The psychological frontline

Mastering the human element in cyber defense

Sarah Gosler, Managing Director — Head of Cyber Human Defense

Executive summary

In the shadow war of modern cybersecurity, the human element has become the adversary's most potent weapon. These days, it’s more than just the brute-force attacks on steel and silicon; today's elite threat actors target the mind, employing social engineering, deepfakes, and psychological manipulation to breach even the most formidable digital fortresses.

Cyber Human Defense is not merely an upgrade; it is a paradigm shift — a strategic imperative for financial institutions where trust is currency and every employee is a potential, unwitting gateway. This white paper illuminates the modern threat landscape, dissecting the psychology of deception, revealing the true cost of human-driven breaches, and charting a course through proven frameworks. Through gripping, real-world case studies — from the social engineering that crippled a casino to the insider manipulation at a cryptocurrency exchange — we reveal a pattern of attacks that bypass technology to target human trust. We then provide the blueprint to defend against them.

Introduction

The new frontline: When the target is the mind

The doctrine of cyber warfare has fundamentally changed.

The enemy no longer exclusively targets the hardened perimeter of your digital infrastructure; they've found a softer, yet far more potent entry point: your people. This is the new battlefield, where trust is weaponized and the human mind becomes the ultimate exploit. Social engineering, sophisticated phishing campaigns, and the sinister rise of AI-driven deepfakes now bypass even the most advanced technical barriers, leveraging innate human behaviors and established trust networks.

The alarming reality: Why humans are the new frontier of attack

The modern enterprise, with its distributed workforce, pervasive digital connectivity, and the insidious creep of digital fatigue, has inadvertently expanded this human attack surface to unprecedented scales. To truly defend against this evolving threat, firms must embrace Cyber Human Defense — a strategic convergence of behavioral science, organizational culture, continuous education, and immersive simulation. This isn't just about training; it’s about transforming every individual into an active, conscious operative against threat actors.

95%

BREACHES INVOLVE A HUMAN ELEMENT[1]

98%

CYBERATTACKS INITIATE WITH SOCIAL ENGINEERING[2]

