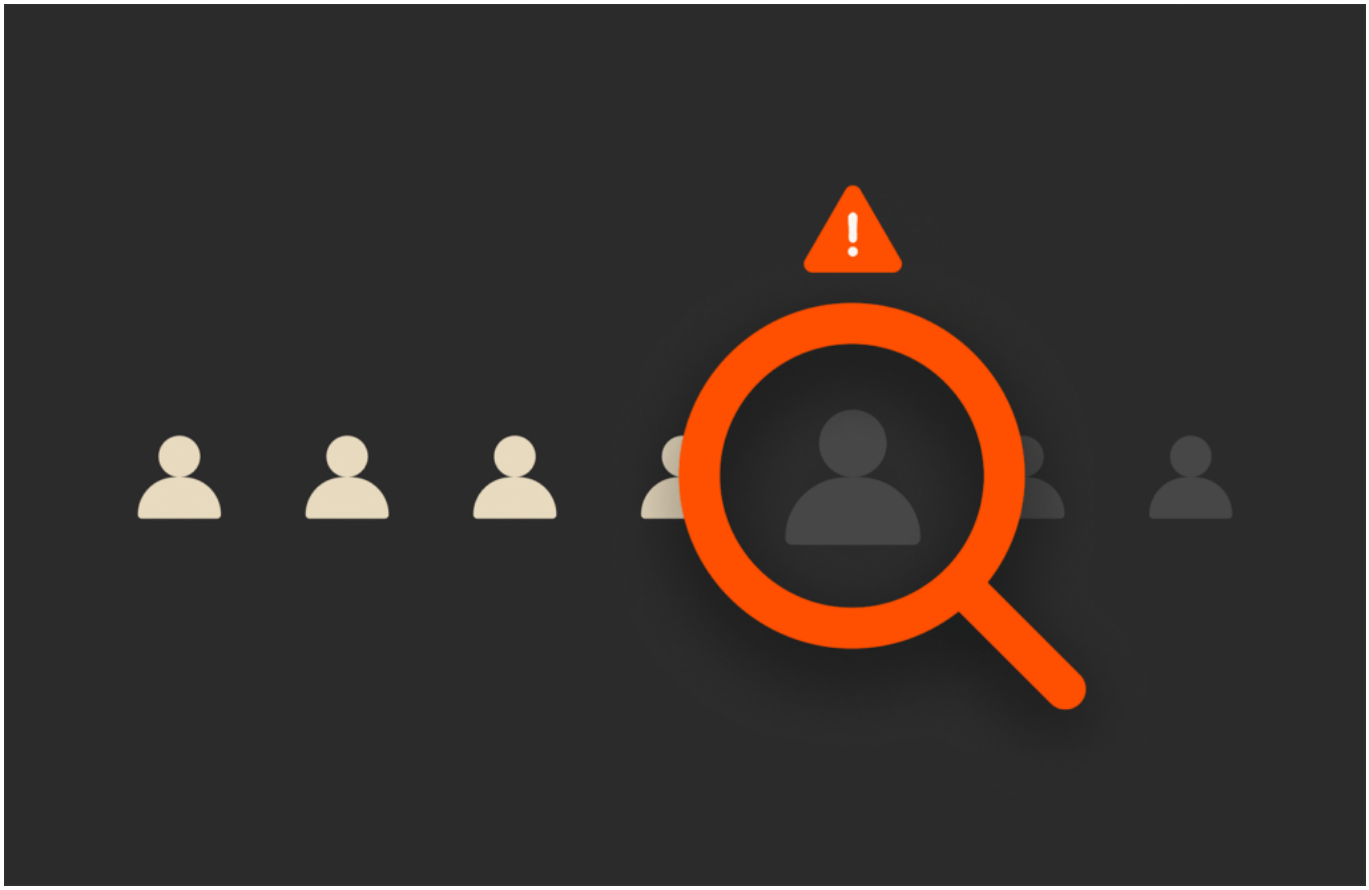
What Are Insider Threats and How Can You Combat Them?



[bws_pdfprint display='pdf,print']

In mid-July 2024, security awareness company KnowBe4 hired a software engineer–or so they thought. The new hire passed all the usual background and security checks and was cleared to start work with their new company computer. But then they started downloading tons of malware and executable software.

As KnowBe4 explained, the new hire was using a stolen identity. The company's security team dug into the data surrounding the hacker's activities, shutting down access to the company device. " If it can happen to us, it can happen to almost

anyone," the company said.

The KnowBe4 experience is a prime example of why threats aren't limited to career cybercriminals and ransomware attacks. An estimated quarter of all enterprise cybersecurity incidents stem from insider behavior, according to Forrester. Forty percent chalked it up to an accident, 47% noted malicious intent, and 13% felt the event was a mix of the two.

What can CISOs and IT leaders do to minimize this risk? Read on to learn more and download the "Beyond the Firewall" report for insights from CISOs on combating modern insider threats.

What's Behind Internal Security Threats?

A couple of things. As I've previously mentioned, identity is the new perimeter. Identities, including company insiders, are often targets for hackers using social engineering tactics and create a multitude of endpoint vulnerabilities outside of a network's four walls.

"There are very limited things that I can do from a traditional security perspective. So it becomes very much process-focused. Also, specific privilege access management is critical." – "Beyond the Firewall: Insights and Strategies from Leading CISOs"

Then, there's the rapid proliferation of distributed workforces and cloud-based workspaces that scatter users and data beyond the four walls of an office's protected networks. Employees, wherever they're working, can pose a variety of risks that corporate data protection strategies must address and mitigate:

- Employees working from home might be on a shared Wi-Fi network that has weak security. Hackers exploiting the vulnerability might piggyback onto the connection for unauthorized access to your digital resources. It opens the door for data theft, possibly in the form of a costly ransomware attack.

