity (Like their financial records), or availability (Like e-commerce platforms) in order to prioritize security investments. Compliance with legal standards also matters here, with regulations like HIPAA and GDPR legally mandating protections for data's confidentiality and integrity. Therefore MFA and RBAC are essential controls for demonstrating compliance within IAM.

As aforementioned, an IAM manager has to be proficient in upholding the principles of being empirical about matters, being ethically neutral in conduct, and having a healthy skepticism of system security, but they must also employ the principle of determinism, the belief that cyberattacks have identifiable causes and patterns. They can uphold the principle of determinism through understanding the MITRE ATT&CK framework, which is a curated knowledge base of adversary behaviors and attack patterns. MITRE ATT&CK has a released central repository for gathering and querying data as the source of truth (Greunke, 2022). For instance, an IAM manager can study techniques such as "Valid Accounts" (T1078) and "Account Manipulation" (T1098) to deterministically trace the steps an attacker would take after a breach. This will allow IAM managers to proactively mitigate risk by removing unnecessary and potentially abusable authentication and authorization mechanisms where possible or enforcing compliance by regularly auditing user accounts for activity and deactivating or removing any that are no longer needed (MITRE ATT&CK).

Marginalization

Within Cybersecurity and especially within the field of IAM, certain demographics face potential marginalization. For example, undocumented immigrants, day laborers, felons, and homeless individuals remain outside of the mainstream data flow and institutional attachments necessary to flourish in American Society which creates a surveillance gap that harms people with physical and mental injuries, economic instability, and data marginalization and invisibility to policymakers (Green & Gilman, n.d.; Stanford Law School et al., 2024). Furthermore, marginalized groups may be discriminatorily flagged as “high-risk” due to developers inputting historical data into AI algorithms that replicate pre-existing biases that the model is trained to believe are accurate.

(Stanford Law School et al., 2024). Marginalized communities based on age, income brackets, ethnicity/race, educational level, and especially geographical location also face economic barriers to even baseline digital services such as broadband access and adoption, meaning IAM systems that rely on smartphone apps for MFA or require large data downloads automatically exclusionary for these individuals (Sanders & Scanlon, 2021).

Within cybersecurity, whether through law or protocol, there has been great efforts to bridge the gaps. For example, California passed the Internet for All Act, a bipartisan law which allocates $330 million and extends the California Advances Services Fund (CASF) towards broadband deployment in marginalized areas by amending sections of the public utility code (Sanders & Scanlon, 2021). In May 2024, Colorado enacted the Artificial Intelligence Act which requires "developers" and "deployers" to use "reasonable care to avoid algorithmic discrimination in high-risk artificial intelligence systems." Californian lawmakers have advanced around 30 bills on AI to protect consumers and jobs (Stanford Law School et al., 2024). These policies may be used by IAM specialists to properly audit and make sure marginalized groups are actually being accounted for in access management and also that the AI used for data analysis does not overlook them.

Career Connection to Society

Cybersecurity professionals contribute to the safety and stability of financial systems, healthcare, and more. Without them, our entire world economy would suffer from an influx of natural and human threats. Of cybersecurity professionals, IAM managers play a key role in contributing to societal safety. IAM Managers help fortify security by meticulous control over user account and application access rights. They integrate robust authentication systems, regular updates to user rights, aligning access with digital identities, employ advanced mechanisms like MFA and strong password policies, and respond to security flaws through implementing immediate changes to access controls, updating authentication methods, and reinforcing security measures across the system (Team Zluri, 2025).

These policies benefit society on a profound level. For example, in the financial sector, the IAM discipline can make sure banks don’t face data breaches, account takeovers, and fraudulent transactions that may

undermine public trust in banking institutions which would destabilize economic systems. Within the healthcare sector, IAM controls can help protect patient safety by making sure only authorized personnel can access or modify sensitive health records, thus preventing medical errors and protecting privacy. IAM professionals implement these changes to access controls and reinforcement to security measures in order to maintain the integrity of the essential services that society depends upon.

Provide at least three scholarly sources that explore different aspects of the cybersecurity profession

Scholarly Articles on IAM

In their paper "A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity," Glöckler et al. outline the initial step of analyzing numerous requirements for IAM, eventually recognizing four major clusters - security and compliance, operability, technology, and user. These clusters signified the primary core IAM requirements for them. After reflecting on the said requirements, they discern the advantages that a self-sovereign identity (SSI) may offer - a model where the dependency on passwords is eliminated, and the end users are given cryptographic attestations that are stored in digital wallets in order to further identity management (Glöcker et al., 2023). This paper supports the field to have a thorough and research-oriented understanding of IAM and the key issues it faces, and also suggests an innovation that would help evolve the field.

The article “Identity and access management in cloud environment: Mechanisms and challenges” by Indu et al. discusses IAM and how complicated systems secure an organization, but potentially at the cost of structural access barriers (Indu et al., 2018). For example, MFA and strict credential management requires users to have a certain level of digital literacy or have a stable internet collection. This causes some demographics to be excluded from essential online services such as baking, government portals, and healthcare. Overall, the article’s discussion of technical difficulties with cloud security leads to the implication that they have a sociological dimension concerned with digital equity, privacy risk, and the risk of technological progress only deepening these social exclusions.

