Microsoft

Securing the weakest link: How to turn employees into your greatest strength

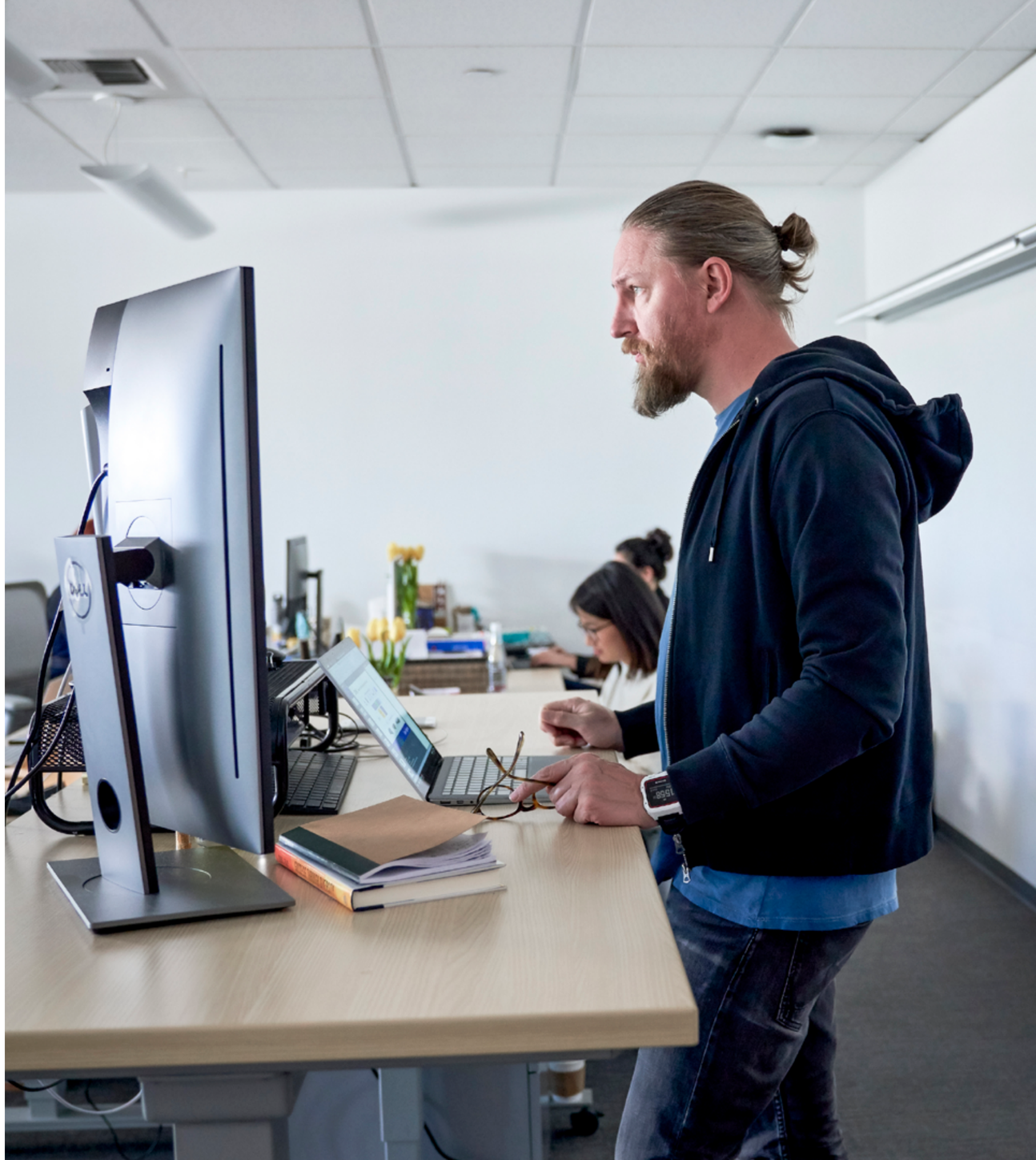


Table of contents

01

02

03

04

As a security decision maker, you know that an enterprise's security is only as strong as its weakest link. Social engineering—using psychology to trick people into compromising their own privacy or network security—is now the leading tactic in cyberattacks. This means that insiders—such as employees, contractors, partners, and colleagues—are primary threat vectors, whether they intend to be or not.

