SecurID™

Step by Step by Step by Step:

Managing Identity Risk in the Hybrid Workforce

The days of a workforce made up almost exclusively of full-time employees working on-site has given way to an era in which a hybrid workforce—on-site and remote, full-time and flexible, employed and contracted—is increasing flexibility and adaptability, but also introducing identity risk. Keeping risk in check in these circumstances requires a well-planned, methodical process for identifying and managing risk. Read on to learn about the four main steps to take to address new and evolving identity-related risk in the hybrid workforce.

Step 1

Increase Identity Assurance

Increasing your level of assurance about who is accessing systems and data is critical to managing the increased data security and privacy risk that comes with extending access to workers beyond traditional firewalls and perimeters.

Recommendations

- Rely less on passwords and more on multi-factor authentication or passwordless authentication.
- Prioritize highest-risk resources, such as VPNs, digital workspaces and SSO portals, for advanced authentication.
- Introduce conditional access policies that use contextual attributes.

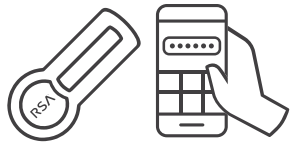
Take advantage of a constantly growing list of multi-factor authentication methods:

Push notification

One-time password

FIDO

Biometrics



Hardware and software tokens

Rely less on passwords and more on multi-factor authentication or passwordless authentication.

Step 2

Improve Access Governance

To manage access and compliance risk, you need increased governance over all the people who combine to create a revolving-door workplace of joiners, movers and leavers. Access governance ensures that they have what they need on the job—and that their access ends when they leave.

Recommendations

- Automate provisioning and de-provisioning to keep pace with the rate of change.
- Limit access to only those for whom it's essential.
- Avoid excess entitlements and accumulated access.
- Regularly perform access reviews and recertifications.

Today's workforce is much more than long-term, full-time, on-site workers—including:

- Remote workers
- Freelancers
- Gig workers
- Temporary staff
- Seasonal help

Access governance ensures that people have what they need on the job—and that their access ends when they leave.

Step 3

Manage Insider Threats and Digital Workers

Whether the result of user negligence or intentional abuse, insider threats have long represented a security challenge—made even tougher by the complexities of a hybrid workforce. Minimizing insider threats requires building on a strong foundation of identity and access management with advanced analytics.

Recommendations

- Use identity analytics to continuously detect anomalies and toxic combinations of access.
- Consider augmenting static-based authentication rules with self-learning, context-based rules.
- Apply user behavior analytics to monitor user activity and quickly spot problems.

Insiders aren't the only ones who can contribute to identity risk. Digital workers (bots, AI, IoT, robotics), in the wrong hands, can be used to wreak havoc. Close control over who manages and updates them is critical.

- Gain fine-grained visibility into digital workers' entitlements and interactions.
- Develop resiliency plans to prevent disruptions as more nonhuman workers perform critical functions.
- Carefully manage routine events like pricing changes and system updates, which can interfere with automated processes.

Close control over who manages and updates bots and other digital workers is critical.

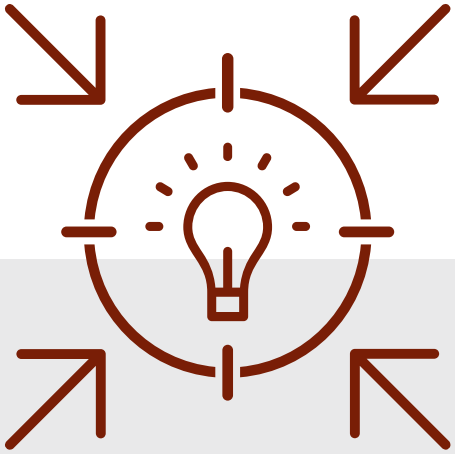
Step 4

Build a Human Firewall

Though not intentionally, workers will inevitably misuse resources, mishandle sensitive data and violate acceptable use policies. A variety of security tools can help contain actions of this kind that put organizations at increased risk. And expanding efforts beyond just technology is vital too.

Recommendations

- Mix and match animated, instructor-led simulations and gamification to custom-fit workers.
- Take a top-down approach. Changing the security culture doesn't happen overnight; it requires everyone to be all-in.
- Establish baselines for worker cybersecurity knowledge and susceptibility to social engineering attacks.
- Continually train, assess and communicate findings.
- Find ways to make security awareness valuable for workers, including incentives and positive reinforcement.



Take a top-down approach. Changing the security culture doesn't happen overnight; it requires everyone to be all-in.

The Future of Workforce Risk

While it's nearly impossible to predict how change and disruption will specifically impact the workforce, it's reasonable to assume they will continue to create a variety of new and intensified risks. Therefore, the most important next step is to undertake planning and action that will prepare your organization for whatever the future holds. Follow the recommendations in this guide to help minimize impacts to the workforce and remain resilient as the future unfolds.

Learn more about how **identity and access management for the hybrid workforce** can help you manage workforce risk.

About SecurID

SecurID, an RSA business, is the trusted identity platform for 13,000 organizations around the world, managing 50 million identities and providing secure, convenient access to 30 million users. SecurID empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, SecurID connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to **securid.com**.

SecurID™
An RSA Business