ZEROFOX® Intelligence

Brief

The Accidental Insider Threat

B-2025-08-07a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Insider Threat, Social Engineering

August 7, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 11:00 AM (EDT) on August 6, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Accidental Insider Threat

| Key Points

- Unintentional insider threats represent an often overlooked attack vector that threat actors regularly exploit to gain unauthorized access to sensitive data and networks. Although unintentional and lacking overtly malicious intent, these behaviors risk impacting a company’s reputation, operational continuity, and long-term competitiveness.

- Insiders inadvertently expose sensitive organizational data by falling victim to manipulation or mishandling information through unintentional lapses in adherence to security protocols.

- The consequences of unintentional insider threats are often immediate and severe and include losses of private customer data, proprietary information, and sensitive internal communication.

Unintentional Insider Threats

Unintentional insider threats represent an often overlooked attack vector that threat actors regularly exploit to gain unauthorized access to sensitive data and networks. Although unintentional and lacking overtly malicious intent, these behaviors risk impacting a company's reputation, operational continuity, and long-term competitiveness. In the context of protective security, an "insider" refers to an individual with privileged access to an organization's systems, networks, and proprietary information.

- A multitude of near-daily reports reveal the causational relationship between employees negligently or accidentally engaging with malicious content and successful ransomware and digital extortion (R&DE) attacks against organizations that result in exposed sensitive data.[1]

Unintentional insider-related security incidents differ greatly from insider threats such as espionage or sabotage, which are overtly malicious. Unintentional insider behaviors are almost always the result of either negligence or accident; regardless of intent, the threats—through negligence or accident—can lead to organizational and reputational harm.[2]

- In August 2022, employees of a multinational technology corporation negligently exposed the login credentials to a vector of the company's infrastructure. The access potentially could have exposed other internal systems as well.[3]
- This exposed access vector was thwarted before actors could maliciously leverage it. However, if threat actors had been able to exploit the credentials, there likely would have been detrimental ramifications for the organization.

Negligent: Insiders who are generally aware of policy compliance standards but disregard them out of carelessness or convenience are negligent. This behavior increases the risk of exposure through repeated non-compliance or lax security hygiene.

[1] hXXps://link.springer[.]com/content/pdf/10.1007/s10111-021-00690-z.pdf
[2] hXXps://www.cisa[.]gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats
[3] hXXps://www.mimecast[.]com/blog/insider-threat-examples/

- In 2023, negligent insider threats represented 55 percent of all insider threat-related incidents.[4]

Accidental: Insiders who make mistakes due to human error that result in organizational harm are considered accidental insider threats. This behavior is unintentionally harmful—as these insiders are compliant with training and policies—but can manifest in misdirected emails, misconfigured systems, or interacting with malicious links. These errors are difficult to eliminate entirely, even with well-trained personnel.

- Notably, 88 percent of all data breach incidents occurred as a result of or were worsened by the mistakes of employees, underpinning the significant harm caused by unintentional insider threats.[5]

Inadvertent Methods of Data Exposure via Insider Threats

Insiders inadvertently expose sensitive organizational data by falling victim to manipulation or mishandling information through unintentional lapses in adherence to security protocols. The risk is not limited to untrained staff; well-informed employees across all levels may unknowingly contribute to security incidents. The fundamental human element of organizations cannot be overlooked in the context of cybersecurity risks, as employees naturally have the capacity to accidentally give threat actors unauthorized access to organizational systems and data.[6]

Social Engineering

Insiders possess the information required for threat actors to gain illicit access to a network's attack surface and conduct malicious operations against organizations using exploitable human attributes prone to manipulation through well-crafted attacks. Social engineering attacks target insiders and seek to trick employees into providing actors

[4] hXXps://www.stationx[.]net/insider-threat-statistics/

[5] *Ibid.*

[6] hXXps://www.apu.apus[.]edu/area-of-study/information-technology/resources/cybersecurity-vulnerabilities-do-employees-pose-a-risk/

