RSA

20 Predictions for 2020

Preparing for the Future of Digital Risk

If the past decade has taught us anything, it's that change is a constant.

Fueled by technological innovation and digital transformation, our world is evolving and changing more quickly than ever—and that includes unprecedented digital risk.

What changes can you expect in 2020?

We've outlined RSA's top 20 predictions for the security and risk industry with a focus on the elements of digital risk that will shape the future of your business.

Read on for the challenges and threats most likely to affect organizations, governments and individuals over the next year and beyond.

#1

The rise of the cyber-savvy board

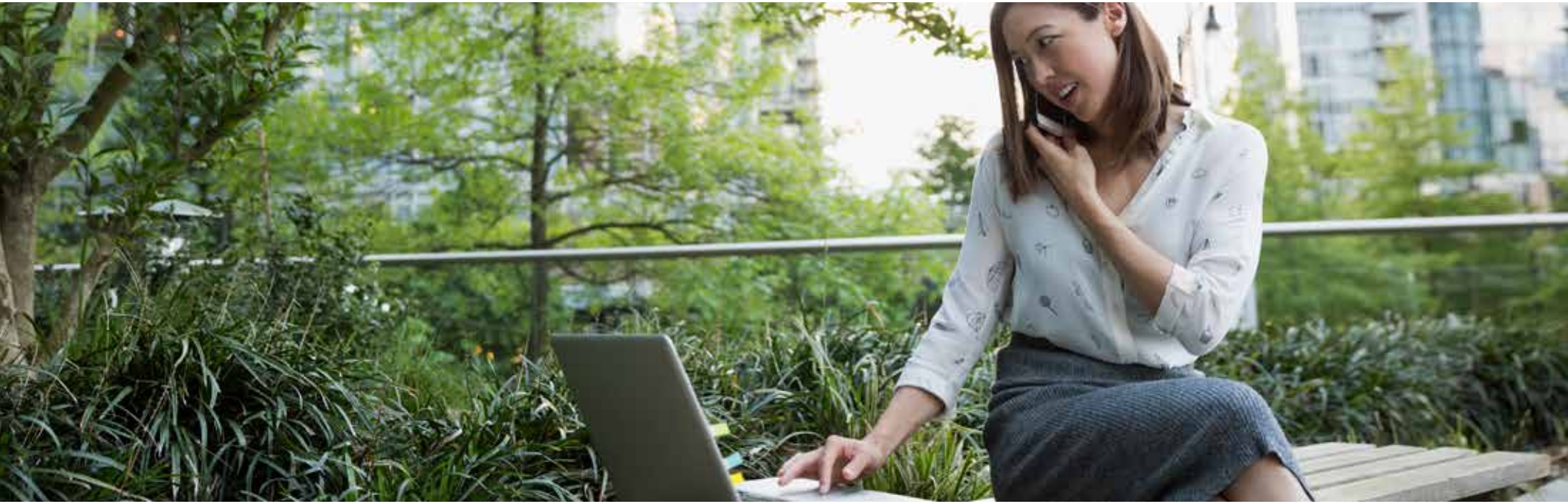
Accountability for cyber risk will move up the org chart, with forward-thinking businesses appointing board members with experience in risk management and information security. Over time, investors will further elevate the need for clear digital risk management strategies, and such board expertise will become the new normal.

What risk factors will threaten your success in 2020?

Assess your digital risk exposure with the RSA Digital Risk Index.

#2 Authentication demands adapt to evolving needs

Despite a growing list of options, there is still no one-size-fits-all solution for identity and access management. Better buyer support and more decision-making guides will help businesses looking to strike a balance between security and user experience.



#3

A focus on data sovereignty in the Middle East

As Turkish, Middle Eastern and North African businesses rush to the cloud, countries will demand that data centers be established within their borders. Major technology providers will feel the pressure, and invest more heavily in the region.

#4 Brexit brings new risk assessments

With the UK's exit from the E.U. looming, businesses must reevaluate their risk assessment—including identifying and mitigating Brexit-associated cyber threats.

#5 Security shifts left

Increasing demand for cloud-native apps will force security teams to work more closely with DevOps. Moving pentesting and code analysis up in the development lifecycle will boost product security. But security teams will need to communicate with developers in a language they understand—for example, referencing delays and unplanned work instead of talking about vulnerabilities.

