5 BEST PRACTICES TO SECURE YOUR HYBRID WORKFORCE

64% of IT decision makers indicated "improving data security" as their #1 objective related to IT investments in the next 12 months.[1]

Starting in 2020, companies across industries and the globe have transitioned employees into remote-work settings at unprecedented rates. By March 2020, nearly half of companies (47%) claimed they had transitioned at least half of their workforce, Forrester reports, with the possibility that "the pandemic will usher in a future with more flexibility for remote work."[2]

Indeed, experts agree that "hybrid workforces"—featuring at least some employees working and collaborating from remote work settings like home, at least some of the time—are becoming a new standard. But this presents entirely new sets of challenges for cybersecurity professionals, who must mitigate threats introduced by this transition. "Attackers seek to exploit the gaps opened when telecommuting employees use insecure devices and networks," McKinsey described in a July 2020 article. They also reported that Google tallied more than 18 million malware and phishing emails related to the coronavirus on its service each day in April.[3] As hybrid workforces continue to evolve cyber attacks will evolve as well, and enterprise IT leaders must stay vigilant.

Fortunately, new best practices that will help security experts protect their employees and their companies are now coming into focus. Rapid cloud migration, cloud-based security solutions and emphasizing cybersecurity awareness training for employees are among the most important ways to respond.

Employees must move beyond compliance and commit to changing their behaviors, with a newfound awareness for security risks and their own potential roles in attacks as well. In addition to implementing leading enterprise security solutions, getting everyone committed is a key element for making your cybersecurity program work.

THE STATE OF SECURITY IN HYBRID ENVIRONMENTS

Countless employees have had to adapt to remote work. For most, the transition has been a struggle—without a dedicated workspace or best practices for internet security at home, the rapid pace at which this transition took place had introduced unexpected, individual risks that can translate into threats to the enterprise.

Experts agree that "hybrid workforces" featuring some employees working and collaborating from remote settings are becoming a new standard.

RISKS TO YOUR ENTERPRISE

Phishing attempts have increased during the pandemic as employees take on new behaviors and fail to recognize bad actors playing off their anxieties and fears. Millions of new malware and phishing attempts arose playing off fears about the pandemic and workers' unfamiliarity with working from home.

While these threats emerge from criminal activity, the true risk lies in the new habits of your employees. Employees may not know how to use tools for remote collaboration safely. The vast majority of cybersecurity breaches are already the result of human error, where attacks that have cost companies millions of dollars to remediate often emerge from a single employee's mistake.

A NEW SECURITY PARADIGM

If your business is extending remote work opportunities, there is an impetus to train and prepare your hybrid workforce for longer term secure remote work. Doing so means moving beyond the infrequent and prescriptive security training of the past. Security training must truly reflect how employees work and learn today, inspiring them to commit to safety and actively adapt to threats through cultural changes in the enterprise.

5 BEST PRACTICES IN THIS NEW ENVIRONMENT

The most advanced protections and threat intelligence cannot protect against human error. **But you can make your employees part of the solution.** Hybrid security means a new underscoring of security's importance—but also, more regular and engaging trainings, and an enthusiastic commitment from employees to factor security into their daily decisions. Here's a closer look at five best practices that will put you on track to a more secure company in the future.

1. Gain support from company leadership

Your employees' habits will change only if your senior leadership prioritizes and articulates those changes. Building an enduring hybrid security program depends on senior leaders setting an example and rallying behind these new initiatives. Be sure your senior leaders are aware of the new imperatives and understand the core principles of your hybrid security initiatives as you begin.

2. Provide awareness training that actually makes a difference

Most companies provide only quarterly or annual training. Employees participate often begrudgingly, perceiving the training as a requirement they must temporarily endure. A slight cultural shift can help transition the preconceived thoughts and behaviors about enterprise security and can help employees understand the critical role they each play in protecting the network.

Your awareness training must engage employees, not simply "check a box" based on company requirements. It should be strategic, injecting humor and introducing use cases so that the lessons are more engaging and real to the individuals they seek to help. Your goal is to begin a virtuous cycle that helps employees change their behavior and reduce risk, even as new threats emerge.

3. Target Individual Employee Behavior

Remember, the vast majority of incidents occur because of a single or a small number of human errors. Making this clear to employees in cybersecurity trainings and communication makes these threats more "real" and gives you an opportunity to teach good security hygiene to employees. Transform the ways you and your employees approach key security areas by:

- Improving email security, helping employees recognize sketchy buttons and attachments
- Making each employee aware of popular attack methods, schemes, and sources
- Providing timely micro-trainings targeting the top threats of the day (consider using video for these updates to better engage your employees)
- Quizzing individual employees in a friendly way and honing in on areas for improvement

4. Transform your company's security culture

Longer term remote work is causing the lines to blur between home life and work life, but you can help steer good behaviors by embracing a new security culture. For example, countless employees are already using company devices for personal reasons in their homes. Many of them are using unapproved digital tools for productivity and collaboration, possibly on unsecured home networks that attackers are increasingly targeting.

Prepare your employees for frequent password updates and encourage them to use workplace devices strictly for work reasons, with only the apps and tools you provide. Your company leaders must listen to employees to learn what's working and what's not from an operational standpoint as well, with a vocal willingness to adapt to their needs.

As employees begin to understand what's at stake, they can change their attitudes and daily habits to drive lasting, positive change for the organization.

5. Adopt digital tools that will protect you long term

Remote work environments mean cloud-based security and applications are now critical parts of all enterprise security stacks. Start by re-evaluating your existing security applications. You will find that cloud adoption makes all your security controls—including network, email, endpoint, identity, access management, authentication, and others—"follow" remote employees wherever they go, rather than remain confined to an often irrelevant on-premises environment.

EVOLVED SECURITY FOR A NEXT-GENERATION WORKFORCE

Remember, the vast majority of attacks are avoidable through better employee habits, and you can empower your employees through continuous education. Transforming your company culture, securing commitments from employees, and transforming their behavior dramatically reduces risk in the future.

Your security tools needn't be your last line of defense, either. New security means automated methods for threat detection and prevention, including stopping threats at bottlenecks where employees are most likely to make that one egregious mistake. With the right approach, you can not only build a program around cybersecurity awareness, but protect your company and employees at every turn.

INTRODUCING MIMECAST

Mimecast helps companies protect their employees, intellectual property, customer data, and brand reputations by providing comprehensive, cloud-based security and compliance solutions that mitigate risk and reduce the cost and complexity of creating a cyber-resilient organization. It is an ideal option for hybrid workforces as they adapt to this new work paradigm.

TALK TO WEI TODAY

Contact WEI's security experts today to learn more about introducing Mimecast as part of your security improvement initiatives.

Sources:

1 IDG Research commissioned by WEI, January 2021.

2 "Managing The Risks Of The New Remote Workforce." Forrester blog, July 14, 2020. https://go.forrester.com/blogs/managing-the-risks-of-the-new-remote-workforce/

3 "A dual cybersecurity mindset for the next normal." McKinsey & Company, July 7, 2020. https://www.mckinsey.com/business-functions/risk/our-insights/a-dual-cybersecurity-mindset-for-the-next-normal

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 30 years.