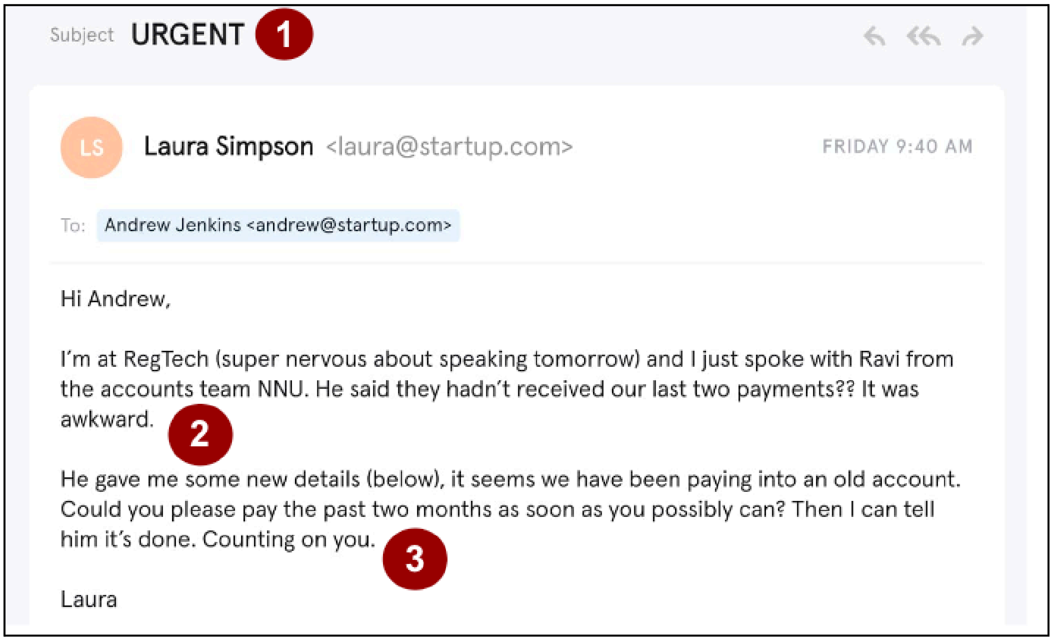
with access to internal systems and communications, financial accounts, or other sensitive information such as personally identifiable information (PII) or proprietary data.

- These attacks are designed to prey on human vulnerabilities by masquerading as legitimate executive leadership, other employees, or third-party vendors. Messages will appear authentic, as they are engineered to impersonate trustworthy sources.[7]
- Fabricated messages will rely on trust, curiosity, fear, and urgency while also considering predictable behavior and standard routines within the employee's organization and daily work flow. Human psychology is used against employees to lower their guard and lead them to disregard known security protocols.[8]

Phishing attacks deceive users through emails, text messages, or spoofed websites designed to appear legitimate and elicit trust, which prompt individuals to click on malicious links or submit sensitive data such as credentials or financial information into illegitimate sources. When successful, an employee falls victim to the phishing attack—thus providing threat actors with access to internal infrastructure, email accounts, PII, or proprietary data.

- According to the U.S. Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) report, phishing/spoofing, extortion, and data breaches comprised the top three cybercrimes in 2024.[9]
- In 2024, approximately 68 percent of cyberattacks involved a human element—typically achieved through social engineering attacks such as phishing.[10]

[7] hXXps://www.coalitioninc[.]com/blog/the-psychology-of-social-engineering
[8] *Ibid.*
[9] hXXps://www.fbi[.]gov/news/press-releases/fbi-releases-annual-internet-crime-report
[10] hXXps://www.coalitioninc[.]com/blog/the-psychology-of-social-engineering



