Key Strategies to Prevent Accidental Insider Data Breaches

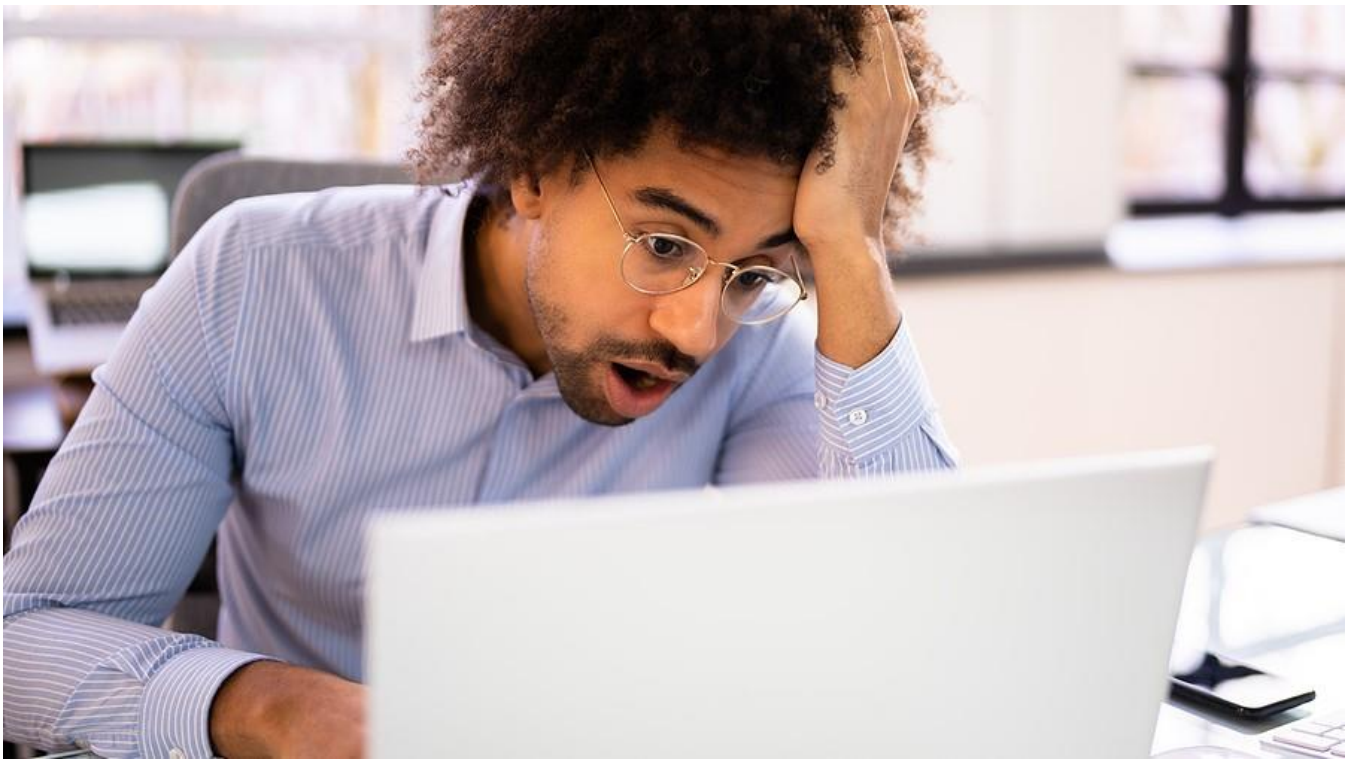
The biggest threat to your organization may come from just down the hall. In fact, in a recent survey by Egress, 94 percent of companies reported insider data breaches just in the last year. Those incidents resulted in some huge financial losses, as well as loss of reputation and customer trust.

In an insider threat, someone uses authorized access to harm the organization's system or network, lose sensitive data or allow hackers inside. While some insider threats are caused by malicious insiders, many happen accidentally. A combination of end user training, proper access management and automated behind-the-scenes protection can help.

Three Ways Insiders Pose a Threat

Most employees do not intend to expose sensitive data or damage systems. In some cases, insider data breaches result from employee negligence. Employees may not understand company security policies, or they may deliberately choose to ignore them. For instance, an employee might use unapproved file sharing services that lack proper security.

In other instances, end users do not fully understand the technology they use. For example, a remote worker may not understand how to adjust security settings or apply security patches. Or an employee may not know how to encrypt a mobile device that later winds up stolen.



Finally, many insider threats happen by accident. An employee may click on a malicious hyperlink in a phishing email or mistype an email address and unintentionally send sensitive information to the wrong person.

Prevent Insider Data Breaches with Engaging, Actionable Training

Employees represent the last line of defense against data breach. They need to understand cyber security best practices, and they must have a solid knowledge of company policies. They must also know how to recognize phishing attempts and how to report suspicious activity.