3.5 MILLION
cybersecurity jobs
will go unfilled around the world by 2021.[2]

#6

Technology helps close the skills gap

Even with the best tools, processes and budget, a lack of talent makes it hard to manage cyber risk—and more than half of companies surveyed report a "problematic shortage" of cybersecurity skills.[1] Businesses will look to reduce dependency on talent via security orchestration and automation software, risk-based prioritization, and comprehensive threat analytics.

RSA partners with local governments and universities across the Asia-Pacific region to train the **next generation of cybersecurity talent.**[3]

#7

A.I.'s black box opens a crack

Artificial intelligence (AI) will evolve to a point where recommendations based on its analysis can be more readily understood—even by those without technical skills.

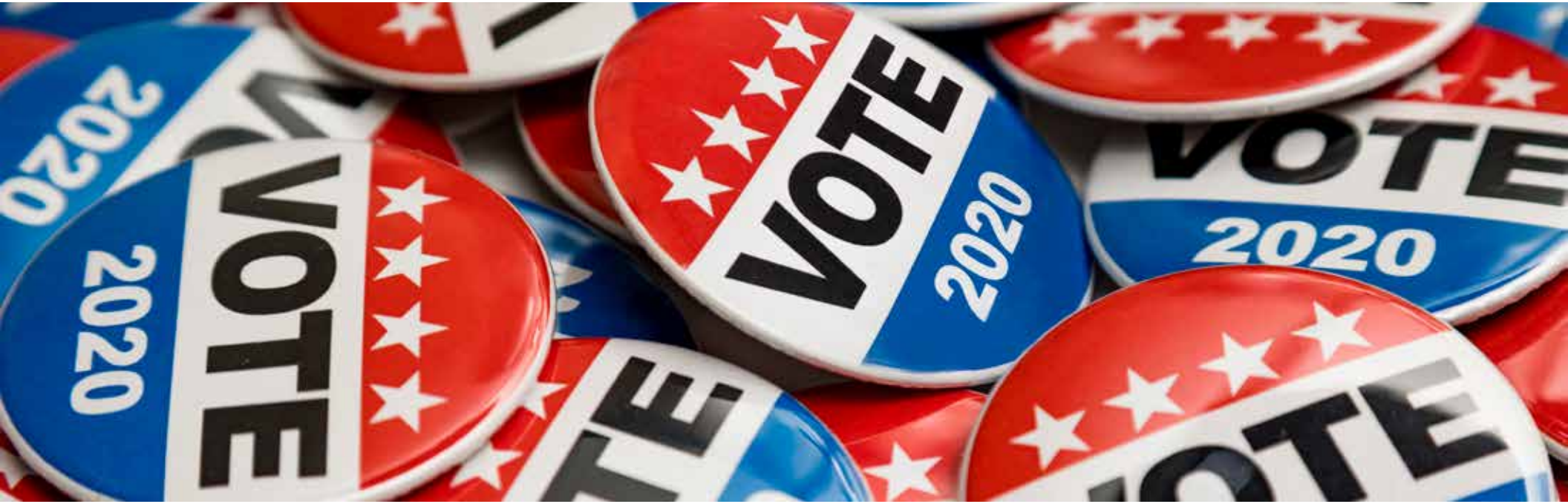
$30.9 BILLION
will be spent on AI-based cybersecurity systems and services by 2025.[4]

#8 Legacy systems under the microscope

Many businesses operate on a fragile network of legacy systems, stitched together with API connections. The stage is set for a security incident that disrupts this patchwork, triggering major outages and serving as a wake-up call to evaluate legacy system security.

#9 Cybersecurity and democracy collide

Have governments learned anything from 2016? This election cycle will prove pivotal in shaping the future of election security.



#10 Hacking attacks rise in the cryptosphere

The security of cryptocurrencies rests on safeguarding users' private keys. Cybercriminals tend to follow the money, so expect cryptocurrency to be at the top of attackers' wish lists in 2020.

#11 An attack at the edge puts businesses on notice

The continued proliferation of IoT devices is making edge computing an essential component of IT infrastructure. But threat visibility becomes more critical as the number of endpoints in the network multiplies. A major security incident could see enterprises rushing to invest in monitored and controlled device gateways.