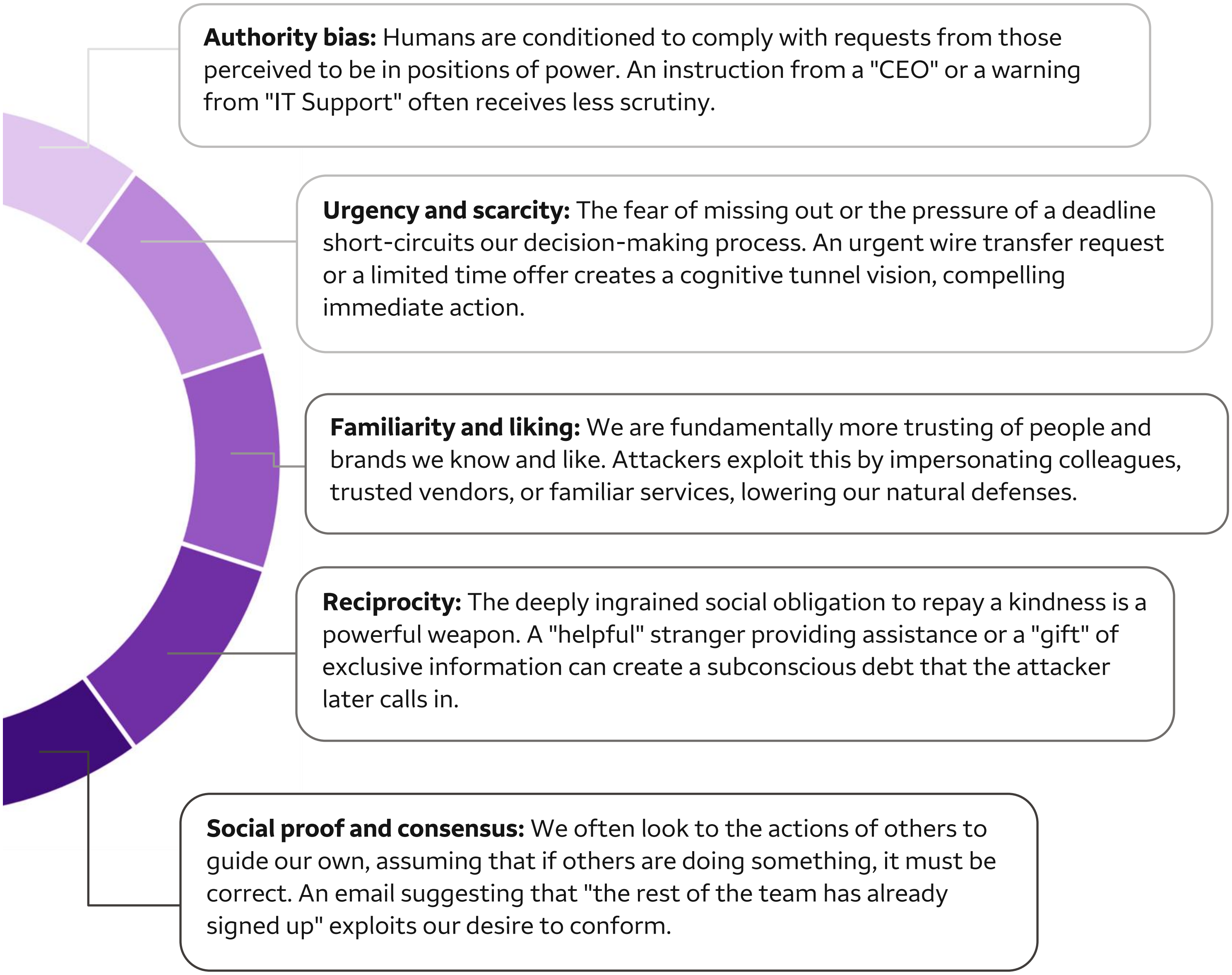
59%

EMPLOYEES ADMIT TO PASSWORD REUSE[3]

Chapter 2. The adversary's playbook

The levers of manipulation: Core psychological principles

Every effective social engineering attack is built upon a foundation of established psychological principles. The adversary knows which levers to pull to bypass rational thought and trigger an automatic, compliant response.



Authority bias: Humans are conditioned to comply with requests from those perceived to be in positions of power. An instruction from a "CEO" or a warning from "IT Support" often receives less scrutiny.

Urgency and scarcity: The fear of missing out or the pressure of a deadline short-circuits our decision-making process. An urgent wire transfer request or a limited time offer creates a cognitive tunnel vision, compelling immediate action.

Familiarity and liking: We are fundamentally more trusting of people and brands we know and like. Attackers exploit this by impersonating colleagues, trusted vendors, or familiar services, lowering our natural defenses.

Reciprocity: The deeply ingrained social obligation to repay a kindness is a powerful weapon. A "helpful" stranger providing assistance or a "gift" of exclusive information can create a subconscious debt that the attacker later calls in.

Social proof and consensus: We often look to the actions of others to guide our own, assuming that if others are doing something, it must be correct. An email suggesting that "the rest of the team has already signed up" exploits our desire to conform.

The adversary's toolkit is honed to exploit predictable human responses.

By dissecting these deceptive tactics, organizations can equip their workforce not just to recognize, but to actively counter, the adversary's psychological warfare — transforming every employee into an informed counter-intelligence agent.

The playbook in action: Key breach vectors

These cognitive biases are not theoretical; they are the specific vulnerabilities exploited by the following breach vectors. Understanding this linkage is the first step toward building an effective defense.

Business Email Compromise (BEC) and CEO Fraud: This vector is a masterclass in exploiting **authority bias**. By impersonating a high-level executive, often the CEO or CFO, attackers issue commands that employees are culturally and psychologically conditioned to follow.

The requests — typically for urgent wire transfers or sensitive data — are designed to create a powerful sense of **urgency**, compelling finance or HR personnel to bypass standard verification protocols. The attacker manufactures a crisis that only the target can solve, making them feel like a crucial part of a covert operation.

Spear phishing and whaling: Unlike generic phishing campaigns, spear phishing is a targeted intelligence operation. Attackers leverage open-source intelligence (such as LinkedIn and other social media) to craft highly personalized lures. Whaling is another type of phishing that targets high-profile individuals within an organization, such as executives, senior managers, or other decision-makers, with the goal of deceiving these individuals into revealing sensitive information, authorizing fraudulent transactions, or granting access to critical systems.

This approach weaponizes **familiarity** by using a target's name, job title, and professional connections to build instant credibility. These campaigns often dangle a tailored lure — such as a fake invoice from a known vendor or a document related to a real project — which plays on the principle of **reciprocity** by offering something of apparent value to trick the target into clicking.