Subject URGENT

Laura Simpson <laura@startup.com> FRIDAY 9:40 AM

To: Andrew Jenkins <andrew@startup.com>

Hi Andrew,

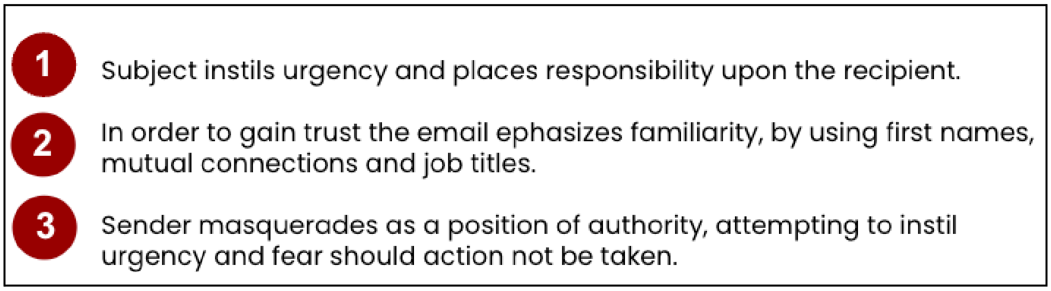
I'm at RegTech (super nervous about speaking tomorrow) and I just spoke with Ravi from the accounts team NNU. He said they hadn't received our last two payments?? It was awkward.

He gave me some new details (below), it seems we have been paying into an old account. Could you please pay the past two months as soon as you possibly can? Then I can tell him it's done. Counting on you.

Laura

Example of a phishing email

Source: ZeroFox Intelligence



1 Subject instils urgency and places responsibility upon the recipient.

2 In order to gain trust the email ephasizes familiarity, by using first names, mutual connections and job titles.

3 Sender masquerades as a position of authority, attempting to instil urgency and fear should action not be taken.

Characteristics of a typical phishing email

Source: ZeroFox Intelligence

Business email compromise (BEC) is a high-effort phishing technique in which an employee is tricked into providing sensitive information to a legitimate but compromised business email address. In these scenarios, employees unknowingly engage with a threat actor who has illicitly obtained access to legitimate business email accounts of an organization (typically belonging to its key leadership or suppliers) and utilizes the email accounts to request sensitive information or funds. These attacks rely on pretexting, spear phishing, and other social engineering methods that exploit trust and routine workflows and intercept communications by masquerading as a legitimate employee or supplier.

- In France, a real estate developer’s Chief Financial Officer (CFO) was the victim of a BEC attack wherein the actor masqueraded as a lawyer at a well-known accounting firm. The CFO mistakenly trusted these emails and subsequently transferred EUR 39 million to an account controlled by the threat actor.[11]
- The widespread adoption of remote work environments has contributed to a proportional increase in BEC attacks, as organizations rely more heavily on digital communication, virtual environments, and reduced in-person oversight.[12]

BEC can be achieved in a number of different ways but can be divided into two broad categories: spoofing and account takeover.

Spoofing: The falsification or slight alteration of email addresses, display names, or domains to impersonate trusted individuals. Spoofed addresses or names appear to be legitimate at first glance and trick employees into trusting the sender.