53% of those engaged in digital transformation say cyber-attack risk is their **PRIMARY RISK MANAGEMENT CONCERN.**[5]

#12 Criminals focus on taking over accounts

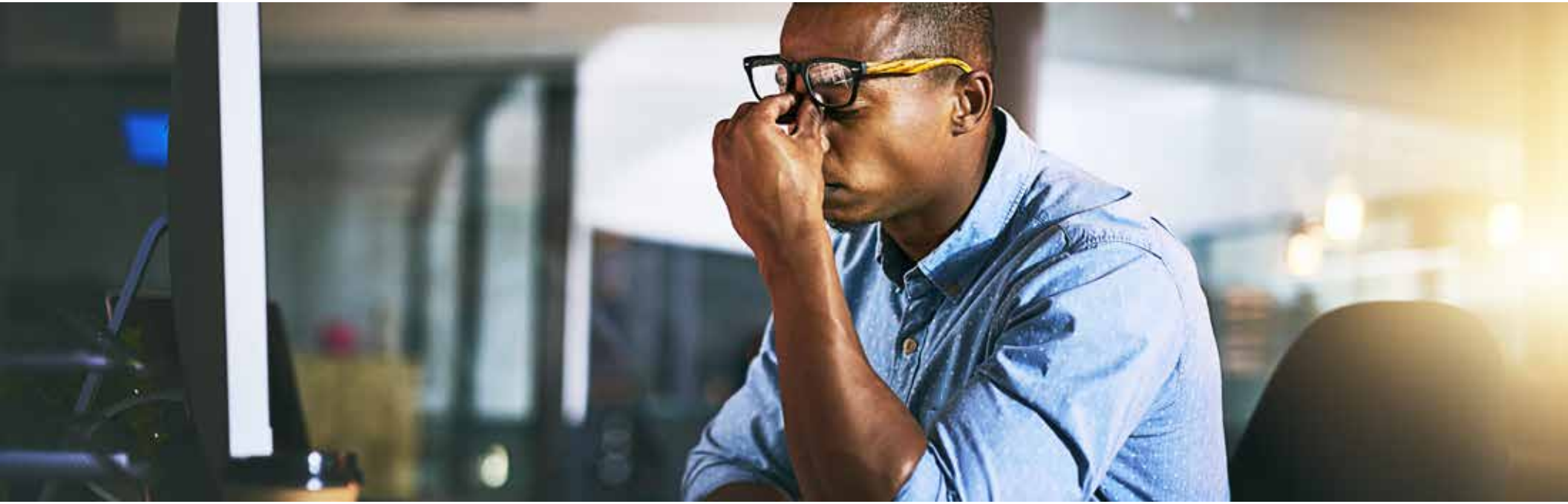
Savvy cybercriminals are shifting their focus from stealing credentials to infiltrating password recovery mechanisms, with a goal of harvesting and resetting user credentials en masse. User identities will be reestablished with new usernames and passwords as fast as you can say "cybercriminal."

#13 A target on the infrastructure backbone

Too much of global infrastructure, including fundamentals like water and power, relies on aging technology vulnerable to exploitation. Expect to see nations bolster industrial control system (ICS) monitoring and defenses, in hopes of fending off increasingly commonplace—and devastating—attacks.

#14 A new angle for ransomware

The popular attack vector won't just hold your data hostage—it will stop you from connecting to critical infrastructure. How much would you pay for access to your systems and accounts?



#15 Cybersecurity gets physical

With global events such as the Summer Olympics and Dubai World Expo delivering experiences through a blend of infrastructure and connected systems, cybersecurity will move beyond data to encompass more and more of our physical well-being—or "cyber safety."

In the first six months of 2019, RSA detected **63% MORE GLOBAL FRAUD ATTACKS** than it did over the same period in 2018.[6]

#16 Companies pass the BYOD hot potato

Bring Your Own Data (BYOD) programs bring tremendous assets—and new cybersecurity liabilities. More and more businesses will use BYOD policies such as user-owned decentralized storage to limit liability—and leave it to employees. Meanwhile, organizations that don't directly monetize data will make data security consumers' problem.

#17 IoT attacks shake consumer confidence

Motivated more by vast disruption than a big payout, malicious actors will attack the unsecured IoT endpoint of a popular connected device. Consumers will question their security assumptions—raising important questions about weaknesses in, and governance of, virtual assistants.