Consequently, companies that make security awareness a priority see results. For instance, a study by The Aberdeen Group indicated that security awareness training reduced the instance of successful social engineering threats by up to 70 percent.

However, to be effective, training must be done right. Annual training will not prove sufficient. Instead, present training at regular intervals, making it interactive and emphasizing the why. Training that builds a scenario engages the participants, helping them understand the context and importance.

Follow Up with Phishing Simulations

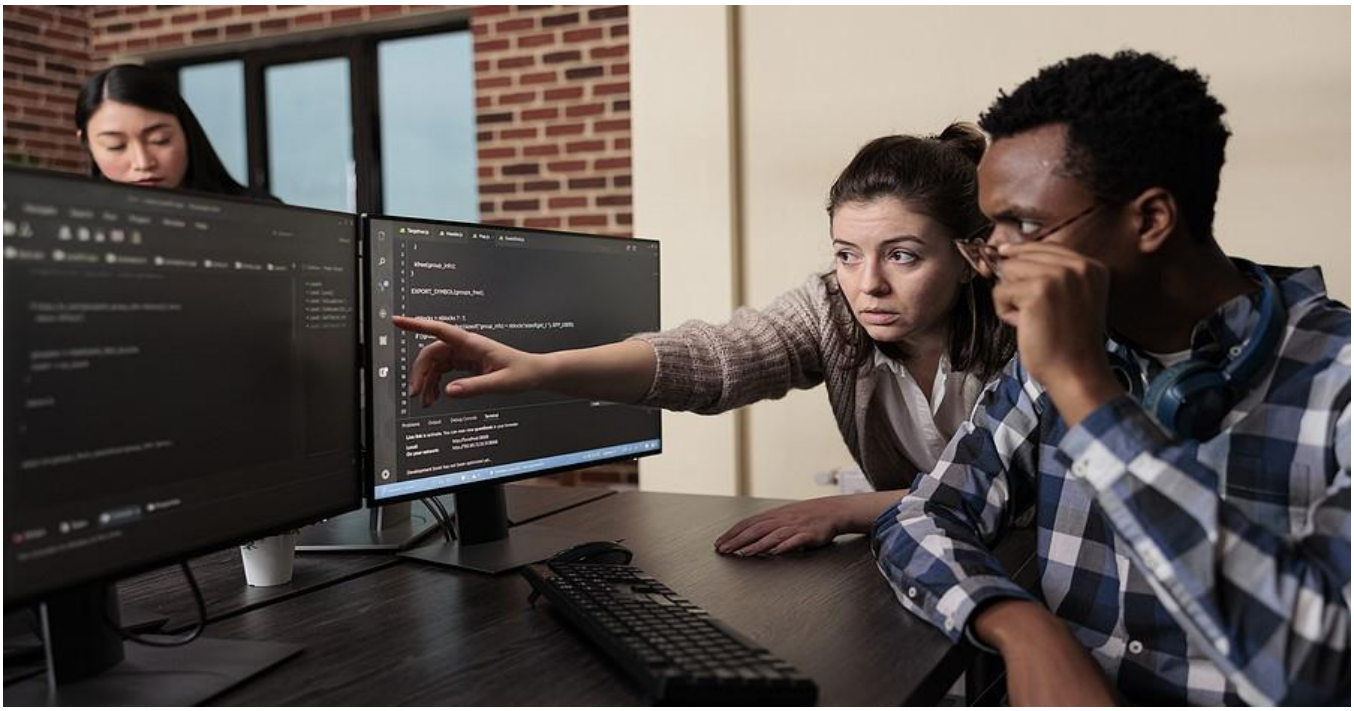
Once employees know the signs of a phishing attempt, drive the training home with phishing simulations. In a simulation, employees periodically receive staged phishing emails, and the organization tracks open rates and click through rates. They can then use the phishing emails as a teaching tool, following up with additional training as necessary.

Carefully Approach Access Management

In addition to security awareness training and phishing simulations, organizations must take a close look at their access management. This includes the policies and tools surrounding how users access the organization's applications and systems.

To begin with, use a policy of limited access. That is, assign users just the access they need to do their jobs. And grant admin access only when absolutely necessary. Wherever possible, implement multi-factor authentication (MFA).

Additionally, protect the organization by improving communication between HR and IT security personnel. That is, implement procedures so that IT is alerted and can revoke access immediately when an employee leaves the company.



Add Automated Protection Behind the Scenes

To further guard against insider data breaches, organizations should implement several protections behind the scenes. For instance, data loss prevention software classifies and monitors critical data, reducing the risk that it will fall into the wrong hands.

Policy-based email filtering provides additional key protections. Filters check incoming email for spam and phishing attempts. And they can be set to scan outgoing email for certain keywords or phrases that might indicate a breach of security policy.

Implement a Multilayered Defense

Businesses of all sizes run the risk of insider data breaches. With solutions like MXINSPECT, even small businesses enjoy enterprise-class protection. Combine email protection with advanced threat protection, security awareness training and phishing simulations for a complete defense.