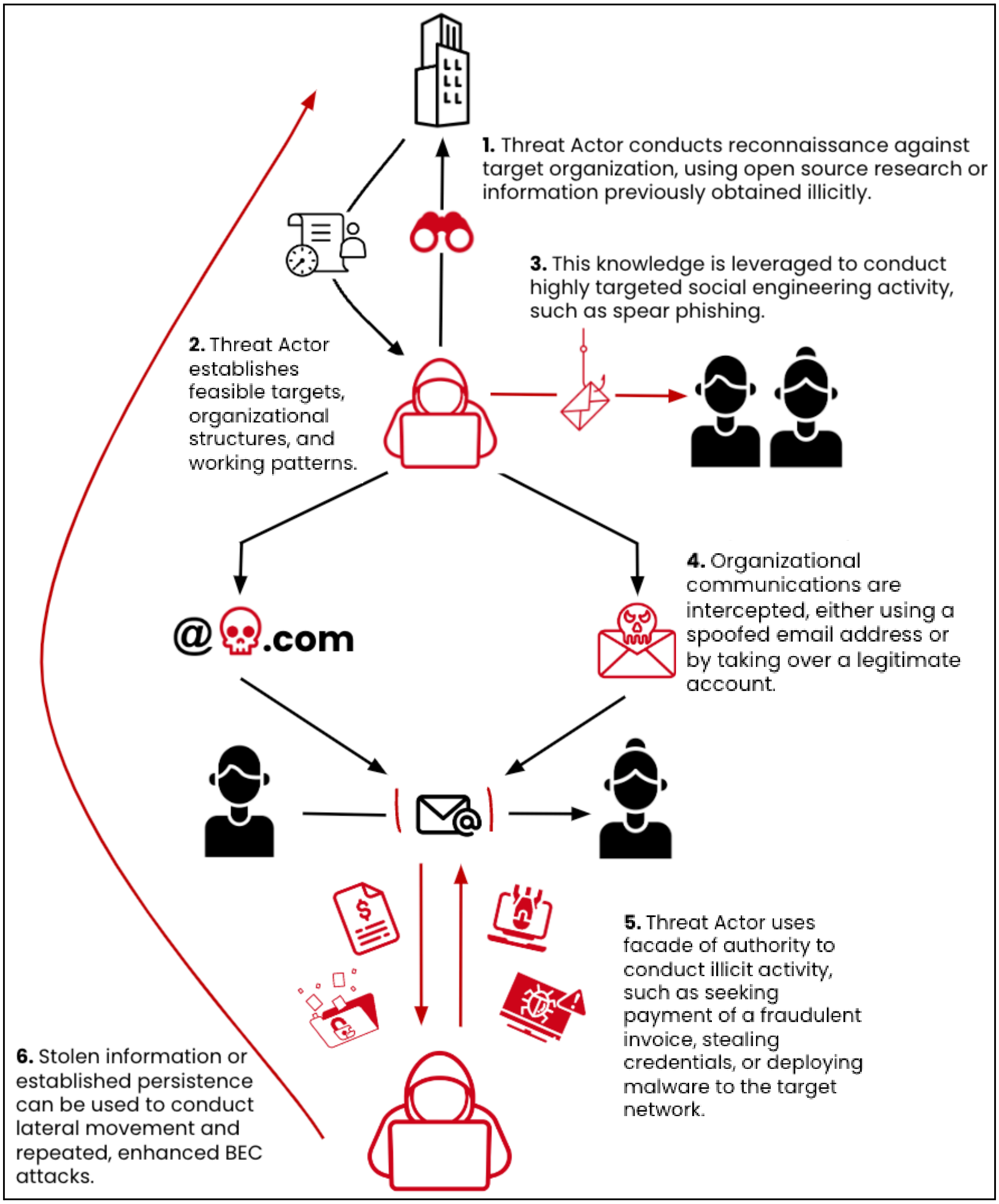
- Messages from spoofed accounts will attempt to exploit psychological triggers—familiarity, authority, urgency—in communications to employees to increase the likelihood of their interacting with masqueraded actors, thus further compromising the organization.

Account takeovers: Also referred to as email account compromise (EAC), these are higher-effort, complex attacks that involve actors using obtained login credentials or access through malware or credential harvesting to send legitimate-appearing communications to employees without scrutiny from either the email servers or message recipients.

- Employees who engage with these communications unknowingly transfer sensitive data or redirect funds to actors, while further compromising their organization by providing actors with additional attack vectors for subsequent operations.

