RSA

21 Predictions for 2021

Cybersecurity for a Changed and Changing World

This time, the future unfolds in the shadow of the past.

2020 may be over, but organizations will continue to feel its impact in 2021, when plans and decisions will be profoundly influenced by the challenging events of the past year.

Unprecedented changes in how we work, play and connect aren't going away anytime soon. We'll continue to work from home, do more shopping online and stream much of our entertainment, to varying degrees. These shifts will continue to affect how organizations handle identity and access management, threat detection and response, fraud prevention, and risk management in 2021 and beyond.

What can you expect in 2021?

Inundated with new cybersecurity threats in an expanded attack environment, organizations will take a serious look at taking action to adopt zero trust, consolidate cybersecurity operations, deploy new fraud prevention technologies, and rethink their approach to risk and regulation.

On the following pages, we share 21 predictions for 2021 that illustrate the many ways in which 2020 is changing the shape of cybersecurity. Read on to learn more about the challenges and opportunities that will redefine security and risk in the year to come.

#1

Doubling down on digital transformation

The unprecedented events of 2020 didn't slow digital transformation—they accelerated it. From securing the remote workforce to extending cybersecurity to the cloud, this acceleration will continue. Building on the insights and experiences of 2020, organizations will embrace transformation with even greater urgency to regain competitive advantage.

Identity and Access Management

Organizations will continue to find it challenging to ensure that people are who they claim to be when they seek access to work apps and data, personal financial accounts and other resources online.

#2

A more critical role for identity governance

As the workforce continues to evolve in light of some people returning to the office and others continuing to work remotely, organizations will benefit from a focus on ensuring that they can easily manage changing user rights and access privileges.

#3

Cybercriminals exploiting access changes

Organizations should anticipate ongoing attempts to steal credentials when many in the workforce are continuing to access resources from home. It will be critical to work to limit the negative impact by addressing issues such as use of unhardened devices, cloud application access outside the VPN and sharing of work devices with family members.

#4

The shift to zero trust

Cybersecurity will pivot to embrace zero trust, as security teams rethink their defense postures to adapt to an expanding attack surface and a growing reliance on third parties. Zero trust defense postures will combine a range of governance processes, multi-factor authentication methods and other measures to manage emerging identity-based threats.

#5

Stepped-up DDoS attacks

Distributed denial-of-service (DDoS) attacks will rise as the attack surface expands and dependence on the internet grows, building on a threefold increase in DDoS attacks in 2020. The shift to zero trust (#4) will help combat DDoS attacks by rejecting the concept of trusted systems—a concept that is vital to successful DDoS attacks.

#6

Youthful vulnerability and synthetic identity

Synthetic identity theft, in which pieces of legitimate user information are combined with fictitious information to create a fake identity, will increase as fraudsters specifically target younger users who may not monitor their identities closely. This will ultimately lead to a massive surge in new account fraud.

Threat Detection and Response

More kinds of threats and threat actors will target more organizations across a vastly expanded attack surface, prompting the adoption of new strategies, tactics and technologies for defending against threats.

#7

The remote workforce is here to stay—and so is the risk that comes with it

While many workers will return to the workplace, some degree of remote work will remain a permanent feature of many employees' workdays. The expanded attack surface associated with remote work will still create cause for concern as the workforce continues relying on a combination of personal networks, third-party resources and new resources.

#8

Dangerous times for healthcare

Healthcare organizations, already targeted for cyber attacks throughout the pandemic, will continue to face ransomware demands that threaten to expose sensitive data, as well as dangerous spear-phishing attacks aimed at stealing IP. Vaccine companies in particular will increasingly be the focus of attacks as they race to get vaccines into widespread distribution.

#9

The rise of XDR

Organizations will increasingly extend detection and response from the user, through the network and into the cloud, to provide visibility anywhere and everywhere data and applications live. Extended detection and response—XDR—will be critical for security teams to stay ahead of sophisticated and aggressive threats.

