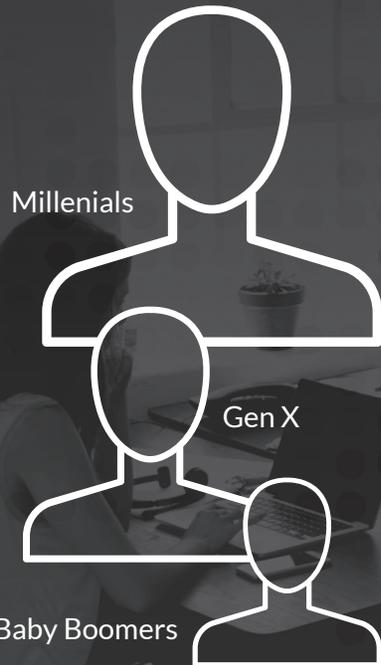


RSA®



3 KEYS TO MANAGING DYNAMIC WORKFORCE RISK

THE DRIVERS OF WORKFORCE TRANSFORMATION



The face of today's workforce is undergoing profound changes sparked by shifting demographics, digital transformation, globalization, and the immutable truth that the ways we connect to information and to each other will continually evolve.

Shifting Demographics

Your organization's workforce likely includes Baby Boomers, Gen Xers and millennials working in full-time, part-time, temporary and contract positions. Each of these groups has different attitudes toward employment and preferences about how and where they do their work that employers must try to support.

Digital Transformation

There's no denying the fact that work has become more automated, more digital and more mobile, and today's digital transformation initiatives are only accelerating this trend. Meanwhile, new technologies, like easy-to-use, personalized digital workspaces, give employees the freedom to collaborate anywhere their jobs take them.

Globalization

The workforce isn't just shaped by shifting demographics and changes in technology. Globalization continues to have a far-reaching impact, too. Organizations continue to expand their operations around the world, whether to serve new markets, tap into burgeoning talent pools, or source new materials and suppliers for their products.

WORKFORCE TRANSFORMATION BRINGS NEW RISKS

PCI
PIPEDA | ISO
GDPR
NIST | HIPAA
NERC

As companies adjust their workforces to compete more effectively in today's market, these changes create a number of risks:

A Revolving Door of Workers

Companies are increasingly turning to “gig” or freelance workers to gain hard-to-find skills and staff for short-term projects. Bringing on board more of these gig workers generates a revolving door of “joiners, movers and leavers” for IT departments to manage. If their access is not managed diligently throughout their employment lifecycle, they could gain excess privileges leading to compliance violations or insider threats.

An Expanding Attack Surface

The employee-led BYOD and consumerization of IT movements have wreaked havoc on security. The cloud applications and mobile devices that have subsequently flooded the workplace have given bad actors more vulnerabilities to exploit and more ways to evade detection. Meanwhile, these technologies often have conflicting requirements for security, support and the user experience, making them harder for IT organizations to manage.

Regional Differences

Organizations that “go global” need to address regional variations in workers’ attitudes toward handling sensitive data. The more regions in which a company operates, the more technologies it likely must assimilate into its IT infrastructure and the more privacy and security regulations it likely needs to harmonize.

WORKFORCES GONE WILD

How do these workforce risks materialize across your organization? Dell conducted a survey and found that 45 percent of respondents admitted to engaging in at least one of the following unsafe behaviors at work:



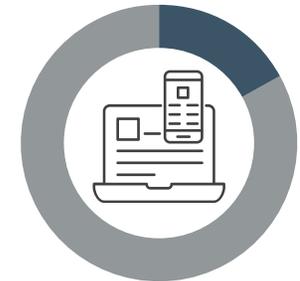
46%

Using public (open) Wi-Fi to connect to company recourses.



49%

Sharing confidential data via personal email accounts.

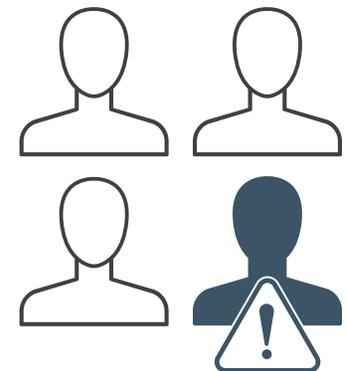


17%

Losing devices, like laptops and phones, with company information on them.

Perhaps even more telling: Nearly 1 in 4 respondents said they engaged in unsafe behavior simply to get their job done, while 18 percent revealed they didn't know their actions were risky.

Although cybersecurity training is extremely important to any digital risk management program, organizations cannot rely on their workforce to always do what's in the best interest of the company.



GETTING YOUR ARMS AROUND DYNAMIC WORKFORCE RISK

The dynamic workforce has become an increasingly complex challenge for cybersecurity and risk management practitioners to address.

The more people accessing your systems and data, the more identities you need to manage, and the greater the odds that one (or more) of these identities will be abused or compromised, potentially leading to a security breach or hefty fines from compliance violations.

To manage dynamic workforce risk, organizations must have the following three key capabilities in place:



Identity assurance: Verify that users (and entities) are who they claim to be with frictionless, risk-based authentication that works across different computing platforms and environments.



Access assurance: Get a complete picture of the resources to which each user has access. Understand what users can do with their access and how any related access risks may impact security and compliance.



Activity assurance: Gain insight into what users are doing once they're logged into resources to determine whether their activity is appropriate or to spot abnormal behaviors that could signal compromised credentials and insider threats.

CAN YOU ANSWER THESE CRITICAL QUESTIONS?

With those three capabilities in place—identity assurance, access assurance and activity assurance—you'll be able to answer the following questions, indicating that your organization is well on its way to managing dynamic workforce risk:



RSA HELPS YOU MANAGE YOUR DYNAMIC WORKFORCE RISK

Only RSA has the people, the technology, the experience, the partnerships and the vision to help organizations manage dynamic workforce risk. We enable your diverse and mobile workforce to do more by giving them the freedom to securely work wherever, whenever and however they choose.

HOW WE HELP

ACCESS ASSURANCE

- Identity, Governance & Lifecycle Management
- Access Policy Violation Detection
- Risk-Based Access Reviews
- Regulatory Compliance Reporting

RSA
SECURID®
SUITE

IDENTITY ASSURANCE

- Multi-Factor Authentication
- Risk-Based Authentication
- Machine Learning Identity Confidence
- Authentication Assurance Levels

RSA
SECURID®
SUITE

ACTIVITY ASSURANCE

- Security Monitoring
- Endpoint Detection & Response
- UEBA
- Orchestration & Automation

RSA
NETWITNESS®
PLATFORM

RSA DYNAMIC WORKFORCE RISK FRAMEWORK

- Cybersecurity Advisory Services
- Maturity Assessment
- Benchmark Report
- Roadmap

RSA
RISK & CYBER
SECURITY PRACTICE

Review other resources that will help you take the next step toward managing your dynamic workforce risks. RSA – [Manage Dynamic Workforce Risk](#)



DIGITAL RISK IS EVERYONE'S BUSINESS HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at [rsa.com](https://www.rsa.com)

RSA[®]

© 2019 Dell Inc. or its subsidiaries. All Rights Reserved. RSA and the RSA logo are trademarks of Dell Inc. or its subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. Published in the USA, 5/19 eBook H17724 W233085