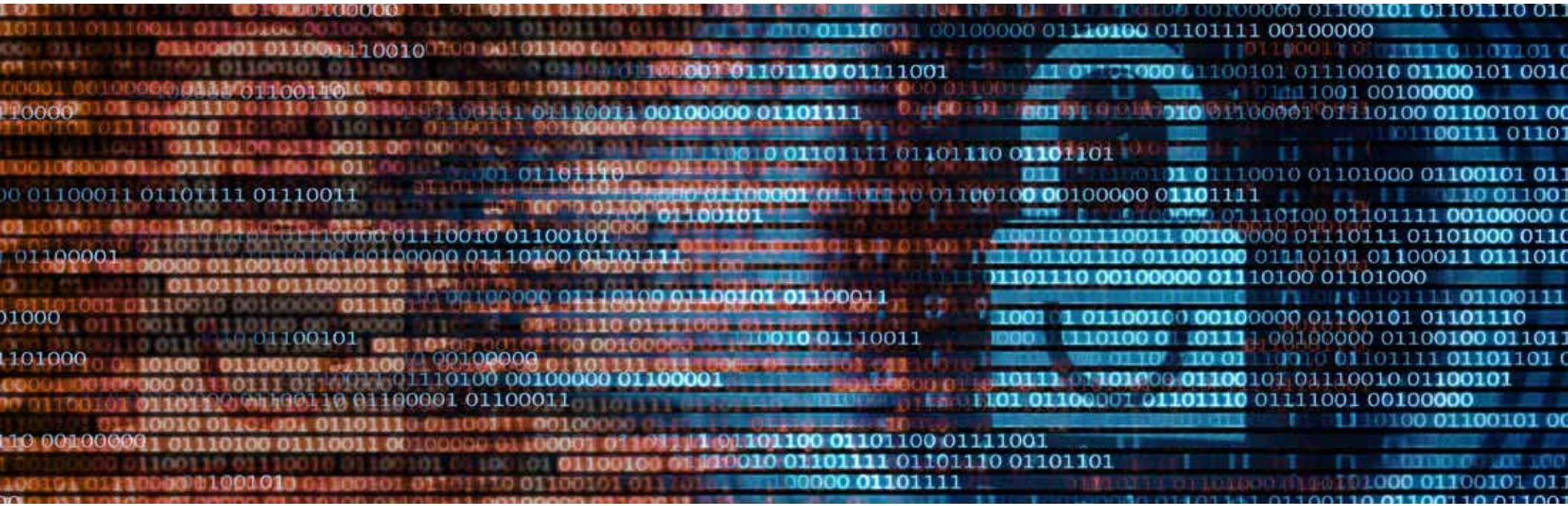
#18 Spoofing goes mainstream

A popular mobile app will offer consumers on-demand animated spoofing—and trigger widespread discussion of deepfakes, media integrity, and how to regulate and police false content.

#19 Breach accountability gets even murkier

A high-profile organizational breach will be traced to an API integration. So, who pays the GDPR fine? The resulting controversy will spark debate about regulatory accountability in a growing third-party ecosystem.

DATA PRIVACY
is a top risk management concern for North American organizations with more than 5,000 employees.[7]



#20 The Feds punt on privacy

Despite many states ratifying data privacy laws in 2019, the U.S. federal government won't reach agreement on 2020 privacy legislation—leaving states to regulate the issue.

The future is full of business opportunity—much of it increasingly subject to digital risk. As cyber attacks, the mobile workforce, regulatory issues and data privacy elevate the level of threats, companies must keep pace with risk and security strategies that combine awareness, collaboration, investment and innovation.

Learn how RSA can help you manage digital risk in 2020 and beyond.

1. Jon Oltsik, "The Cybersecurity Skills Shortage Is Getting Worse," Enterprise Strategy Group, January 2019.
2. Steve Morgan, "Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021," Cybercrime, October 2019.
3. Edward Lim, "Taking the Lead: Addressing the Cyber Skills Gap in Asia-Pacific," rsa.com, July 2019.
4. "Global Artificial Intelligence (AI) in Cyber Security Market," Zion Market Research, August 2019.
5. *RSA Digital Risk Report*, September 2019.
6. *RSA Quarterly Fraud Report*, Q2 2019.
7. *RSA Digital Risk Report*, September 2019.

RSA®