#10 Cybersecurity consolidation: out of many, one

Forced by the expanded attack surface to fundamentally rethink defense postures and plan for increased risk, organizations will continue to move toward a cybersecurity strategy built on a single, cohesive operation. This is in contrast to the multiple point solutions they relied on previously to meet specific needs.

#11 Automation and AI in the SOC

Security teams will focus on how to approach threat detection and response in an expanded threat environment where there may be much less control. One response will be to add automation security and artificial intelligence (AI) to help identify new threats and prioritize responses in the security operations center (SOC).

Fraud Prevention

Fraudsters who hit the jackpot in 2020 by taking advantage of surging online activity will be looking for ways to continue their success into the next year—and retailers and consumers will need to be ready to fight back.

#12 Victimizing the vulnerable

Until a robust economic recovery is underway, fraudsters will continue to find ways to profit by exploiting people in desperate financial straits. Using phishing, rogue mobile apps and other types of fraud attacks to offer easy money, they will trick recipients into sharing bank account numbers or other sensitive information.

#13 A bigger role for AI/ML in fraud prevention

As merchants work to balance fraud prevention and regulatory compliance with frictionless customer experiences, we will see AI/machine learning (ML) advance to the point where merchants can more easily assess transaction risk and comply with SCA and other regulatory requirements.

#14 3-D Secure 2.x: Take that, CNP fraud

The surge in e-commerce that the pandemic brought in 2020 came at a price: a corresponding rise in targeted card-not-present (CNP) fraud. The urgent need to recognize and reduce transaction risk, while also reducing customer friction, will lead more U.S. merchants and card-issuing banks to adopt the 3-D Secure 2.x authentication protocol.

#15 Surges in QR code and BOPIS fraud

Cybercriminals will exploit consumer demand for contactless transactions, driving surges in buy-online-pickup-in-store (BOPIS) fraud, where fraudsters use stolen cards to buy online and send mules to retrieve purchases at curbside, and quick response (QR) code fraud, including QRs that request payment or personal information or that trick users into downloading malicious programs.

#16 Loyalty points looted when no one’s looking

Travelers who aren’t traveling as much anymore are also likely not checking their airline and hotel loyalty points and account balances as much either. That’s not lost on cybercriminals, who will quietly use credential-testing and account takeover to harvest points when they know few people are paying attention.

Integrated Risk Management

More and changing regulation in response to a changing world will expose organizations to more regulatory risk, forcing them to reexamine how they manage that risk.

#17 Consolidated, proactive risk management

For many organizations, enabling the remote workforce revealed outdated, fragmented risk management processes. These will give way to systems and structures designed to help proactively manage risk, as organizations consolidate risk management, compliance and governance into a total managed view, and prioritize having risk data that's as close to real-time as possible.

#18 Regulatory landscape complexity, continued

The recent rise in regulatory compliance regimes around security and privacy, and the ongoing emergence of new regulations, will continue to create complexity. These challenges will force organizations to grapple with simplifying their internal data architectures to achieve a better understanding of their own compliance posture.

#19 More data regulation—and tougher penalties

The value of data will continue to increase, leading to more data privacy and security regulations being developed, debated and enacted, particularly when it comes to critical infrastructure. There will also be harsher penalties for failing to protect data, not disclosing attacks or otherwise being out of compliance with applicable laws.

#20 Assigning accountability in a breach

The issue of regulatory accountability in a growing third-party ecosystem will come to a head, likely because of a high-profile General Data Protection Regulation (GDPR) case in which an organization suffers a data breach due to an application programming interface (API) integration—and the courts end up having to determine who is responsible for paying the fine.

#21 AI regulation: all eyes on the EU

The speed with which EU organizations have been adopting AI will put increasing pressure on European regulators to prioritize it over other areas for regulatory initiatives. Indeed, 2021 could bring the first draft of formal AI regulations in the EU, along with guidance on how to adopt AI ethically.

In the wake of a year of unimaginable change and tumult, 2021 promises to be a year of extraordinary challenges. Whether your organization is striving to overcome them, or simply understand them, **RSA** is here to help.

About RSA

RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational 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.