The Human Factor in Cybersecurity

Posted on January 10, 2025

Introduction

Cybersecurity is often described as a technical problem involving firewalls, encryption, malware, and network defense. Technology is essential, but many incidents begin or worsen through human decisions. Employees click links, reuse passwords, approve fraudulent requests, mishandle data, misconfigure systems, or delay reporting suspicious activity. Attackers deliberately exploit trust, urgency, authority, curiosity, and fear because manipulating a person can be easier than defeating a strong technical control. The human factor therefore includes users, administrators, developers, leaders, vendors, and the organizational conditions that shape their behavior. Effective cybersecurity should not assume that people can be trained into perfect compliance. It should combine usable technology, clear processes, realistic training, supportive reporting, and system design that limits the consequences of ordinary mistakes. (Haney, 2024)

Human Error and Cybersecurity

Human error can occur through action or omission. An employee may attach the wrong file, enter credentials into a fraudulent website, leave a device unlocked, or fail to install an update. An administrator may configure a cloud storage resource incorrectly or grant excessive privileges. A developer may expose a secret in source code. A manager may approve insecure practices because of schedule pressure.

These errors should not be treated as evidence that employees are careless by nature. Workload, interface design, ambiguous policy, time pressure, poor training, conflicting goals, and excessive security friction influence behavior.

A mature security program investigates why an unsafe action made sense in the user's context and redesigns the environment so that secure behavior becomes easier.

Social Engineering

Social engineering manipulates people into revealing information, transferring money, installing software, or granting access. Common forms include phishing, spear phishing, business email compromise, pretexting, impersonation, smishing, vishing, and physical tailgating.

Attackers often create urgency or authority. A message may appear to come from a senior executive

requesting immediate payment, an IT technician asking for a password, or a vendor changing bank details.

Training should teach employees to slow down high-risk requests, verify through an independent channel, and report suspicious communication quickly.

Phishing

Phishing uses fraudulent messages or websites to obtain credentials or deliver malware. Modern phishing can be highly personalized and may use information from social media, breached data, or public company websites.

Generative artificial intelligence can improve grammar and personalization, reducing some traditional warning signs. Employees should therefore rely on verification processes rather than simply looking for spelling errors.

Technical defenses such as email filtering, domain authentication, safe-link scanning, browser protection, and multi-factor authentication reduce dependence on user detection. (NIST, 2024)

Password Behavior

Weak, reused, or shared passwords create risk. Users may reuse credentials because they cannot remember many unique passwords or because organizational rules are burdensome.

Password managers can generate and store strong unique passwords. Organizations should avoid forcing frequent password changes without evidence of compromise because predictable changes may encourage weak patterns.

Multi-factor authentication provides additional protection, particularly when phishing-resistant methods are used.

Multi-Factor Authentication

Multi-factor authentication requires more than one type of evidence, such as something known, possessed, or inherent. It can prevent many account takeovers even when a password is stolen.

Not all factors offer equal security. SMS codes may be vulnerable to SIM-swap or interception, while push notifications can be abused through repeated prompts. Hardware security keys and passkeys can provide stronger phishing resistance.

Implementation should consider accessibility and recovery so that legitimate users are not locked out

or forced into insecure workarounds.

Insider Threats

Insider threats involve people with authorized access who cause harm intentionally or unintentionally. Malicious insiders may steal information, sabotage systems, or commit fraud. Negligent insiders may expose data through mistakes or unsafe practices.

Organizations should apply least privilege, separation of duties, logging, periodic access review, and prompt deprovisioning. Behavioral monitoring should be proportionate and respect privacy.

Insider programs should avoid treating unusual behavior as proof of wrongdoing. Investigation requires context and fair process.

Privilege and Access Control

Excessive access increases the consequence of compromise. Employees often accumulate permissions when roles change unless access is reviewed.

Least privilege grants only what is necessary for current duties. Privileged accounts should be separate from ordinary accounts and protected with stronger authentication.

Temporary access should expire automatically when possible.

Security Culture

Security culture refers to shared expectations about protecting information and reporting risk. A strong culture treats cybersecurity as part of ordinary work rather than a yearly training requirement.

Leaders influence culture by following the same rules expected of employees. If executives bypass controls for convenience, staff learn that security is optional.

Security teams should communicate respectfully. Users who fear embarrassment or punishment may hide mistakes until the damage becomes worse. (Haney et al., 2020)

Blame and Reporting

Employees should be encouraged to report accidental clicks, suspicious messages, lost devices, or mistaken disclosures immediately. Rapid reporting can allow security teams to revoke credentials or contain malware.

Automatic punishment for every error discourages disclosure. At the same time, deliberate or reckless violations require accountability.

A just approach distinguishes ordinary error from repeated disregard of security requirements.

Security Awareness Training

Training should be relevant to job roles and realistic threats. Employees need practical skills such as verifying payment changes, recognizing suspicious login prompts, handling sensitive documents, and reporting incidents.

Short repeated learning may be more effective than a long annual presentation. Scenarios should reflect the organization’s technology and work processes.

Training effectiveness should be measured through behavior and incident outcomes rather than completion rates alone.

Phishing Simulations

Simulated phishing can identify training needs and reinforce reporting. Poorly designed simulations can also damage trust, especially when they exploit sensitive topics or publicly shame employees.

The objective should be learning, not catching people. Results should be analyzed for system improvements, such as better filtering or clearer reporting controls.

Employees who report quickly should receive positive reinforcement.

Usability and Security

Security controls that are difficult to use encourage workarounds. Long authentication processes may lead staff to share sessions. Complex data-transfer procedures may encourage use of personal email or unapproved cloud storage.

Security teams should observe real workflows and reduce unnecessary friction. A secure process must be practical under normal workload and emergency conditions.