[11] hXXps://www.proofpoint[.]com/us/blog/email-and-cloud-threats/10-real-world-business-email-compromise-bec-scam-examples

[12] hXXps://www.commercebankwyoming[.]com/resources/learn/blog/protecting-your-business-from-business-email-compromise-bec-scams-in-2025


1. Threat Actor conducts reconnaissance against target organization, using open source research or information previously obtained illicitly.
2. Threat Actor establishes feasible targets, organizational structures, and working patterns.
3. This knowledge is leveraged to conduct highly targeted social engineering activity, such as spear phishing.
@ .com
4. Organizational communications are intercepted, either using a spoofed email address or by taking over a legitimate account.
5. Threat Actor uses facade of authority to conduct illicit activity, such as seeking payment of a fraudulent invoice, stealing credentials, or deploying malware to the target network.
6. Stolen information or established persistence can be used to conduct lateral movement and repeated, enhanced BEC attacks.

High-level overview of how a BEC attack occurs

Source: ZeroFox Intelligence

Social engineering remains one of the most effective methods of exploiting employees within organizations to access sensitive data. These attacks are deliberately designed to exploit employees' cognitive biases and routine behaviors. Victims are accidental insider threats by interacting with threat actors posing as trusted sources; the near-immediate consequences often include data breaches, financial loss, and exposure to secondary threats such as ransomware deployment.

Shadow IT

Shadow IT refers to any software, hardware, or cloud service used within an organization without the explicit approval or knowledge of the IT or security departments. This includes tools such as unauthorized messaging applications, file-sharing platforms, or personal devices connecting to corporate networks, which are often used by employees to fill the gap between deficient tools and efficiency requirements or for convenience.

- Shadow IT usage has reportedly increased significantly in recent years, with some figures demonstrating a 59 percent increase—likely due to a proportional increase of remote work arrangements.[13]
- Reporting also suggests that IT departments attribute the usage of Shadow IT to a 54 percent increased risk of data breaches within their organizations.[14]

Employees are accidental insider threats when they store or share sensitive data on unapproved cloud services, download unauthorized software that contains malware, use unsecured devices or networks (such as personal devices or public Wi-Fi), and ignore security updates on unofficial tools. Shadow IT most often occurs in flexible or remote work environments where employees operate outside of the direct supervision of their IT department, thus creating an insecure work environment.

- Confidential data that exists outside of regularly monitored and secure internal systems is more difficult to secure and back up. Insecure networks that are not regularly monitored by IT professionals present an additional risk to connected corporate devices.

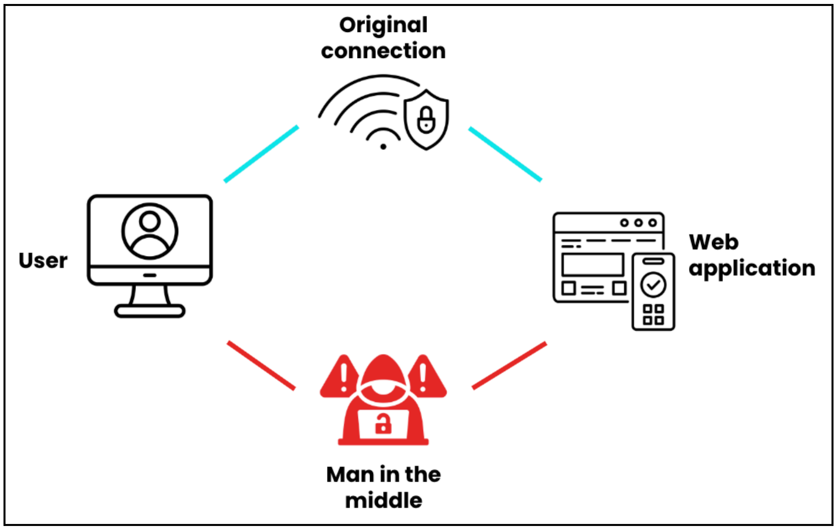
Remote employees often rely on public Wi-Fi or home networks that may lack proper configuration—or at least are not configured to the security standards of an

[13] hXXps://www.cloudflare[.]com/the-net/shadow-it/

[14] hXXps://f.hubspotusercontent40[.]net/hubfs/6033395/2020%20was%20a%20year%20of%20change%20-%20a%20Core%20research%20report.pdf

organization's network—unintentionally exposing sensitive data. Data sent over insecure networks can be intercepted in what is referred to as man-in-the-middle (MITM) attacks.