Vishing (voice phishing) and AI-enabled impersonation: Vishing exploits the inherent trust and emotional connection of the human voice. It creates high-pressure scenarios using **urgency** and **scarcity** ("Your account will be suspended," "This investment opportunity closes in one hour").

The advent of real-time deepfake audio has elevated this threat to a new level. An attacker can now leverage **authority bias** and **familiarity** not just by claiming to be the CEO, but by speaking with the CEO's exact voice, turning a simple phone call into a devastatingly effective psychological weapon.

Smishing (SMS phishing): This vector leverages the immediacy and perceived intimacy of text messages. An urgent notification on a personal device feels more private and credible than an email.

Smishing attacks exploit **familiarity** by impersonating trusted services like banks, delivery companies, or internal IT departments. They create a false sense of **urgency** — "Your account has been compromised, click here to secure it" — knowing that the mobile interface encourages quick taps over careful analysis.

Insider threats (malicious and unintentional): The adversary's playbook is not limited to external attacks. They actively recruit or manipulate insiders, turning trusted employees into unwitting or willing accomplices. Malicious insiders are often cultivated by exploiting financial hardship or disaffection, creating a perverted sense of **reciprocity** where the employee feels a stronger loyalty to the external actor than to their employer.

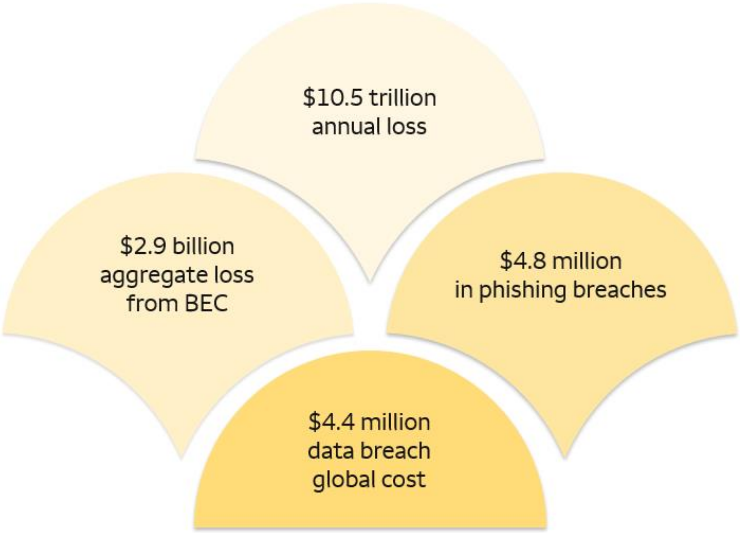
Unintentional insider threats are the result of successful external social engineering, where an employee is manipulated into using their legitimate credentials to provide the attacker with access, becoming a pawn in a much larger game.

Chapter 3. The hidden tax

Quantifying the toll of human cyber exploits

The financial fallout from human-centric cyber incidents is not just a line item; it's a silent bleed on the balance sheet, often dwarfing the cost of technical exploits. These are not merely IT problems; they are existential threats to reputation, trust, and ultimately, profitability across sectors, especially financial services. This isn't a single blow; it's a slow, debilitating poison.

The economic aftermath: A chilling calculus



- IBM stated in its 2025 report that the global cost of data breaches is $4.4 million[4]. This isn't just remediation; it's lost productivity, regulatory fines, legal fees, and the insidious erosion of customer confidence.

- Phishing-related breaches cost organizations an average of $4.8 million in 2024.[5]

- However, the true financial juggernaut of human exploitation lies in Business Email Compromise (BEC) schemes. The FBI's 2023 data reveal a staggering aggregate loss of $2.9 billion[6], where sophisticated impersonation tactics trick organizations into wiring funds directly to the adversary.

The horizon darkens further. Cybersecurity Ventures projects that by the end of 2025, the global economic impact of cybercrime will skyrocket to $10.5 trillion annually[7]. A massive portion of this unprecedented sum will be directly attributable to the exploitation of human weaknesses through manipulation and deception, underscoring that the most significant vulnerabilities are not found in code, but in cognition. These figures are not just statistics; they are a powerful appeal, demanding immediate and comprehensive investment in defenses that prioritize the human dimension of cybersecurity.