Unfortunately, business leaders at all levels remain generally unaware of the urgency of this threat. A recent survey of US companies revealed that only 21 percent of respondents listed insider threats as a top area of concern. Data shows that four out of five employees have experienced a social engineering attack in the past 12 months.

To be clear, the problem is less about attackers hacking employees and more about exploiting the vulnerabilities that employees in busy corporate environments create. It's true that some insider threats are malicious—a disaffected employee wreaking revenge or succumbing to the lure of a payoff. Mostly, though, insider breaches occur because otherwise well-meaning employees are too distracted or unaware to take action in defense of their organization's digital estates.

Fully engaged defenders understand the stakes and internalize their own responsibility in digital security. Strengthening employees as your front line must be an ongoing effort, one that incorporates dynamic training—including "live" simulations and drills—and reflects the same level of sophistication as the attackers you face.

Users are both my first line and my last line of defense.

Bret Arsenault,
Microsoft Chief Information Security Officer

Microsoft's Bret Arsenault advises fellow CISOs to create clarity and generate energy to turn users into defenders. The key is to make things simple for all your employees, not just the technical teams. Follow the steps[1] in this roadmap to get started.

01

02

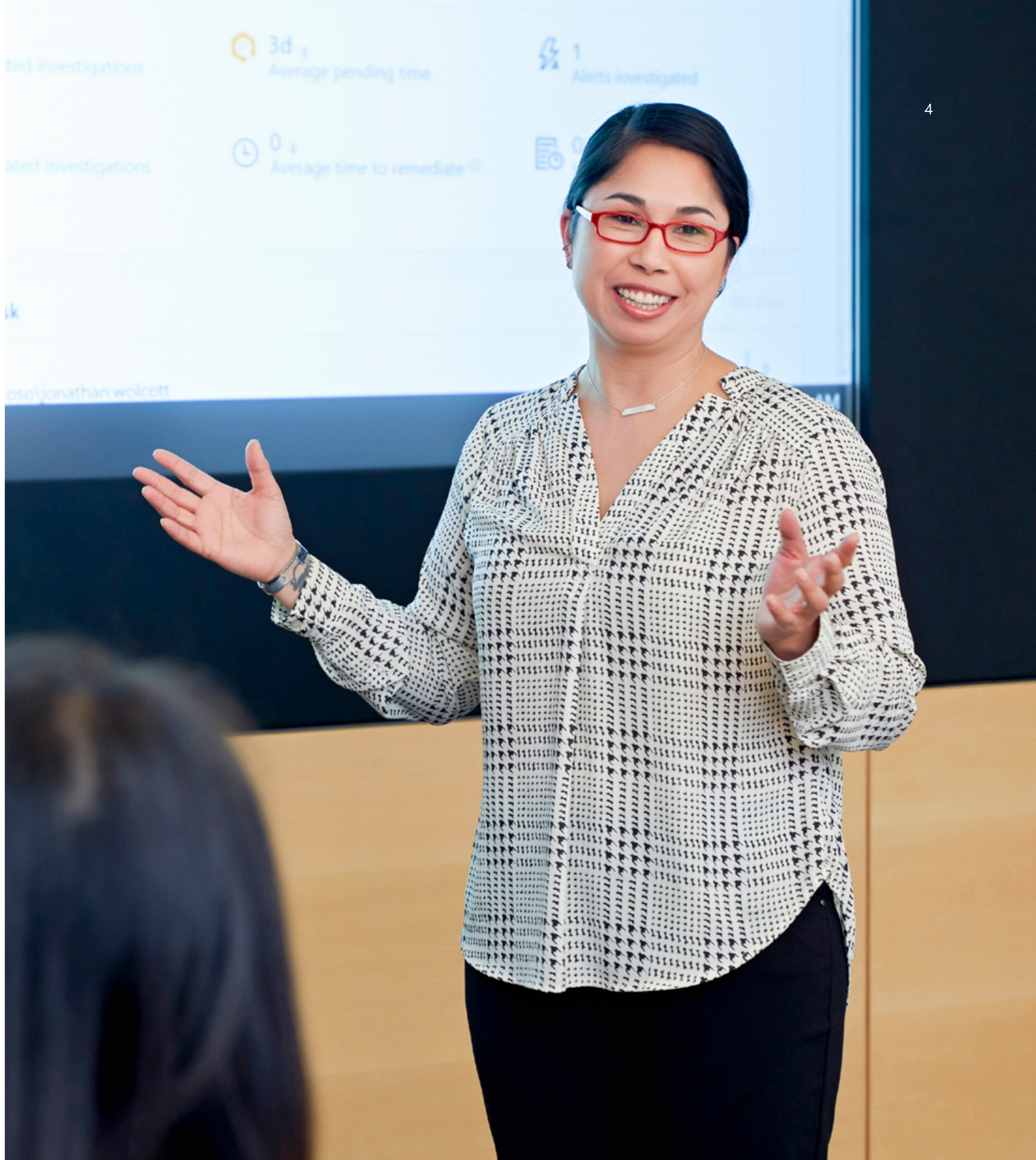
03

04

01

Establish your organization's operational baseline

You need a clear overview of what normal business activities look like across departments before you can recognize deviations that might signal threat behavior.



01

02

03

04

Deploy solutions for monitoring regular activity and correlating insights

Strong security requires strategic data analysis within the enterprise. To produce accurate and relevant threat intelligence, you'll need to collect behavioral and resource information from many internal sources, as well as from partners and customers.

Microsoft Security Intelligence Report

Explore real-world security data.

Read the report

Take a risk-focused approach, starting with your organization's critical assets and data, then expand outward.

Assess and report on current security posture using a risk assessment tool like Secure Score.

Monitor for and block malicious emails and attachments.

Think beyond network activity logs: an intelligent security information and event management solution, such as Microsoft Azure Sentinel, can correlate data from different sources and multiple cloud platforms, and alert your security team based on threat activity patterns you identify.

01

02

03

04

Identify the “normal” benchmarks of your organization

Use your collected data to develop insights about regular network, app, and device usage patterns. What are employees’ working hours and authentication habits? Which resources do different departments access frequently? Build operational models for departments, roles, and levels of privilege.

Microsoft Cloud App Security is easy to learn and use, and it unified our network access policies. Thirty minutes after we got the product, we were already auditing our third-party apps for the vulnerabilities we knew shadow IT introduced.