Ishaq Azhar Mohammed's article titled "Systematic Review Of Identity Access Management In Information Security" stresses that the IAM profession is not only about technical functions but is rather a business-wide discipline that changes the way risks are collaborated across all sectors. The paper further states that there is an urgent need for a plethora of IAM professionals conversant with roles in cloud security, compliance, and provisioning who will be the drivers to help organizations in complying with regulations, thus avoid the payment of fines for noncompliance. The analyzed review indicates how IAM specialists are tasked with the implementation of the security principle of "least privilege" through the definition of the user roles and permissions; this would be a level of security to be a shield against the access of information by both external and internal threats. Moreover, the role of IAM as one social issue interlinks with identity theft and fraud since IAM practitioners guarantee the security of a business as well as the individual's security by preventing fraudulent acts in the business (Mohammed, 2017). To summarize, this article demonstrates that IAM is fundamental in the core of cybersecurity and is a consistent concept across society.

Bibliography

Auth0. (n.d.). *Introduction to Identity and Access Management (IAM)*. Auth0 Docs. https://auth0.com/docs/get-started/identity-fundamentals/identity-and-access-management

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. *Business & Information Systems Engineering*, *66*. https://doi.org/10.1007/s12599-023-00830-x

Green, R., & Gilman, M. (n.d.). *The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization*. N.Y.U. Review of Law & Social Change. https://socialchangenyu.com/review/the-surveillance-gap-the-harms-of-extreme-privacy-and-data-marginalization/

Greunke, B. (2022, August 22). *Taking the Cyberworld by Storm: Developing with MITRE ATT&CK*. Meetascent.com. https://www.meetascent.com/resources/developing-with-mitre-1

How do you keep data secure and maintain compliance with all this complexity and a network perimeter that is expanding? Cisco Identity Services Engine (ISE). (2025, March). Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-identity-access-management.html

IBM. (2024, January 22). *Identity access management*. Ibm.com. https://www.ibm.com/think/topics/identity-access-management

IMI. (2025a, January 22). *IAM MARKET REPORT 2025 - Identity Management Institute®*. Identity Management Institute®. https://identitymanagementinstitute.org/iam-market-report-2025/

IMI. (2025b, February 28). *Identity and Access Management Career Guide - Identity Management Institute®*. Identity Management Institute®. https://identitymanagementinstitute.org/identity-and-access-management-iam-career-guide/

Indu, I., Anand, P. M. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering Science and Technology, an International Journal*, *21*(4), 574–588. Sciencedirect. https://doi.org/10.1016/j.jestch.2018.05.010

Jones, A. (2024, November 6). *Human Error Cybersecurity Statistics*. I.S. Partners. https://www.ispartnersllc.com/blog/human-error-cybersecurity-statistics/

Kosinski, M. (2024, June 19). *User behavior analytics*. Ibm.com. https://www.ibm.com/think/topics/user-behavior-analytics

MITRE ATT&CK. (n.d.). *Account Manipulation, Technique T1098 - Enterprise | MITRE ATT&CK®*. Attack.mitre.org. https://attack.mitre.org/techniques/T1098/

MITRE ATT&CK. (2017, May 31). *Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®*. Attack.mitre.org. https://attack.mitre.org/techniques/T1078/

Mohammed, I. A. (2017). SYSTEMATIC REVIEW OF IDENTITY ACCESS MANAGEMENT IN INFORMATION SECURITY. *International Journal of Innovations in Engineering Research and Technology*, *4*(7), 1–7. https://repo.ijiert.org/index.php/ijiert/article/view/2780

Ribeiro, A. (2024, March 14). *US Federal Budget for FY 2025 boosts cybersecurity investments amid escalating threats*. Industrial Cyber. https://industrialcyber.co/critical-infrastructure/us-federal-budget-for-fy-2025-boosts-cybersecurity-investments-amid-escalating-threats/

rwike77. (2023, October 23). *Introduction to identity - Microsoft Entra*. Learn.microsoft.com. https://learn.microsoft.com/en-us/entra/fundamentals/identity-fundamental-concepts

Sanders, C. K., & Scanlon, E. (2021). The digital divide is a human rights issue: Advancing social inclusion through social work advocacy. *Journal of Human Rights and Social Work*, *6*(2), 130–143. https://doi.org/10.1007/s41134-020-00147-9

Stanford Law School, Pham, H., Kohli, T., Llano, E. O., Nokuri, I., & Weinstock, A. (2024, June 29). *How will AI Impact Racial Disparities in Education?* Stanford Law School. https://law.stanford.edu/2024/06/29/how-will-ai-impact-racial-disparities-in-education/

Strukhoff, R. (2025). *Global Digital Economy Report - 2025 | IDCA*. Idc-A.org. https://www.idc-a.org/insights/qUi9XgvyrzSkyDUy9Tqr

Team Zluri. (2025, January 5). *7 Key Benefits of Identity and Access Management | Zluri*. Zluri.com. https://www.zluri.com/blog/identity-access-management-benefits#7-key-benefits-of-identity-and-access-management

Why Identity Access Management (IAM) Is So Important? (2017, August 11). Optimal IdM. https://optimalidm.com/resources/blog/importance-of-iam/