Chapter 4. Fortifying the human element: A strategic defense framework

Strategic pillars of cyber human defense

Now, the counter-operation begins…to forge a solid human defense, organizations must deploy a multifaceted arsenal, each strategy a critical pillar in transforming human vulnerability into a strong firewall. These aren't isolated initiatives; they are integrated components of a comprehensive counter-intelligence operation designed to empower every employee as an active guardian.

Security awareness training

The intelligence briefing

Beyond mere compliance, this is continuous intelligence for your workforce — foundational to inoculating employees against modern threats. Regular, targeted initiatives drastically reduce human error, which is the leading cause of breaches. Organizations with security awareness training saw a 70% drop in social engineering attacks.[8] This transforms staff from liabilities into active participants, empowered to spot the subtle tells of digital deception.

Cyber champions program

The covert operatives network

A true security culture goes beyond technology; it needs advocates at every level. Cyber Champions are embedded operatives — championing best practices, serving as key contacts, and acting as role models within their teams. Organizations with strong reporting cultures detect threats earlier, cutting breach detection time from the 197-day industry average to far less, saving millions in potential losses.[9] This grassroots approach fosters pervasive vigilance and shared responsibility across the enterprise.

Phishing and social engineering simulation

Live fire drills

These indispensable live fire drills test and sharpen your team's readiness. Mock phishing emails, vishing calls, and advanced social engineering scenarios measure real employee resilience. LinkedIn reported a mid-sized law firm hit by a phishing attack exposing client data. They responded with monthly simulations and tailored training. In six months, click rates dropped from 32% to 4%, proving ongoing education builds awareness and changes behavior.[10] These proactive exercises not only pinpoint vulnerabilities, but hardwire secure behaviors, making real-world attacks far less likely to succeed.

Cyber wargaming

Scenario-based counter-ops

Cyber wargames are high-fidelity, interactive simulations that thrust teams into realistic incident scenarios, forcing them to respond under extreme pressure. These sessions are crucible moments, exposing critical gaps in communication, escalation protocols, and technical response, driving relentless improvement. A 2022 Ponemon Institute study of 550 organizations in 17 countries found that nearly 75% have an incident response plan (IRP), and 63% regularly test it. These organizations saved an average of $2.66 million in breach costs — about 58% less than those without a tested IRP.[11] Beyond technical acumen, wargaming builds executive readiness, fosters seamless cross-functional collaboration, and fortifies organizational resilience at its core.

Behavioral engineering

The invisible hand of security

This pillar leverages deep insights from behavioral psychology to subtly guide users toward inherently secure actions. It's about designing secure defaults, implementing intelligent "nudges," and deploying timely prompts that make the secure path, the path of least resistance. A Sosafe report claimed that after high-quality training, the share of users able to spot phishing emails jumped from 11% to 64%.[12] By meticulously shaping habits and decision-making environments, behavioral engineering bridges the critical gap between mere awareness and decisive, secure action.

Each of these strategic pillars addresses a unique facet of the human element in cybersecurity. Woven together, they construct a comprehensive, dynamic defense that not only dramatically mitigates risk, but fundamentally strengthens organizational culture, resilience, and trust.

Chapter 5. Case studies

Unmasking the attacks — lessons from the front lines

Case study 1: A casino breach — the urgent voice of deception

In September 2023, a major casino suffered a debilitating cyberattack that brought its operations to a near standstill. This incident was not the result of a sophisticated malware deployment or a zero-day exploit, but rather a meticulously executed social engineering campaign that preyed on human trust and procedural weaknesses.

What happened

The attack began with a simple yet effective reconnaissance phase: a threat actor leveraged publicly available information on LinkedIn to identify a casino employee. Armed with details about this individual, the attacker then executed a classic "vishing" (voice phishing) attack. Within a mere 10 minutes, they contacted the casino's IT helpdesk, skillfully impersonating the identified employee. Through confident and urgent-sounding demands, the attacker successfully convinced the helpdesk staff to reset the employee's access credentials. This swift compromise granted the attackers an initial foothold into the casino's network. Once inside, the malicious actors moved rapidly, deploying ransomware across critical systems. The immediate consequences were severe and widespread, including the loss of access to essential services like hotel check-ins, slot machines, and various digital amenities. The attack resulted in an estimated $100 million in revenue impact, exposed sensitive customer data, and significantly damaged the casino's brand reputation.[13,14]

How humans were exploited

The casino's breach starkly highlighted the critical vulnerabilities within the human element of an organization's security posture:

- **Manipulation of helpdesk staff:** The attackers masterfully exploited the human tendency to be helpful and responsive, particularly when faced with what appeared to be an urgent request. Helpdesk staff, under pressure, were manipulated by the attacker's confident demeanor and urgent tone.

