# What the future holds: Cyber security predictions for 2021

The effects of the COVID-19 crisis that began last year are still visible across the cyber security landscape, making it difficult to predict the trends for cyber security in 2021. Considering the unprecedented events of 2020, any predictions for the immediate future cannot be definitive. The COVID-19 pandemic brought the world to a standstill for most of 2020 and going forward, organisations would need to prioritise the health and safety of their employees over organisational goals and objectives.

The pandemic and the worldwide adoption of remote working resulted in cyber security undergoing years' worth of transformation in a matter of months. While the pandemic has certainly had an indisputable impact on the adoption of digital technologies across organisations worldwide, the trend was already increasing. We have attempted to analyse recent global events and how they may impact and transform the cyber security landscape in 2021. Working closely with our clients gave us a ring-side view of the various challenges faced by organisations and the solutions being implemented to resolve them. This helped us gain a better understanding of the trends that are likely to unfold in 2021.

pwc

## 1. Sovereign cyber security

Rising geopolitical tensions worldwide have resulted in governments and enterprises increasingly focusing on cyber security to protect their assets from cyberattackers. Instances of cyberattacks by national/state actors targeting critical infrastructure and nationally important establishments are becoming more common.

**In 2021, there will be an increased focus among countries on developing stricter cyber security regulations and efforts to build both defensive and offensive capabilities.**

## 2. Big Tech and consumer privacy

As far as clichés go, data is the new oil is still a very relevant one. As online transactions/interactions become a larger part of our daily lives, data's importance has risen meteorically, and so have attempts by cyberattackers to use data for nefarious purposes. Technologies, especially consumer-facing ones that rely on data to solve important problems, have gained notoriety due to instances of consumer privacy and digital dignity being compromised.

**In 2021, organisations will face greater penalties for not adhering to data privacy regulations. Regulators are also expected to carefully observe how data and consumer privacy are being managed by organisations.**

## 3. Shift to active defence

Traditionally, organisations focused on preventing cyberattacks by relying on security practices such as patching and blocking bad internet traffic or internet protocol (IP) addresses. While practices around Protect, Detect, Respond and Recover were effective against older types of threats, they are not as effective in stopping new advanced attacks. Further, these old mechanisms fail to provide any knowledge of what an adversary does once it penetrates a network.

Defenders can develop a robust set of counter-adversary tactics, techniques and procedures (TTPs) against a range of targets over a period of time only by understanding the behaviour of adversaries. With the help of these TTPs, defenders can gain insights into the behaviour of attackers and their modus operandi, thereby improving their ability to predict attacker behaviour and create more dynamic defences.

**In 2021, we will see active threat hunting becoming mainstream as organisations move beyond just rule-based or machine-based Protect, Detect and Respond strategies.**

## 4. Cyberthreats and increased weaponisation

The scale, velocity, and complexity of cyber threats are increasing exponentially, and artificial intelligence (AI) and machine learning (ML) are being used to automate malicious activities. The pandemic has further strained existing controls as organisations are increasingly adopting the concept of work from anywhere and a distributed enterprise architecture. Existing counter-intelligence and security technologies are no longer fit for purpose as the scope of remote work has increased worldwide.

**We predict that 2021 will see an increase in human intelligence being augmented by the computing prowess of AI and ML to combat emerging cyber threats.**

## 5. Transformation of cloud computing

Cloud computing has gone through dramatic changes due to the pandemic. It has quickly transitioned from a helpful, tactical resource to reduce costs and speed up the delivery of IT services to an important and strategic method to enhance resilience. But cloud computing still has some distance to cover. The transition from on-premises to cloud involves a complex interplay of old and new technologies. The shifting of core businesses to cloud makes it a target-rich environment that would need to be secured.

Thankfully, enhancements in cloud security are evolving and cloud environments are becoming more secure.

**2021 would be a year of secure cloud adoption and also leveraging security technology from cloud.**

## 6. Identities to take centre stage

Ecosystems and asset classes that were traditionally being protected by identity management solutions are rapidly evolving. With the expansion of security perimeters and the need to allow what was previously deemed as risky access, untrusted digital environments bring organisations face to face with unplanned threat scenarios. Digital identity assertion needs to be more rigorous and primarily focused on a risk-based approach to balance user convenience and cost. Advanced identity protection should be extended to not only end users, but privileged users, third parties and customers as well.

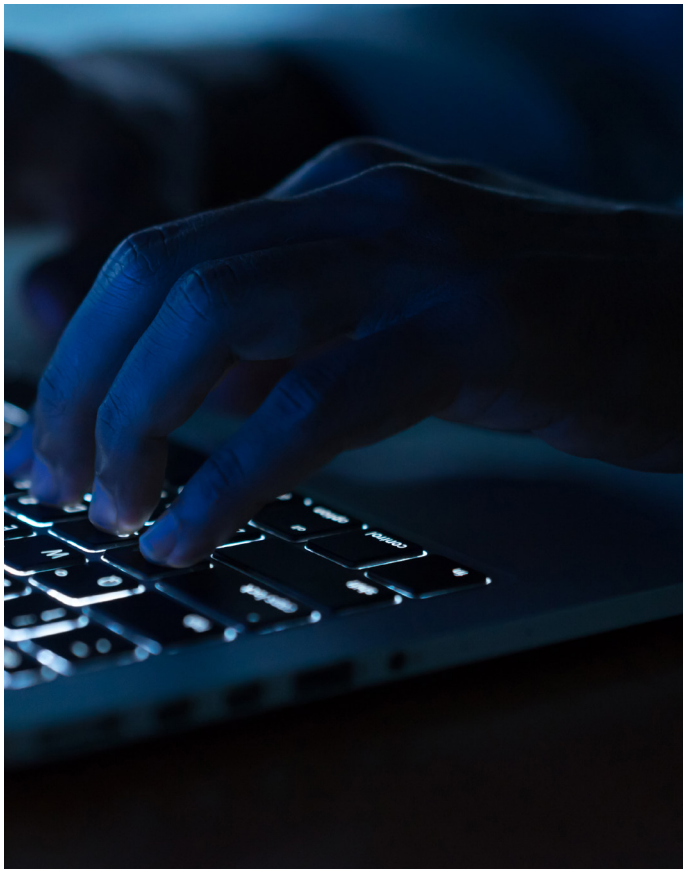
**In 2021, organisations would be required to embrace risk-based adaptive authentication that helps them to go beyond one-time assertion and enhance protection based on the criticality of transactions, and challenge end users to prove their identities using different form factors.**

## 7. Cyber security as a core business strategy

With increased digital transformation across organisations, cyber security would no longer be an adjunct function within IT and instead be a part of their core business strategy.

Building digital resilience and customer trust in the post-pandemic world would be a top priority for organisations.

**In 2021, we expect CISOs to become a part of core leadership teams within organisations due to an increased executive focus on cyber security.**



**While the above predictions are based on our prior experiences in the cyber security domain and interactions with clients, they are not the only predictions for the sector. Continuous developments in the cyber security domain make it difficult to foresee whether these predictions would come true or not. It is our constant endeavour to serve the cyber security community and we would continue to study macro trends, and keep our eyes on the horizon to assess changes.**

# About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Find out more about PwC India and tell us what matters to you by visiting us at www.pwc.in.

## Authored by

**Siddharth Vishwanath**
Partner and Cyber Advisory Leader
PwC India

pwc.in



KS/February 2021-M&C10596