Charles Sims,
Head of Technology
Los Angeles Clippers

01

02

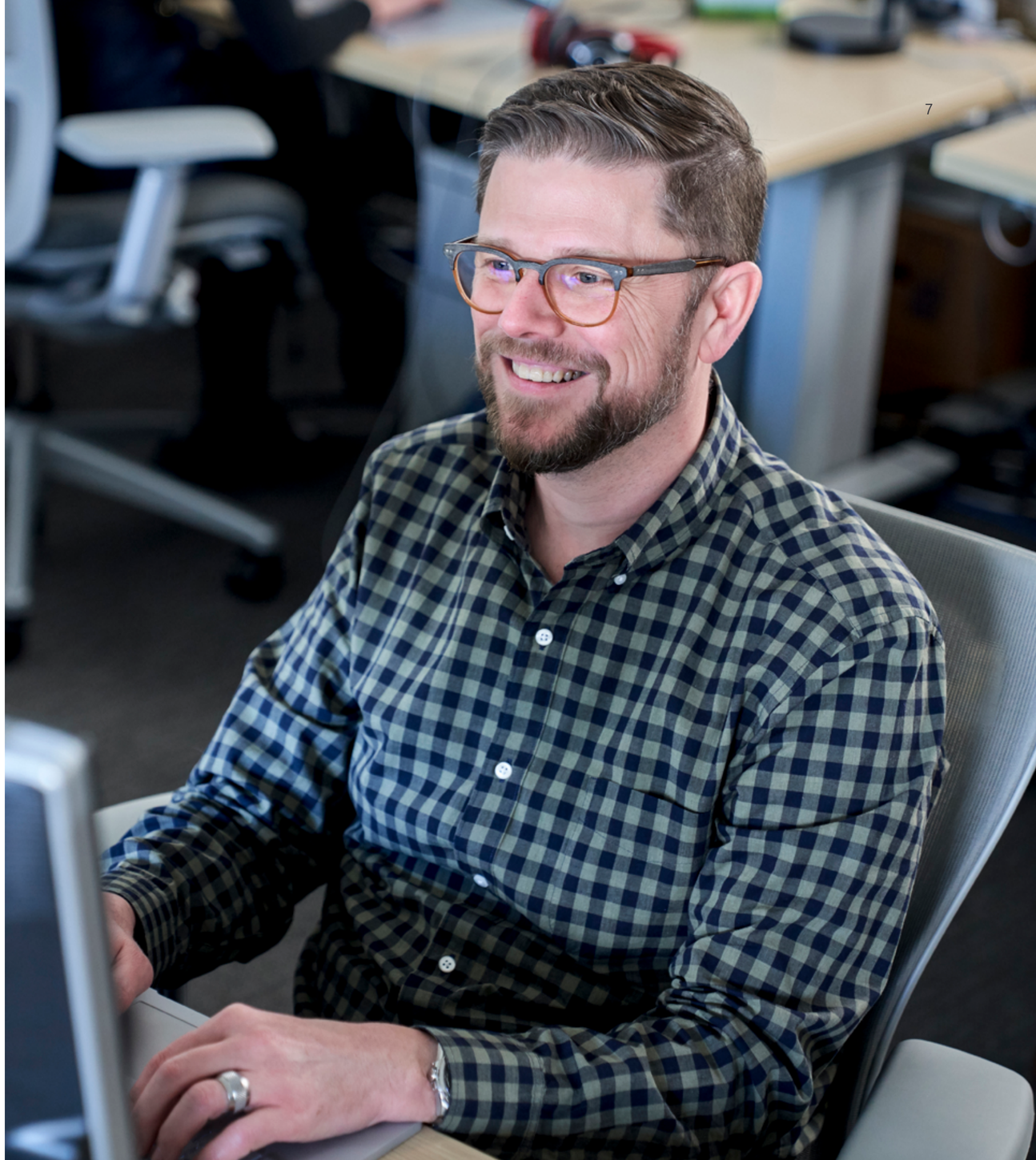
03

04

02

Minimize the cultural potential for mistakes

Understand and help mitigate the negative impacts that high-powered workspaces and always-on contexts have on your employees' ability to be strong defenders. Employees who are always juggling priorities and feeling pressure may be distracted and less likely to notice spear-phishing emails or tailgating strangers in the building. Worse, they may not care. Resentment or disaffection is a key risk factor for intentional insider threats.



01

Promote a human-oriented, rather than project-oriented, management style.

02

Engage employees in the planning and scheduling of their projects, and encourage them to contribute new ideas and problem-solving to benefit the whole organization.

03

Implement work policies and processes that focus on mission-oriented objectives.

Enforce separation of duties and least privilege for all employees, partners, and contractors to help limit damage from insider threat to critical processes, systems, and information.

04

NASA has a saying: “There’s no situation so bad that you cannot make it worse.” It’s a reminder to stay focused and work through problems rationally. Mistakes happen when people are distracted or panicked.