- **Deficient identity verification protocols:** The attackers exploited gaps in identity verification protocols to reset credentials by impersonating an employee, perhaps indicating that the verification process relied too heavily on verbal confirmation rather than multi-factor authentication or out-of-band verification.

- **Lack of empowerment and escalation paths:** Employees at the helpdesk level may not have felt empowered to question unusual requests or to escalate suspicions to a higher authority without fear of reprimand, contributing to the success of the social engineering attempt.

- **Absence of modern social engineering training:** The incident revealed a gap in specialized training, particularly concerning advanced social engineering tactics like deepfakes or highly convincing impersonation scenarios. Staff were unprepared for the speed and conviction with which the attacker operated.

The casino's actions post-incident

In the aftermath of the breach, the casino initiated a comprehensive overhaul of its cybersecurity and human-centric defense strategies:

1. **Conducting tabletop wargames:** To prepare all departments for various cyberattack scenarios, the casino implemented regular tabletop wargames. These simulations aimed to improve incident response coordination and decision-making across the organization.

2. **Deploying phishing and vishing simulations:** Recognizing the success of the social engineering attack, the casino significantly ramped up its phishing and vishing simulation exercises. These ongoing training programs were designed to inoculate employees against similar future attempts by teaching them to recognize and report suspicious communications.

3. **Launching an internal champions program:** The casino introduced an internal champions program spanning both hotel and IT operations. This initiative aimed to foster a culture of vigilance by empowering key employees to act as security advocates and first responders within their respective teams, ensuring security best practices were disseminated and maintained throughout the organization.

The breach chillingly exposes how confident social engineering and inadequate human protocols can unravel an enterprise in minutes, underscoring the critical need for rigorous identity verification and empowered, vigilant human gatekeepers.

Case study 2: An attack on a cryptocurrency exchange — a masterclass in human exploitation

In May 2025, a major cryptocurrency exchange suffered a significant data breach that primarily exploited human vulnerabilities through social engineering and bribery.

What happened

Instead of a direct technical breach of the cryptocurrency exchange's systems, threat actors targeted the company's human element by bribing or manipulating overseas customer support agents. These compromised insiders gained access to sensitive customer data including names, addresses, phone numbers, email addresses, partial Social Security numbers, masked bank account information, government-issued ID images, account balances, and transaction histories. Armed with this information, the attackers launched sophisticated social engineering campaigns, impersonating exchange representatives to trick affected users into transferring their cryptocurrency to fraudulent wallets. The threat actors also demanded a $20 million ransom from the exchange, which the company refused to pay, opting instead to offer a $20 million reward for information leading to their arrest. The financial fallout from the breach is estimated to be $400 million, covering remediation costs and customer reimbursements.[15]

How humans were exploited

The breach was a textbook case of human exploitation, enabled by several factors:

- **Bribery and manipulation of support agents:** The direct compromise of support agents, facilitated by bribery or sophisticated social engineering, provided threat actors with an internal gateway to sensitive systems.

- **Inadequate third-party risk management:** A significant number of the compromised agents were third-party employees stationed overseas, suggesting potential challenges with oversight and security protocols for third-party vendors.

- **Weak access controls:** Support agents may have had broader access to sensitive customer details than necessary to conduct their daily tasks, which violates the principle of least privilege.

- **Insufficient security training:** The agents fell victim to the hackers' tricks, indicating a lack of adequate training to recognize and resist sophisticated social engineering attempts.

- **Lack of real-time monitoring:** This activity went undetected for several months, suggesting that the exchange's monitoring systems may not have sufficiently detected unusual behavior or identified insider threats in a timely manner.

The cryptocurrency exchange's actions post-incident

Following the incident, the exchange took several measures to address the human element vulnerabilities and enhance security:

1. **Termination and law enforcement collaboration:** The involved employees and contractors were immediately terminated and the exchange began cooperating with law enforcement to pursue criminal charges.

2. **Bounty program and reimbursements:** The exchange refused the ransom and instead launched a $20 million reward program for information leading to the identification and arrest of the attackers. They also pledged to reimburse affected customers who lost funds due to the social engineering attacks.

