Reducing Human Errors That Influence Data Breaches

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 201S: Cybersecurity & Social Science, Professor Trinity Woodbury

February 12, 2025

Discussion Board Topic #2, Assignment Question:

Discussion Board Topic #3, Assignment Question:

Security breaches are common in organizations, and many of these breaches are caused by human errors. What are some ways to reduce human errors and improve security?

Summary

Poor human performance and human errors cause many data breaches. Stress, security fatigue, and burnout negatively impact employees' abilities to maximize cybersecurity (Nobles, 2022). Identity and Access Management (IAM) solutions help boost human performance, reduce human error, and improve security by ensuring that the right individuals have access to the right resources for the right reasons (Mohammed, 2013). The IAM process includes four key parts: Identification, Authentication, Authorization, and Accounting (Malik, 2024). The benefits of IAM include enhanced security, improved user experience, compliance and audit readiness, operational efficiency, and risk mitigation (Nieles, Dempsey, & Yan Pilli, 2017). IAM implements human-centered solutions like Password Management, Network Access Control systems, and Digital Identity Management policies to achieve its goals.

What is Identification, Authentication, Authorization, and Accounting? How do they help prevent human errors and improve organizational security?

First, Identification is when a user claims an identity utilizing one or more unique attribute(s) or qualifier(s) (e.g., username, email address). The goal is to ensure the information is legitimate and accurate on the front end for later use. For example, an organization may implement identity proofing before the creation of a user's account and conduct annual reviews or attestation events during the life of the account. The organization will require the user to submit personal details or formal identification documents like a driver's license, passport, or monthly household bills showing one's full name and address. In my own experience, I have had to provide many personal identification documents when taking on new employee roles to use specific systems and applications with the companies (e.g., ID.me account creation to gain access to VA mortgage records). Also, I have had regulatory agencies request upfront information when conducting background checks while in the process of becoming an executor of estates for various family members.

Second, Authentication is verifying the identity of the user, device, workstation, or system against a stored user database using passwords, biometrics, and multi-factor Authentication. Mult-factor Authentication (MFA) is a security mechanism requiring a user to provide independent categories of layered credentials to gain access to their accounts or confidential information at an organization. Examples of this include Password Managers (Ommeren, Borrett, Kuivenhoven, IBM, & Sogeti, 2014). Password Managers improve user experience and accessibility by streamlining the process of remembering an extensive list of credentials across many different accounts. The Password Manager requires the user to remember only one complex password to

gain entry to their private list of access credentials and passwords. The idea is that one complex password is much easier to remember than one hundred of them at a single time. Password managers also provide complex password generation, auto-filling login inputs, secure sharing, and cross-platform access between different devices and operating systems. From personal and work experience, these tools are instrumental in preventing me from saving sensitive data in an insecure location on my desktop, such as a Shared public folder, or writing down passwords on a notepad and leaving them in my locked desk drawer overnight.

Third, Authorization determines the permissions or access levels of authenticated users. The goal is for users only to access what is appropriate to their role in the organization. To achieve these security goals and reduce the risk of insider threats gaining unauthorized access to certain information, an organization will implement different access control models and segmentation. Role-Based Access Control (RBAC) assigns users to roles and assigns permissions to roles, mimicking the organization's hierarchy and following the principle of minimum or least privileges. For example, an IT Department may segment the Accounting and HR Departments from one another, creating separate group policies and accounts for those users to access different resources based on their unique needs and responsibilities to the organization. The IT department can also create a higher-level group called 'Employees' to allow each department to gain access to essential employee resources like Payroll, Intranet Wikis, and Department Contact Lists.

Fourth, Accounting or 'auditing' is when an organization keeps track and records of every user activity, including logins, actions, and changes. It helps detect security incidents, identify vulnerabilities, and provide evidence in case of breaches. IT Departments will use SIEM (Security Information and Event Management) tools like Splunk, Azure Sentinel, or ELK Stack for real-time monitoring. Log capture details may include user identity, timestamps, accessed resources, actions

performed, and sourced IP addresses. These recordings may seem reactive rather than proactive when trying to prevent human error; however, keeping tracking and keeping records of all network activity can help understand the causes of human error and modify existing security policies to prevent them in the future.

Personal Experience in Corporate America

In my prior role as a Loss Mitigation Underwriter for a few financial institutions, I had the authority to read, write, and modify many different documents within specific applications. For example, I didn't have access or authority to write/modify the original mathematical formulas to our Retention and Liquidation Excel calculator spreadsheets, but my direct managers had such access. Also, there was a time when my colleagues and I could edit our notes in some parts of MSP (Mortgage Service Platform) after we submitted them within the system. However, employees began abusing the editing privilege. Our management eventually denied the privilege to us because of legal and compliance concerns related to a few high-level cases where investors needed complete documentation integrity.

Conclusion

Data breaches are caused by many things involving human errors, usually from stress, security fatigue, and burnout, negatively impacting employees' abilities to maximize cybersecurity (Nobles, 2022). My Dad would always say: 'If you take care of your car and house, they'll take care of you; if you take care of your family and your employer, they'll take care of you, etc. ….'. My understanding of that is if I make your job and life easier, you'll eventually make my job and life easier. However, if I create obstacles and division for you and it makes your life more

difficult, then you'll reciprocate and do the same to me. In other words, don't make life harder for people already when it comes to cybersecurity, reducing human errors, and preventing catastrophic consequences to others. Instead, we should streamline processes by 'cutting off the fat,' educating people about cybersecurity, and conducting routine reviews to measure the effectiveness and success of current cybersecurity protocols and procedures.

References

Malik, F. (2024, September 4). *Identity and Access Management Implementation: 8-Step Plan*. Retrieved from Strongdm: https://www.strongdm.com/blog/identity-and-access-management-implementation

Mohammed, I. A. (2013). Intelligent authentication for identity and access management: a. *International Journal of Management, IT and Engineering*, 696-705.

Nieles, M., Dempsey, K., & Yan Pilli, V. (2017). An Introduction to Information Security. *Computer Security, NIST Special Publication 800-12 Revision 1*, 101.

Nobles, C. (2022, July 1). Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *Holistica Journal of Business and Public Administration*, pp. Vol. 13, Iss. 1, 49-72.

Ommeren, E. v., Borrett, M., Kuivenhoven, M., IBM, & Sogeti. (2014, April). *Staying Ahead in the Cyber Security Game: What Matters Now.* Creative Commons.