- An MITM cyberattack occurs when two individuals believe they are directly and privately communicating with each other while an unknown third party intercepts the relays, which exposes usernames, passwords, and financial information.



Example of an MITM attack
Source: ZeroFox Intelligence

Personal devices without company oversight often lack the necessary security configurations and controls mandatory on corporate-issued hardware. Such devices likely do not have endpoint protection or patch management, and files are saved locally or synced to personal storage without encryption.

- It is increasingly common for organizations to allow personal devices to connect to work email addresses, internal communications applications, and virtual meeting platforms.
- This can leave an organization vulnerable through varied personal mindfulness and physical locations, as well as the device's settings and passwords.

Improper Data Disposal

Improper data disposal is an organization's failure to securely erase, destroy, or decommission sensitive data, systems, or access when the data is deemed as no longer needed or a new system is adopted. As a result of oversight or convenience, improperly disposed data persists beyond its authorized use, leaving it vulnerable to exploitation by threat actors.

- Over the last 10 years, secondhand device studies have consistently shown that organizations and individuals alike often assume that superficial actions are enough to completely wipe data from devices, unaware of the survival of lingering data.[15]
- Organizations are held to compliance standards and regulations to ensure data is safeguarded. When employees fail to properly dispose of data, it can be at risk of being used in R&DE attacks, identity theft, and other financial crimes, which can cause legal ramifications for organizations.[16]

Sensitive, confidential, or regulated data stored insecurely lacks proper protections against unauthorized access, theft, alteration, or loss. This can occur on physical devices, local systems, or cloud-based platforms where data is unencrypted; on legacy servers; or on personal cloud accounts without approval. Unauthorized storage—like copying work files to a USB drive or emailing data to personal email addresses in order to work from home—creates gaps in security measures.

Outdated or forgotten cloud accounts or platforms never properly decommissioned or sanitized will continue to contain sensitive data and credentials. It is also possible that employees leave access permissions intact, allowing users to gain a foothold. These environments are often left active without proper monitoring or security updates, which leaves data exposed indefinitely.

- In 2025, cybersecurity researchers monitored abandoned cloud-based file storage systems previously used by several entities, such as governments, corporations, and cybersecurity firms.[17]
- While researchers gained control over the abandoned infrastructure before threat actors did, had it been accessed by malicious actors, this infrastructure could have been leveraged in large-scale supply chain attacks, ultimately impacting the implicated organizations and industries worldwide.

[15] hXXps://www.ingrammicrolifecycle[.]com/blog/returned-devices-data-risks
[16] hXXps://ncsglobalinc[.]com/insights/secure-data-destruction/
[17] hXXps://cyberscoop[.]com/abandoned-cloud-aws-s3-buckets-security-risk-watchtowr/

Organizations that fail to fully and securely remove a departing employee's access to systems, data, and services leave critical infrastructure and sensitive information at risk. As a result of insufficient offboarding processes, a departing employee can retain access to email accounts, cloud storage, project management tools, and customer and vendor systems; such accounts can be unintentionally accessed or unsecured.

- Insufficient offboarding processes result in employees retaining sensitive information or access upon their departure, underpinning the significance of this overlooked vector of data disposal.[18]
- Leftover accounts can be targeted and used by threat actors in future credential stuffing or phishing attacks.

Physical data—including printed documents, storage media (such as hard drives or USBs), and other devices that contain sensitive information—left unprotected poses a significant risk of misuse or theft. While most breaches occur over the digital landscape, threat actors often exploit the human and physical side of security, seeking vulnerabilities to infiltrate and extract data.