3. **Enhanced insider threat detection:** The company increased investment in tools and strategies for real-time insider threat detection and monitoring across all company locations.

4. **Improved access controls:** The exchange implemented more granular access controls for support agents, ensuring they only have access to data essential for their roles.

5. **Mandatory scam-awareness prompts:** New security features, such as mandatory scam-awareness prompts during high-risk transactions, were integrated to educate users and prevent further social engineering attempts.

6. **Shift in support operations:** The exchange announced the opening of a new U.S.-based support hub to reduce reliance on overseas contractors for sensitive functions.

7. **Enhanced withdrawal verification:** Additional identity verification steps were implemented for large withdrawals from affected accounts to prevent unauthorized funds transfers.

The breach starkly underscores the imperative of stringent third-party oversight, robust access controls, and continuous, advanced training against the insidious threat of insider manipulation and bribery.

Case study 3: A cyber attack on an airline — the third-party human vulnerability

In June 2025, a foreign airline confirmed a significant cyber incident that exposed the personal data of millions of its customers. Unlike many breaches targeting an organization's direct infrastructure, this attack exploited human vulnerability within a third-party customer servicing platform, underscoring the critical importance of supply chain security and human vigilance.

What happened

The incident originated not from a direct assault on the airline's core systems, but from unauthorized access to a third-party platform utilized by one of its offshore call centers. Threat actors, widely suspected to be the notorious Scattered Spider group, employed social engineering tactics, specifically "vishing" (voice phishing). They successfully deceived a call center employee, convincing them to grant access to internal systems. This initial compromise led to the exposure of sensitive customer data including names, email addresses, phone numbers, birth dates, and frequent flyer numbers for up to six million customers (later refined to 5.7 million unique records after deduplication). Fortunately, the airline confirmed that highly sensitive financial details, such as credit card numbers, personal financial information, passport details, passwords, PINs, or login credentials, were not stored on the compromised system and thus were not accessed. While the airline's flight operations and safety were unaffected, the breach inflicted significant reputational damage and raised concerns about customer trust.[16,17]

How humans were exploited

This cyber attack serves as a stark reminder of how human factors can be the weakest link in an otherwise robust security chain:

- **Social engineering through vishing:** The attack hinged on a successful vishing attempt where a call center employee was expertly manipulated into granting unauthorized system access, proving how confident deception can bypass even technical controls.

- **Third-party risk and extended human perimeter:** The breach originating from a third-party vendor highlights a common vulnerability: an organization's cybersecurity posture is inherently tied to the security practices, including human element training, of its entire supply chain. The human component within third-party providers often presents an expanded attack surface.

- **Inadequate training against advanced tactics:** Social engineering attacks have led to successful breaches at numerous companies and highlights the need for continuous security training of employees to recognize and detect sophisticated vishing attempts, particularly against attempts by cybercriminal groups such as Scatted Spider, known for exploiting human trust.

- **Targeting helpdesk functions:** Cybercriminal groups, including Scattered Spider, are increasingly targeting IT help desks and call centers because these roles often have elevated access privileges and are susceptible to impersonation tactics designed to reset credentials or gain initial system entry.

The airline's actions post-incident

In response to the incident, the airline implemented a series of measures to mitigate the impact and strengthen its defenses:

1. **Rapid containment and investigation:** Upon detecting unusual activity, the airline took immediate steps to contain the compromised system and launched an investigation to understand the full scope of the breach.

2. **Enhanced security protocols:** The airline implemented additional security measures including further restrictions on system access, strengthened monitoring, and heightened detection capabilities. This also involved requiring extra identification for any changes to frequent flyer accounts.

3. **Collaboration with authorities:** The airline engaged closely with Australian cybersecurity and law enforcement agencies, including the Australian Cyber Security Centre, the Office of the Australian Information Commissioner, and the Australian Federal Police, to aid in the investigation and response efforts.

4. **Promoting customer vigilance:** The airline advised its customers to remain highly vigilant against potential phishing emails, calls, and messages, and encouraged them to enable multi-factor authentication on their accounts where available.

This breach serves as a powerful reminder that robust human-centric security strategies must extend across an organization's entire digital supply chain to account for third-party human vulnerabilities.