Usable security treats human behavior as a design requirement.

Remote and Hybrid Work

Remote work expands the environment in which employees handle organizational data. Home networks, shared spaces, personal devices, and public Wi-Fi may introduce risk.

Organizations should provide managed devices, secure remote access, encryption, automatic updates, and clear guidance for physical privacy.

Employees should know how to report lost devices or suspicious activity outside business hours.

Bring Your Own Device

Personal devices can improve convenience but create questions about patching, malware, data separation, and privacy. Bring-your-own-device programs should define supported devices, security requirements, remote wipe capability, and acceptable use.

Employees should understand what organizational administrators can access on a personal device before enrolling.

Where risk is high, organization-owned devices may be more appropriate.

Physical Security

Human factors also affect physical security. Tailgating, unattended badges, unlocked rooms, exposed documents, and unsecured devices can bypass digital protections.

Employees should challenge or report unusual access in a manner consistent with safety procedures. Visitor management and access controls should support rather than rely entirely on individual confrontation.

Sensitive material should be stored and destroyed securely.

Third Parties and Vendors

Contractors and vendors may have remote access, sensitive data, or privileged accounts. Their employees become part of the organization’s human attack surface.

Contracts should define security requirements, training, access, incident notification, and data handling. Vendor accounts should be reviewed and disabled when projects end.

Organizations should avoid assuming that a trusted business relationship automatically creates

secure technical access.

Leadership

Senior leaders determine whether cybersecurity receives resources and authority. They also decide how risk is balanced with productivity and business goals.

Leaders should receive role-specific training about ransomware, fraud, third-party risk, and incident response. Executives are often targeted because of their authority and access.

Cybersecurity metrics presented to leadership should connect technical findings with operational and financial consequences.

Incident Response and Human Roles

Incident response requires coordination among security, IT, legal, communications, leadership, operations, and affected departments. Plans should specify who can isolate systems, contact authorities, notify customers, and make recovery decisions.

Exercises help participants practice under pressure. Technical teams may know how to contain malware while leadership has never rehearsed whether operations should stop.

Post-incident reviews should examine both technical and organizational factors.

Ransomware

Ransomware often begins through stolen credentials, phishing, exploited vulnerabilities, or remote access. Employee awareness helps, but prevention requires layered controls.

Backups should be isolated and tested. Privileged access should be limited. Network segmentation can prevent one compromised account from reaching every system.

Organizations should plan for business continuity without assuming ransom payment will restore data or prevent disclosure.

Business Email Compromise

Business email compromise manipulates employees into changing payment information, sending funds, or releasing sensitive data. Attackers may impersonate executives or vendors and may observe real email threads before intervening.

Financial changes should require independent verification, especially new bank details or urgent transfers. Email alone should not be sufficient for high-risk transactions.

Strong processes protect employees from being placed in a situation where one convincing message can authorize a major loss.

Security Fatigue

Repeated warnings, passwords, prompts, and mandatory training can produce security fatigue. Users may begin clicking through alerts automatically.

Organizations should reduce low-value notifications and prioritize important actions. Security messages should explain why a control matters and what the user should do.

Automation can reduce the number of security decisions placed on employees.

Behavioral Metrics

Organizations may measure reporting rates, time to report, use of multi-factor authentication, completion of access reviews, and recurrence of risky behavior.

Metrics should not encourage underreporting. A low number of incidents may indicate strong security or poor visibility.

Measures should be interpreted alongside technical controls and organizational context.

Artificial Intelligence and Human Risk

Artificial intelligence can help attackers create convincing messages, voice impersonation, deepfake video, and automated reconnaissance. Employees need verification processes that do not depend solely on recognizing artificial content.

AI tools used by employees can also create data leakage when confidential information is entered into unapproved services. Organizations should define approved tools and handling rules.

Security teams can use AI for detection, but automated decisions should be validated and monitored.

Human-Centered Security Design

Human-centered security begins by understanding users' tasks, constraints, knowledge, and

incentives. Controls are designed so that the safe path is the easy path.

Examples include password managers, automatic encryption, simple reporting buttons, approved file-sharing tools, and clear access-request workflows.

When employees repeatedly bypass a control, the organization should investigate whether the process is poorly designed rather than only increasing training.

Policy Design

Policies should be concise, accessible, and connected to actual technology. Requirements that cannot be followed in practice create hidden noncompliance.

Employees need examples of acceptable and unacceptable behavior. Policies should identify who can answer questions and how exceptions are approved.

Regular review is necessary as technology and threats change.

Cybersecurity Education Beyond the Workplace

Cybersecurity habits develop across personal and professional life. Education about passwords, scams, privacy, and updates benefits employees and their families.

Organizations should avoid demanding access to personal accounts or excessive surveillance in the name of awareness. Training should respect boundaries.

Community education can also reduce fraud targeting older adults, students, and small businesses.

Conclusion

The human factor is central to cybersecurity because technology is designed, configured, operated, and supervised by people. Attackers exploit human trust and organizational processes as well as software vulnerabilities.

Effective security does not depend on eliminating all mistakes. It reduces opportunities for error, limits privileges, uses strong authentication, filters malicious content, and makes reporting easy.

Organizations need a supportive security culture, practical training, usable controls, and leadership accountability. When human behavior is treated as a design factor rather than a weakness to blame, cybersecurity becomes more resilient. (NIST, 2024)

References

Haney, J. M. (2024). Human-centered cybersecurity research and practice. *National Institute of Standards and Technology*.

Haney, J. M., Jacobs, J. L., Furman, S. M., & Barrientos, F. (2020). Toward a common ontology for human-centered cybersecurity. *National Institute of Standards and Technology*.

National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0*.