Shifting demographics and digital transformation drive the risk associated with today’s dynamic workforce.

Gallup estimates nearly one in three U.S. workers already participates in the gig economy in some capacity. These transient workers create a revolving door of joiners, movers and leavers for IT and IAM teams to manage—and they generate access management, compliance and insider-threat risks. At the same time, organizations are rapidly adopting cloud, mobile, internet of things (IoT) and artificial intelligence (AI) technologies. This gives bad actors an exponentially larger attack surface to exploit.

What’s needed is an approach to managing the risk that couples strong protection for the organization with less friction for the workforce. This can make it possible for teams to pursue innovation freely, without being held back by the need for security.
Managing today’s workforce-related challenges requires a comprehensive security and risk management approach that includes capabilities to meet the following objectives:

- Establish strong user identities and associated access policies.
- Assign user access rights and permissions based on roles and responsibilities.
- Authenticate workers with a high level of assurance and minimal friction.
- Continuously monitor user and entity behavior for anomalous activity.
- Evaluate the business impact of digital risks to prioritize resulting actions.
- Automate and orchestrate response to ongoing cyber threats.
- Regularly adapt policies and controls based on changing needs and observed behaviors.

Since the workforce and the technologies they use are continually evolving, two things are critical to supporting the changing needs of the business: knowing how your capabilities measure up to industry standards, and knowing which investments to make to at least be on par with those standards. This requires evaluation of dynamic workforce risk through the lens of a maturity model that analyzes five key domains: governance, identity, privacy, data and systems.

**HOW DO YOUR CAPABILITIES COMPARE WITH INDUSTRY STANDARDS?**

Evaluating your capabilities for managing dynamic workforce risk and gauging how they stack up against industry standards are important steps in ensuring those capabilities support your organization’s needs in this area.
When it comes to managing digital risk associated with a dynamic workforce, organizations need a sound game plan for how staff, business units, IT personnel and executives will protect sensitive information, critical resources and the organization's reputation.

Here are some key governance controls that will aid in the ongoing process of integrating policies, processes, procedures and tools for managing dynamic workforce risk:

1. Define cybersecurity roles and responsibilities for the entire workforce, including employees, independent contractors and temporary workers.
2. Perform background checks that include criminal and credit records, professional/academic references and drug screenings.
3. Create acceptable-use policies and security configuration requirements (authentication, data encryption, etc.) for mobile devices (including BYOD) and removable media.
4. Establish policies and controls for remote, office-based, temporary and hybrid workers.
5. Prioritize resources (e.g., hardware, devices, data, time, personnel and software) based on classification, criticality and business value.
A defensive approach that relies on passwords and static rules is no match for a revolving-door workplace and an ever-expanding cloud-and-mobile attack surface. As organizations become increasingly connected, there must be a high level of assurance users are who they say they are, their access is in line with their responsibilities, and what they are doing with that access is appropriate and doesn’t put the business in harm’s way.

While managing workforce risk has historically revolved around traditional identity and access management tools, today’s digital realities require organizations to go well beyond those basic controls:

- Govern joiner/mover/leaver access rights, and manage credentials and entitlements for authorized devices and processes.
- Apply the principles of least privilege and segregation of duties when granting permissions and authorizations.
- Authenticate (e.g., single-factor, multi-factor) users, devices and other assets commensurate with risk.
- Correlate data across systems to understand the potential security and business risks associated with authenticating users and assigning access rights.
- Continuously monitor user behavior and activity related to connections, devices and software.
- Adapt policies and controls based on changing workforce needs and observed behaviors.
Data is the fuel powering today’s digital economy. IDC predicts there will be 500 million new logical applications created in the five years from 2018 to 2023, which is as many applications as were built over the previous 40 years. And a recent Dell study found that in 2018, organizations handled an average of 9.7 petabytes of data. That’s the equivalent of 9.7 million gigabytes—a lot of emails, files, tweets and videos. The sheer amount of data makes securing it complex. Data security requires organizations understand the data itself, how it’s created and used, and what impact it may have on corporate governance.