01

02

03

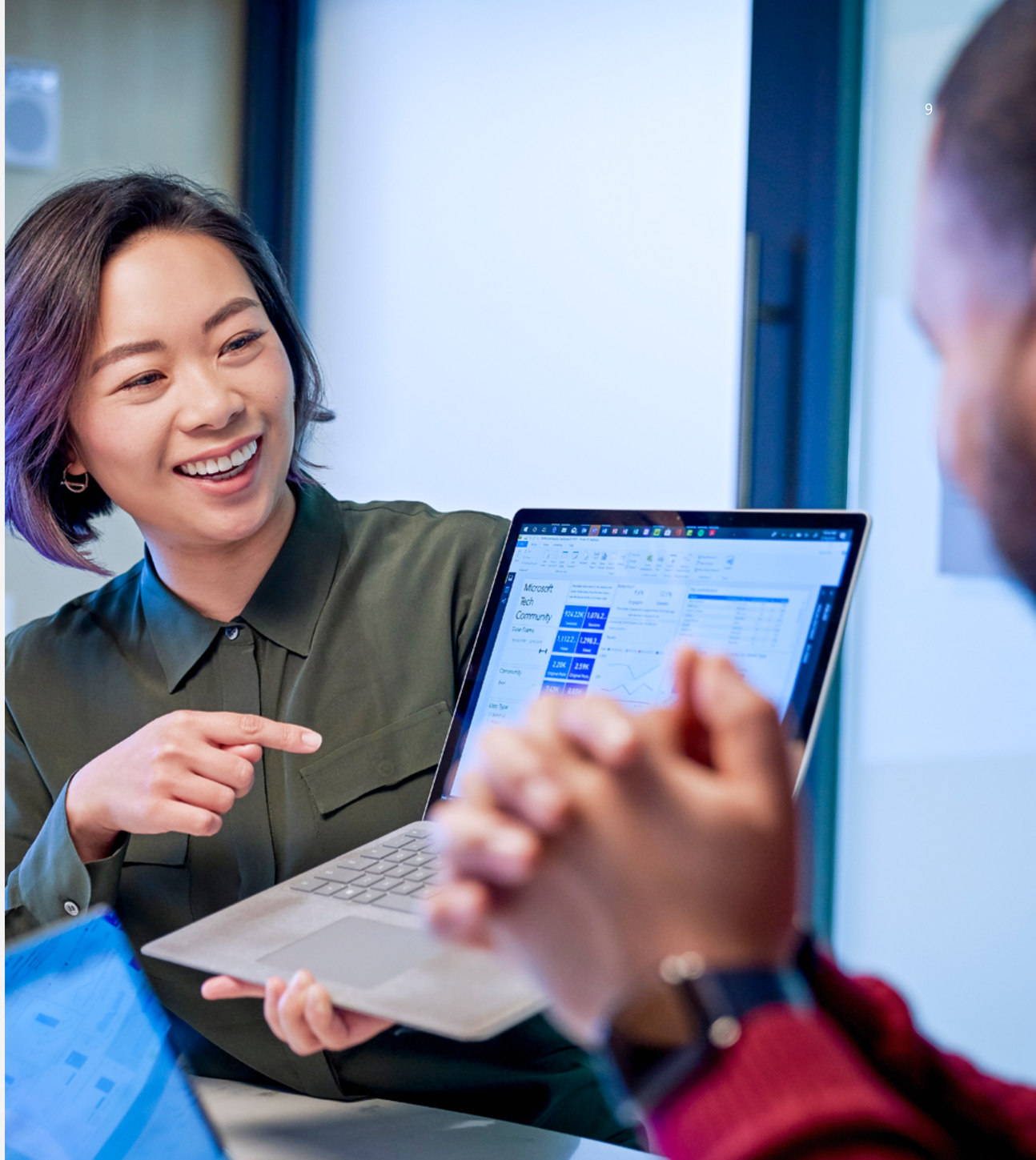
04

03

Use empowerment tactics to encourage adoption of technology best practices

Successful learning happens when students buy into why they are learning. Do your employees understand how technology best practices support them in their individual roles and departments? Are there ways to help them embrace a security-first mindset as a value-add in their careers, as well as for the company? A good security training program should make employees feel empowered and appreciated for their attention and compliance.

Charles Sims, the Head of Technology at the LA Clippers, empowered employees by letting them choose an authentication method that would allow them to maintain high productivity. Clippers staff can choose between using multifactor authentication or updating passwords more frequently. Employees pick the solution that fits their own work needs, which encourages better compliance.



01

02

03

04

For each security best practice, implement empowerment tactics

Institute strict password and account management policies...

Give people choices for implementing best practices. For example, offer an option to choose between multifactor authentication (MFA) or changing passwords frequently. Let employees select the type of MFA that suits their needs.