Chapter 6. The regulatory hammer

Global imperatives for human-centric security

The shift toward human-centric cybersecurity is not merely a best practice; it is rapidly becoming a regulatory mandate, particularly within the highly scrutinized financial services sector. Governments and oversight bodies worldwide recognize that a purely technical compliance checklist is no longer sufficient. The regulatory eye is now firmly fixed on how institutions prepare, empower, and defend their most critical asset: their people.

CISA's "Shields Up" initiative:

Calls for proactive measures like sophisticated wargaming and continuous awareness training, signaling a clear expectation for active human defense.

NIST NICE framework:

Actively promotes the development of behavioral competencies within the cybersecurity workforce, emphasizing the need for skills that extend beyond traditional IT.

EU NIS2 directive:

By 2025, this directive will formally mandate robust workforce cyber hygiene, placing stringent requirements on employee training and incident response capabilities across critical sectors, including financial services.

Regulator scrutiny:

Regulators in the United States, including the SEC and FTC, are intensifying their examination of how organizations prepare and educate their human capital, not just their digital systems. Failures stemming from human vulnerabilities are increasingly viewed as governance failures, leading to significant penalties and reputational damage.

For many institutions, where regulatory compliance is paramount, these evolving mandates are not suggestions but directives. Ignoring the human element is no longer an option; it is a direct path to regulatory sanction and erosion of public trust.

Chapter 7. Human resilience in practice

Measuring impact and ROI

In the competitive landscape of modern business, every investment demands a quantifiable return. The critical question then arises: how does one measure the strategic value of fortifying the human element? The impact of Cyber Human Defense is not merely anecdotal; it is empirically measurable, delivering compelling evidence of its significant strategic and financial ROI.

Quantifying the unseen defense:

Reduced incident rates

Track the tangible decrease in phishing click-through rates, successful social engineering attempts, and overall human-driven security incidents. A decline in these metrics directly correlates to a stronger human defense.

Faster incident response and containment

Measure the Mean Time To Detect (MTTD) and Mean Time To Contain (MTTC) for human-initiated incidents. Effective training and wargaming directly shrink these critical timelines, minimizing financial and reputational damage.

Improved employee reporting

Monitor the increase in suspicious activity reporting by employees. An engaged, aware workforce acts as an early warning system, identifying threats before they escalate.

Reduced cost of breach

Directly link investment in Cyber Human Defense to a lower average cost per breach. Every prevented incident and every contained compromise represents millions saved in remediation, fines, and lost business.

Enhanced compliance posture

Demonstrate adherence to evolving regulatory mandates (such as NIS2 and SEC,) by showcasing robust human-centric programs, reducing the risk of non-compliance penalties.

Strengthened brand trust

While harder to quantify directly, a demonstrated commitment to securing all facets of the organization, including its people, reinforces client confidence and brand resilience in a competitive market.

By establishing clear metrics and consistently measuring the effectiveness of human-centric security initiatives, organizations can move beyond abstract concepts and present a compelling business case for investing in their most invaluable, yet often overlooked, defense asset: their people.

Chapter 8. Strategic directives

Fortifying your human defenses

To effectively counter these evolving, human-focused threats, organizations must implement specific defensive strategies. The following actions are essential for building a resilient, security-conscious workforce:

Mandate monthly phishing and social engineering simulations:
Conduct regular, adaptive attack simulations. Providing immediate, actionable feedback is the most effective way to train your workforce to recognize and resist real-world social engineering tactics.

Establish a robust cyber champions network:
Embed security advocates within every business unit. Empower these "covert operatives" to foster a grassroots culture of vigilance, providing peer-to-peer support and intelligence gathering.

Implement advanced behavioral analytics for insider threat detection:
Deploy intelligent systems to monitor and analyze user behavior patterns. Proactive identification of anomalous activities can uncover malicious or negligent insider threats before they escalate into catastrophic breaches.

Integrate cyber human defense into every onboarding process:
Integrate cybersecurity responsibility directly into the onboarding process. From day one, new hires must understand they are active participants in the organization's defense, not just end-users of its technology.

Leverage gamification and positive reinforcement:
Transform security training from a chore into an engaging mission. Gamified learning modules and rewards for secure behavior drive higher engagement and foster a competitive spirit in collective defense.

Incentivize "Secure by Design" actions:
Reward employees who proactively identify vulnerabilities, report suspicious activities, and champion secure practices within their daily workflows. Make security an intrinsic part of performance.

Sponsor cross-functional cultural programs:
Move beyond purely technical upgrades. Invest in programs that foster a holistic security culture across all departments, reinforcing that cybersecurity is a shared responsibility, not just an IT mandate.