In addition to the identity-related controls on the previous page, the following data security controls will help limit the risk to data posed by a dynamic workforce:

- Identify and classify sensitive structured and unstructured data sets according to their business risk, across all compute environments.
- Secure sensitive data in transit between applications and systems, and at rest within mobile devices, databases, storage and backups.
- Assess the potential risks (likelihood and impact) associated with identified data security threats and vulnerabilities.
- Prioritize data security controls and risk mitigation actions based on which risks pose the greatest measurable impact to the business.
- Automate and orchestrate policies across data security tools, and adapt rules and controls based on changing workforce needs and observed behaviors.
While data privacy and data security are deeply entwined, understanding their fundamental differences is key to meeting both the need to secure operations and the need to manage privacy risk. As we’ve seen in the previous section, data security is about employing technologies and tools to protect data against unauthorized access. Data privacy, on the other hand, is about an individual’s right to have their personal information kept private. Technology alone cannot ensure that personally identifiable information (PII) will stay private, since PII remains vulnerable to intentional or accidental leakage by those with authorized access. As a result, data privacy is much more about the rule of law than it is about the latest technology.

In addition to the data security controls set forth in the previous section, implementing the following data privacy practices will help organizations comply with regulations and limit the risk posed by a dynamic workforce:

- **Ensure PII can be deleted or returned within 72 hours of a request.**
- **Continuously monitor and assess third-party data usage to ensure adherence to regulatory and corporate privacy standards.**
- **Regularly inform employees and customers about data collection practices and the specific data collected about them.**
- **Periodically train employees and third parties on data-handling codes of conduct, information security and data privacy regulations, and their respective responsibilities.**
Systems essentially equate to endpoints—the computers, phones, tablets and other network-enabled devices used daily. According to a recent SANS survey, nearly half of organizations today are managing between 5,000 and 500,000 endpoints. Managing the risks associated with a dynamic workforce requires organizations to protect or, in essence, “lock down” all these endpoints, to ensure their integrity and availability. Endpoint protection once meant little more than host-based firewalls and antivirus software. Today, however, endpoint detection and response (EDR) solutions have evolved to incorporate AI, cloud and mobile technologies, to both dynamically detect threats and respond to them in real time.

As devices increasingly act on their own, or on behalf of their users, organizations must be able to directly trust endpoints. Incorporating the following system-level protections will help extend trust to endpoints and limit the risk posed by a dynamic workforce:

- Periodically perform risk assessments and pen testing against critical servers and endpoints.
- Logically segment systems and networks to maintain minimal access rules and minimize lateral movement by users.
- Employ tools to discover endpoint changes, detect anomalous user and entity behavior, and track how these events are processed.
- Implement security controls to disallow communication programs (email, instant messaging, etc.) from storing, transmitting or propagating malicious code.
- Protect endpoint systems against malware, spyware and malicious mobile code, as well as from physical theft.
Successfully managing dynamic workforce risk starts with a comprehensive assessment that gauges an organization’s ability to identify, protect, detect and respond to workforce-related risks. RSA offers a comprehensive assessment that is grounded in our proprietary RSA Risk Frameworks, a set of professional services leveraging more than 30 years of RSA security and risk expertise.

The RSA Risk Framework for Dynamic Workforce Risk is based on industry-standard guidelines (including the NIST Cybersecurity Framework and ISO standards for cybersecurity and risk management) and uses a model that measures leading indicators of maturity across the five areas of dynamic workforce risk described in this e-book: governance, identity, privacy, data and systems. A detailed scoring system for these categories enables organizations to assess capabilities for each area and baseline an initial score. The results can be used to prioritize investments and adjust dynamic workforce risk management strategy to meet the organization’s risk tolerance and the changing needs of the business.
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

1. The Gig Economy and Alternative Work Arrangements, Gallup, 2018
2. IDC FutureScape: Worldwide IT Industry 2019 Predictions, IDC, October 2018
3. Dell EMC Global Data Protection Index, Dell Technologies, 2018
4. Endpoint Protection and Response: A SANS Survey, SANS Institute, 2018

© 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, 8/19 eBook H17868 W269016