Implement or tighten access controls and monitoring policies.

Greater privilege demands greater accountability. Provide consistent, clear information about access rules so users—especially those with more privilege—don't feel hindered in their work.

Monitor employee actions and correlate data from multiple sources, especially systems and endpoints not managed by your organization.

Provide guidance so that users of technology not sanctioned by IT (such as online file sharing services, personal mobile devices, social media, and chat apps) feel empowered to make prudent choices.

Maintain a safe reporting system and escalation structure for insider threats and error handling.

Provide clear channels for users to report operating anomalies, suspicious activity, or unintentional human error. Ensure people know that such channels won't be used to punish or retaliate for mistakes.

01

02

03

04

04

Institute periodic “live” attack simulation and training

Consider integrating an attack simulation program into your risk management strategy. “Live” simulations, which mimic the unfolding complexities of an attack in real time, are a more engaging way for employees to practice being defenders, from the initiating event through detection, response, and remediation.

01

02

03

04

Commercially packaged simulations often aren't contextualized and immersive enough to make a simulated attack feel relevant to employees in a particular organization or industry. Most are phishing simulations that lack insider threat awareness and response-and-remediation practice. It's often hard for leadership to quantify the results of learning.

Effective attack simulation and training exercises are more like first-responder or military-style training. Your employees may not know exactly how or when a live-threat exercise will occur, but they'll be expected to work through the problems and practice different solutions with stable, thoughtful support from leadership.

01

02

03

04

Tips for better outcomes through simulation training:

Treat employees as your front line

Nobody wants to feel tricked into being a victim or unwitting perpetrator. During insider threat training, everyone should feel safe to admit that they clicked something they shouldn't have. Treat them as trustworthy, and make sure they can report a mistake to management without fear.

Provide means to escalate suspicions securely

In or out of training simulations, a centralized reporting mechanism is essential for the success of your human defense. Insiders reporting a suspected or recent attack must know who to report to, or what email alias or security webpage to contact. Whatever reporting system you use, be sure to provide up-to-date criteria for reporting as well as information about next steps and what employees can expect to happen next.

01

02

03

04

Customize training for contexts and roles

Identify the kinds of risks that different groups and privilege levels in your organization are likely to encounter. What systems or data present the greatest "ROI" to an infiltrator or saboteur? Consider tailoring the attack simulation so that experiences feel authentic.

Motivate through variety and challenge

To keep people engaged, you'll need to differentiate training over time. Set up simulation events for different kinds of response and remediation to different types of infiltration. Plan events that challenge employees progressively, but make sure they are contextualized, immersive, and short. Develop meaningful metrics so that they—and you—can judge progress.

Help employees go from hapless victim to hero

Use attack simulations to identify employees who show aptitude for security operations, and reward people for going above and beyond during the exercise. Some incentives are simple, like gamified badges or MVP rankings. Others could be more substantial, such as tapping high-value employees for greater responsibility and career growth.

01

02

03

04

CISO leadership is the key to reducing insider threats

Security awareness in an organization is always dynamic. Giving your employees reasons to believe they've got real skin in the game takes thoughtful change management and a multi-pronged, leadership-supported campaign.

The best practices and skills that employees adopt today will become outdated tomorrow; therefore—

- DO include simulation exercises that not only provide baseline and progressive measurements, but also reinforce desired behaviors.
- DO move toward dynamic, multi-touch training and knowledge reinforcement to build the skills that set up employees as strong defenders.
- DO weave security awareness messaging into corporate events and resources to help build the security-first mindset in your organization's culture.
- DON'T settle for the traditional, once-a-year compliance training model.

Remember, technology alone cannot replace the initiative of humans when it comes to defending the workspace. Reducing the chance of insider threats isn't easy, but think of your goal as the white hat version of social engineering—using education, motivational tactics, and technology best practices to turn vulnerable insiders into the informed and engaged workforce defending your digital estate.

Get up to speed on the top trends in the threat landscape.

Visit Microsoft Security

[1] Adapted in part from Common Sense Guide to Mitigating Insider Threats, Sixth Edition, Carnegie Mellon University Software Engineering Institute, 2019.