

Don't Become an Insider Threat

An insider threat refers to an individual who has been entrusted with access to or knowledge of a company's confidential resources and information. Due to their unique privileges, insider threats can compromise organizations' most valuable assets and leave them increasingly vulnerable to cyberattacks, also known as insider events.

You may think that insider threats are primarily malicious individuals (e.g., disgruntled staff or fraudulent vendors) intentionally abusing their access to engage in harmful activities for personal gain, but the reality is quite the opposite. Many insider threats are actually well-meaning employees who unknowingly expose their company's data and assets to unauthorized parties. This is often due to a lack of experience, awareness or attentiveness to potential security risks, making them more error-prone and easily manipulated by cybercriminals' tactics.

The Ponemon Institute has found that 55% of insider events stem from well-meaning employees. Additionally, IBM's Cyber Security Intelligence Index found that human error is a factor in 95% of cyber incidents. As such, it's crucial to take steps to avoid becoming an insider threat and putting your employer at risk. This article outlines habits that may lead to cybersecurity exposures, highlights several insider threat scenarios and explains what you can do differently.

Risky Habits

As an employee, you represent the most prevalent type of insider threat. Some everyday habits that can create cybersecurity risks include:

- Reusing passwords across work accounts or sharing credentials with others (even trusted co-workers)
- Clicking unverified links, downloading unanticipated attachments or otherwise interacting with suspicious messages sent by unfamiliar parties
- Oversharing certain company information (e.g., project details or organizational structures) on social media

- Rushing through work assignments and risking additional mistakes, especially when handling sensitive data or assets
- Using unapproved devices or applications to complete work assignments
- Losing or leaving workplace devices in public settings (e.g., airports, hotels or coffee shops)
- Neglecting to regularly review workplace cybersecurity policies and related documentation or attend awareness training
- Ignoring routine software updates or failing to enable company-provided cybersecurity tools, such as a virtual private network (VPN) or multifactor authentication (MFA)

Even the most diligent employees may engage in these habits, whether out of perceived convenience, pressure to meet project deadlines, risk fatigue or complacency, misplaced trust, or overdependence on existing security resources. When left unchecked, these habits can cause serious consequences.

Insider Threat Scenarios

Here are some insider threat scenarios involving well-meaning employees:

- An employee is deceived by a phishing scam, in which a cybercriminal impersonates a manager via email and manipulates the employee into sharing their login credentials, thereby giving the perpetrator unauthorized access to the company's larger IT infrastructure.
- An employee doesn't review company resources and forgets to attend training on a new type of workplace software, resulting in them making several errors while using this technology and compromising the sensitive data stored on it.
- An employee rushes through their work assignments and makes multiple mistakes, ultimately sending confidential business files to the wrong recipients and downloading a malicious program disguised as a software update.

Cybersecurity Essentials

bch

BRADY, CHAPMAN,
HOLLAND &
ASSOCIATES

What You Can Do

To minimize the risk of insider events and play your part in promoting strong cybersecurity on the job, follow these guidelines:

- **Maintain account security.** Utilize complex and hard-to-guess passwords across your work accounts. Passwords should be at least 15 characters; use a combination of uppercase and lowercase letters, numbers and symbols; and spell out unique, unpredictable phrases (e.g., “@pplesRtheB3stFruit!”). Never reuse or repeat passwords or share your credentials with others. Alongside strong passwords, use your employer’s MFA services as an extra layer of account security.
- **Safeguard devices and data.** Only use devices specifically designated for work purposes, and refrain from sharing them with others. If you work from home, ensure a secure connection to your private Wi-Fi network, regularly update your router’s firmware and lock your device whenever it’s not in use. When working in a public setting, never leave your device unattended. In any location, always connect to your employer’s VPN or other secure access solution before handling corporate assets and keep all security software up to date. Furthermore, use only approved applications for communication (e.g., email, direct messaging and video calls) and file sharing.
- **Think before you act.** Be cautious of sharing company information online, especially via public social media accounts. Also, be ready to identify key indicators of phishing scams (e.g., unknown or copycat senders, generic or threatening language, unsolicited links or attachments, and unusual or sensitive requests) and act accordingly. Don’t respond to these messages or answer prompts without first verifying them through an alternative channel.
- **Take your time.** Avoid rushing through work assignments or taking any shortcuts to meet deadlines, as this could increase the likelihood of mistakes and related cybersecurity issues. Never be afraid to ask for help or additional support if you are feeling overwhelmed by your task load.
- **Leverage company resources.** Make the most of all cybersecurity protections available to you. This may entail reviewing workplace policies, attending training sessions and ensuring corporate security tools (e.g., endpoint protection software, host firewalls and automatic updates) remain enabled.
- **Report suspicious activity.** If you notice any unusual activity or suspect a possible cyberthreat, report it immediately. This may entail using your device’s built-in alert system, flagging concerning messages or other content for further review, or contacting the IT team directly.

For More Information

Cybersecurity can be challenging, but you don’t have to navigate this topic alone. Reach out to your employer for more information on cybersecurity best practices.

bch-insurance.com