- An organization is at risk when employees leave printed material on desks, in cars, or in shared spaces; improperly dispose of documents without shredding; discard devices without securely wiping them; and store passwords in easily accessible places.
- In 2021, a healthcare organization discovered that several of their hard drives had been improperly disposed of; thousands of patient PII and financial information was breached, and the organization faced significant fines for data protection violations.[19]

Outlook

The consequences of unintentional insider threats are often immediate and severe, with losses of private customer data, proprietary information, and sensitive internal communications. These losses can further manifest into market disadvantages and

[18] hXXps://www.goworkwize[.]com/blog/protect-company-data-after-employee-leaves

[19] hXXps://eridirect[.]com/blog/2021/09/improper-disposal-of-hard-drives-leads-to-large-healthcare-data-breach/

supply chain vulnerabilities, which can have long-term effects on both the organization and the broader industry.

Market disadvantages: Insider-caused breaches expose intellectual property or customer data, resulting in reputational harm, legal liability, and financial loss. The erosion of consumer trust and investor confidence can reduce an organization's market value and weaken its competitive position.

Supply chain vulnerabilities: Insider-caused breaches can lead to operational disruptions or expose third-party integrations. Delays in production, system downtimes, and security gaps ripple across the enterprise and can affect downstream partners. Resources are diverted to secure the organization, generating additional costs and decreasing productivity. In highly connected industries, such disruptions may cascade across entire sectors or international networks.

Recommendations

Insiders may unintentionally harm an organization due to insufficient training, incomplete organizational policies, or personal mental health factors—all of which may inadvertently increase the likelihood of harmful behavior. Mitigating potentially harmful behavior relies on universal participation across an organization with an adequate and recurring training program that is interactive and engaging.

- Implementing a comprehensive and memorable training program will fortify the human element of an organization against common social engineering attacks.[20]

Training alone may not suffice; ensuring that an organization has accessible industry-standard cybersecurity policies, standard operating procedures (SOPs), and the necessary resources to operate safely and efficiently is another mitigation strategy.[21] Without such resources, employees lack guidance from their leadership and IT teams

[20] hXXps://trustnetinc[.]com/resources/the-human-factor-why-cybersecurity-awareness-training-is-your-first-line-of-defense

[21] hXXps://www.stonehillinnovation[.]com/blog/the-importance-of-standard-operating-procedures-for-cybersecurity