- Employees working at airports, hotels, shopping centers, or other places with public charging stations now run the risk of getting their devices infected by malware via the USB ports.

What Are Examples of Insider Security Threats?

- **Rogue administrators or disgruntled employees** with access to sensitive information might steal data to sell for profit on the dark web. They could use their credentials to sabotage or delete files for revenge. Malicious actors are also approaching employees, offering large sums of money in exchange for credentials or data.

- **Non-human accounts** that go unmonitored can serve as attack vectors. If

these accounts are abandoned or unmonitored after an employee has left, it can be difficult to regain access or note when login attempts occur.

- **Poor data hygiene**. Software administrators might accidentally misconfigure a program, miss an update, or overlook a patch. Engineers who create backdoors could unknowingly create a vulnerability in your company's defenses.

- **Human error.** An employee could mistakenly delete critical files.

- **High-level access engineering errors**—whether it's unwittingly leveraging insecure open source code or intentionally sidestepping protocols. In a recent CISO roundtable, one CISO noted, "A lot of what developers consume is open source. The integrity and quality and authenticity of that code is extremely critical." Testing and the ability to securely roll back is key here. Another noted, "Engineers tend to be very creative. Even if I introduce all of the security controls possible, they'll find a workaround or create a backdoor or a server that will make their life easier—or, easier than the strict controls that I've introduced."

- **A phishing or social engineering scam** could trick an employee into revealing passwords or other sensitive information. In the scam, someone could pose as a legitimate source via email or a phone call. Any information shared could then be used for nefarious purposes, such as hacking into accounts, stealing other sensitive information, committing identity fraud, or mounting a ransomware attack.

10 Ways to Defend against Insider Threats

Preventive measures go a long way toward keeping cyber intrusions and data theft at bay, but the key is resilience. To render the intrusion **a non-event instead of a disaster,** organizations need the capabilities to get critical systems back online, fast:

1. Get visibility into your data. You have to know what is happening and have forensic readiness when the worst occurs.

2. From a process standpoint, automating software patches (i.e., good data hygiene) and updates helps to mitigate human error.

3. Continual, updated education about company policy and best practices for security is also essential—but, make it role-based and relevant. Let employees know the power they wield in allowing something bad to happen. They should ask themselves “How am I a vector?” to understand what behaviors are acceptable to the company and what social engineering (phishing) attempts look like.

4. Start by limiting access from countries that you do not have operations in or that are considered high-threat or high-risk countries. Have a combination of controls. Ideally, introduce a unilateral, layered stack of tools across the environment so if one control fails, another control can compensate. For example, block personal emails to prevent the sending of data at the email level. The same can be done at the network level. Limit how employees can access data to company-owned devices or managed devices at the storage level.

5. A robust asset management and data classification system that allows you

to understand where data resides. Run data discovery exercises and tailor security controls based on findings. This can help organizations understand the level of security that each specific class of data needs to have to avoid having all data be secured at the maximum level, which can be costly. Increase the security measures on data that's classified (whether personal, critical, or industrial data), then have encryptions or other techniques that can increase the access level to that data when needed.

6. Increase security measures and role-based controls on sensitive data. Adopting a zero trust approach to security is another best practice to consider. Zero trust limits application access to only confirmed-safe users, systems, and processes—preventing bad actors from doing damage. Multi-factor identification can reduce reliance on trust or authentication.

7. Bring high-access users to the security conversation. This is all about sharing responsibility. For engineers who have higher privilege or higher levels of access across systems, make security part of their remit. Bring them to the table and ask, "Walk me through what you do normally. What is the normal day-to-day process for you?" Based on what they're doing at the moment, introduce security controls and work with them to implement.

8. Monitor log data for behavior analytics. Organizations cannot live without security logs. These can be used to raise alerts on unusual employee activities. By creating a baseline for each user's typical behavior, behavior analytics programs make it easier to spot an anomaly (such as geolocation changes) as a potential compromise.

9. Threat prevention monitoring and anomaly detection continually analyze traffic flows for anomalous signatures that could indicate the presence of malware or the flooding of host computers to cause a denial of service (DoS) or distributed DoS attack.

10. Finally, make sure users know how to report issues—and make internal security a mandate. Some organizations may even consider a more formal "consequence management" approach—if users know the policy and know the standards but still go around them, they'll face consequences.

Resilience: Make Security Events Non-events

Despite these best efforts, security experts agree that every company's number eventually comes up. For example, **internal errors or misconfigurations** can open your organization up to a ransomware attack, whereby a hacker encrypts your files, deletes the originals, and demands payment for the encryption key—unless you have applications backed up in a format that can't be changed after they're written. In other words, they're "immutable."

What matters most is **resilience**: how well-prepared you are can minimize the damage and speed recovery. A successful attack can be rendered a non-issue with immutable backups like SafeMode™ Snapshots. SafeMode takes immutability to the next level by applying an out-of-band, multifactor-authentication layer to immutable snapshots. Even an administrator can't modify, encrypt, or delete these read-only snapshots without following the out-of-band authentication process.

Attempts to delete SafeMode Snapshots will fail because they're locked down. Resilience comes from being able to simply move the data vo

Written By:

Andy Stone