Chapter 9. Future threats

The evolving human battlefield

The adversary is not static; their tactics are constantly evolving, particularly in the realm of human exploitation. Organizations must anticipate the next wave of threats to ensure their human layer of defense remains robust and adaptive. Staying ahead means not just reacting to past incidents but proactively preparing your human defenses for the unseen battlefields of tomorrow.

Hyper-realistic AI-driven impersonations

Expect increasingly sophisticated deepfake audio and video capable of real-time interaction, making it nearly impossible to distinguish between a legitimate executive call and a malicious imitation.

Exploitation of mental fatigue

As digital interaction intensifies, attackers will likely target cognitive overload and digital fatigue, employing tactics designed to bypass judgment when individuals are most susceptible to error.

Scalable social engineering through AI

AI will enable attackers to generate vast numbers of highly personalized, context-aware phishing emails and vishing scripts, overwhelming human defenses through sheer volume and precision.

Weaponization of emerging tech

The integration of new technologies (such as VR/AR in the workplace and advanced IoT devices) will introduce novel human interaction points, creating new avenues for social engineering and physical security breaches.

Chapter 10. The human layer is real

And it's your ultimate defense

The age of perimeter-only defense is over. In the high-stakes world of financial services, where every transaction is a target and every employee a potential conduit, relying solely on technology is akin to fortifying the castle walls while leaving the gates unguarded. Cyber Human Defense is the critical paradigm shift, moving beyond the outdated notion of people as mere vulnerabilities and transforming them into active, intelligent operatives — alert, empowered, and deeply engaged.

From the high-rolling casino floors to the secure digital vaults of a cryptocurrency exchange and the global flight paths of an airline, the evidence is undeniable. Organizations are proving that through strategic training, continuous reinforcement, and acute psychological insight, the human element can be built into a very resilient, adaptive, and critically important layer of cybersecurity.

This is not just about compliance; it's about competitive advantage. It's about securing your future.

Change behavior. Change the outcome. Build your human operative network.

The future of your firm depends on it.

Sources:

1. https://www.scworld.com/news/95-of-data-breaches-involve-human-error-report-reveals

2. https://gitnux.org/social-engineering-attacks-statistics/

3. https://gkaccess.com/10-alarming-password-statistics-that-should-worry-it-managers-everywhere/

4. https://www.ibm.com/reports/data-breach

5. https://www.dashlane.com/blog/faq-phishing-costs

6. https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf

7. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

8. https://info.knowbe4.com/sat-asap-ps?utm_term=information%20security%20awareness%20training%20for%20employees|p&utm_campaign=google_sat_platform_us&utm_source=google&utm_medium=cpc&utm_content=&gad_source=1&gad_campaignid=22495546785&gbraid=0AAAAACkXGH5A

9. https://keepnetlabs.com/blog/reporting-security-incidents-how-security-awareness-drives-success

10. https://www.linkedin.com/pulse/how-employee-awareness-can-prevent-cyber-attacks-nate-sheen-2u6ac

11. https://www.halock.com/summarizing-the-ponemon-cost-of-a-data-breach-report-2022/

12. https://sosafe-awareness.com/blog/real-world-data-effectiveness-phishing-simulations/

13. https://industrial-software.com/community/news/in-depth-analysis-of-the-2023-mgm-resorts-cyberattack-virsec-systems-blog/

14. https://www.govtech.com/security/teen-arrested-on-suspicion-of-100m-vegas-strip-cyber-attack

15. https://www.csoonline.com/article/4042522/behind-the-coinbase-breach-bribery-is-an-emerging-enterprise- threat.html

16. https://www.abc.net.au/news/2025-07-02/qantas-cyber-attack-significant-data-stolen/105484720

17. https://www.theguardian.com/business/2025/jul/04/australias-privacy-watchdog-warns-vishing-on-the-rise-as-qantas-strengthens-security-after-cyber-attack

January 2026

Wells Fargo provides best practice and general information related to cyber risk and/or topics for educational and informational purposes only. The information provided in this document is not designed for any particular recipient but for the purpose of highlighting industry best practices for operating in a more secure manner. This document does not provide a complete list of all cyber threats or risk mitigation activities, nor does it document all types of best practices. Wells Fargo is not providing cyber-related advice or consulting services and recipients should decide whether to engage a cybersecurity firm for specific questions or advice.