THE 5 FACES OF DYNAMIC WORKFORCE RISK
If your organization’s workforce is like most today, it’s made up of full-timers, part-timers and contract workers who are constantly coming and going, working across a multitude of locations, and connecting from wherever they are to whatever resources they need through a variety of digital technologies.

It sounds like a lot—and it is. Organizations are dealing with more people, places and devices in the workforce than ever before, which means an expanded attack surface, increased insider and third-party risk, and a greater challenge to comply with regulations for keeping data private and secure.

But if you understand the different types of users and potential risks they represent, you can turn a security liability into a competitive advantage: a dynamic workforce that makes your organization more agile, productive and efficient, and less at risk.

Ready to get started? Read on to get to know the five faces of dynamic workforce risk.
“Hey, I know! If I send this strategy doc to my personal email, I can download it and work on it at home tonight.” Great plan—for someone who wants to run the risk of accidentally leaking critical, confidential data to cyber thieves. Of course, that’s not what careless co-workers set out to do; often, they just don’t realize they’re putting their organization’s data at risk by using personal email accounts, or connecting to public Wi-Fi or posting sensitive files to external shared drives. There are plenty of ways to carelessly compromise sensitive information, and plenty of people do it. Fortunately, there are also plenty of ways to manage the risk, from educating workers about how to recognize phishing threats to monitoring user and device access more closely.

#1
THE CARELESS CO-WORKER

49% of employees report they use personal email accounts for work

46% of employees say they connect to public Wi-Fi to access confidential information

Source: Dell End-User Security Survey 2017
Did you hear the one about the luxury carmaker’s employee who was so mad about being reassigned, he allegedly dumped proprietary data to a competitor for a month before he got caught? No? How about the one about the transportation industry sysadmin who got fired and locked the IT staff out of the network on his way out? It’s no joke: According to the 2018 U.S. State of Cybercrime Study, 25% of cyber attacks were caused by insiders. Not all those insiders are acting maliciously, of course, but some do have an ax to grind. And while you can’t stop malicious insiders from trying to cause harm, you can do a lot to keep them from succeeding. A comprehensive insider threat program that combines continuous monitoring of user and entity behavior, rapid threat detection, and robust threat response capabilities will help prevent or limit the damage a disgruntled employee can wreak.

#2
THE DISGRUNTLED EMPLOYEE

92% of insider threats are preceded by a negative work event

59% of employees who leave an organization say they take sensitive data with them

Unlike a careless co-worker or a disgruntled employee, the malicious imposter isn't someone inside your organization. It just looks that way, because they're using stolen credentials to pose as a legitimate member of the workforce. And the more diverse and distributed that workforce is, the more opportunities for cybercriminals to steal credentials—whether to use themselves, or to sell to other bad actors. From there, it’s an easy path to intellectual property, employee personal information (Social Security Numbers!), customer credit card numbers… it all depends on whose credentials they’re using and what those credentials provide access to. That’s why it’s so important to adopt technology that enables you to know who users are, what they have access to and what they do with that access.

69% of data breaches are perpetrated by outsiders

2.2 billion usernames and passwords are freely distributed on the dark web

Source: Verizon Data Breach Investigations Report 2019
Source: Wired, January 2019
Today, the people with access to your organization’s resources are as likely to be contract workers and vendors as they are to be full-time employees. That can help make the organization nimbler and more flexible. But it can also create risk. Just ask the retail giant that got hacked through a mechanical contractor’s poorly secured connection, resulting in 40 million credit and debit card numbers stolen. The problem is growing worse as organizations increase dependence on third parties (and on the third parties’ third parties) in the digital world. This is a good reminder of the importance of a deep understanding of who these “Nth” parties are, the nature of their relationships with the organization and with their own third parties, and the risks those relationships pose. That requires a robust set of capabilities for managing risk through the full lifecycle of each third-party relationship—including the ability to administer access entitlements, continuously measure risk and implement risk treatments.

---

**#4 THE NEGLIGENT NTH PARTY**

- **57 million**
  - U.S. workers participate in the gig economy in some capacity
  - Source: *The Gig Economy and Alternative Work Arrangements*, Gallup, 2018

- **59%**
  - U.S. and U.K. data breaches in 2018 were caused by a third party
  - Source: *Data Risk in the Third-Party Ecosystem*, Opus and Ponemon Institute, 2018
It's remarkably easy to get someone to spy on an organization, and harder than you might think to catch them. Recruited by cybercriminals or foreign agents to steal data or make data systems more vulnerable, corporate spies often arrive in the guise of interns or students, or assume other seemingly harmless roles. Once they're in, they can do a lot of financial and reputational damage in a short time. The best way to deal with this risk is to use preventative measures to make it harder for an insider to commit cybercrime in the first place; the next best way is to respond to this type of attack quickly enough to limit the harm. A combination of detection controls, asset monitoring and access analytics increases the odds of turning the tables on those hoping to benefit themselves at your organization's expense.

45% increase in US District Court economic espionage cases 2014-2019

$600 billion estimated cost to the U.S. economy of theft through economic espionage

Source: Stolen Secrets: With Economic Espionage on the Rise, Silicon Valley Must Better Protect Secrets, NBC Bay Area, February 13, 2019

Source: Update to the IP Commission Report, 2017
RSA can help you manage dynamic workforce risk, by enabling your organization’s users to work wherever, whenever and however they choose—without compromising security. Turn to RSA for comprehensive capabilities including:

- Risk-based multi-factor authentication to ensure users are who they say they are
- Automated identity governance for a growing, constantly changing workforce population
- Threat visibility across logs, networks, endpoints and clouds
- Real-time cyber threat detection and response, including UEBA, orchestration and automation
- Real-time correlation of identity and access data with threat analytics
- Third-party risk management of contractors, supply chain and service providers
- Policy governance including full oversight of regulatory compliance obligations
- Advisory services to assess and benchmark dynamic risk management maturity and develop a roadmap to guide next steps

Learn more about how RSA helps 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