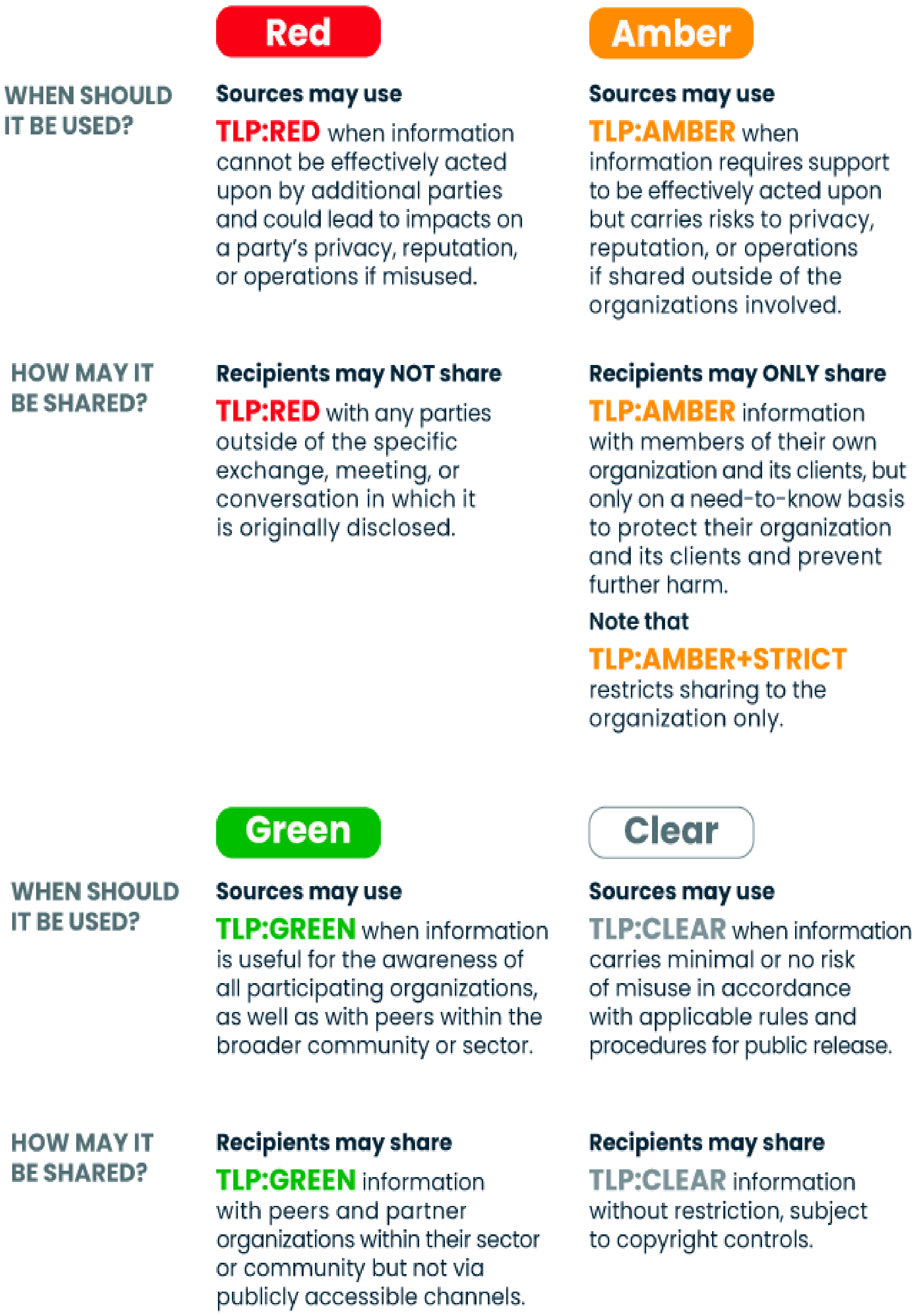
and may be more likely to make mistakes. Updated IT, disposal, and security reporting-channel policies can limit the amount of mishandling within an organization.

Even with exceptional training and thorough corporate guidance, personnel experience varying and uncontrollable circumstances that can affect their daily work performance. Work-related or personal stress, a poor work-life balance, or other extenuating circumstances can increase the likelihood of employees making mistakes.

Establishing a proper security-reporting channel for accidents can facilitate the expeditious retrieval of data or securing of networks.[22] The rapid detection, identification, and assessment of threats and potential indicators can significantly reduce the harm caused by accidental insider threats while ensuring minimal data and infrastructure are exposed.

[22] hXXps://www.gothamtg[.]com/blog/creating-an-effective-process-for-reporting-security-incidents

Appendix A: Traffic Light Protocol for Information Dissemination

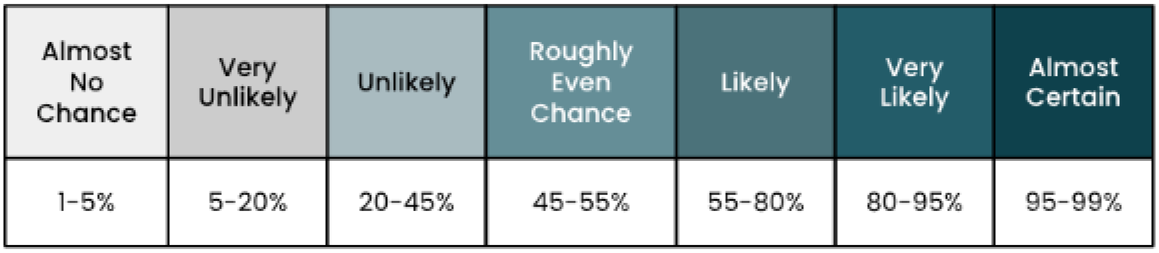


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.



Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%