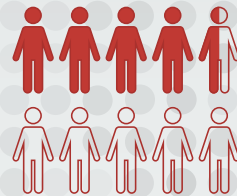# RSA®

THE 5 FACES OF
DYNAMIC WORKFORCE RISK

Dynamic workforce risk refers to the security, privacy and compliance issues that stem from employing a diverse and distributed workforce made up of full-time, part-time, contract and third-party resources—all connected through an expanding array of digital technologies. To help you understand this new concept, we've personified it. Get to know the following five faces of dynamic workforce risk. We're sure you'll recognize many of them.

THE CARELESS CO-WORKER
unintentionally misuses resources, mishandles sensitive data, and otherwise mindlessly violates acceptable use policies.

45% OF EMPLOYEES **admit to engaging in** UNSAFE BEHAVIORS throughout the workday[1]

THE DISGRUNTLED EMPLOYEE
intentionally seeks to disrupt or damage his/her employer's business or advance their personal agenda by stealing confidential information.

92% of INSIDER THREAT CASES were preceded by a NEGATIVE WORK EVENT (such as a termination, demotion or dispute with a supervisor[2])

THE MALICIOUS IMPOSTER
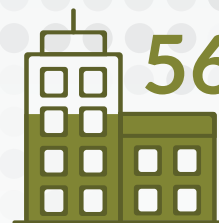exploits compromised credentials or other techniques to gain unauthorized access to systems and data.

2.2 BILLION unique USERNAMES & ASSOCIATED PASSWORDS are freely DISTRIBUTED ON THE DARK WEB

THE NEGLIGENT Nᵀᴴ PARTY
unintentionally compromises security by misusing partner resources, mishandling sensitive data, or exposing weak security practices.

56% of organizations say they've EXPERIENCED A DATA BREACH or cyber attack caused by a THIRD PARTY[4]

THE DOUBLE AGENT
is recruited and paid by external threat actors to steal data or make systems more vulnerable.

20% of DATA BREACHES in 2017 were motivated by CYBER ESPIONAGE[5]

Need help managing the risks associated with your dynamic workforce?
Visit us at rsa.com/en-us/solutions.

1. Dell, "Dell End User Security Survey 2017," https://datasecurity.dell.com/wp-content/uploads/2017/09/Dell-End-User-Security-Survey-2017.pdf; 2. Deloitte, "Insider Threats: What Every Government Agency Should Know," https://deloitte.wsj.com/cio/files/2016/04/2688954-Insider-Threat_4.pdf, March 2016; 3. Andy Greenberg, "Hackers Are Passing Around a Megaleak of 2.2 Billion Records," Wired, https://www.wired.com/story/collection-leak-usernames-passwords-billions/, January 30, 2019; 4. Ponemon Institute, "Data Risk in the Third-Party Ecosystem" (2017); 5. Verizon, "2018 Data Breach Investigations Report," p.6