TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

CYBERSECURITY IN 2021

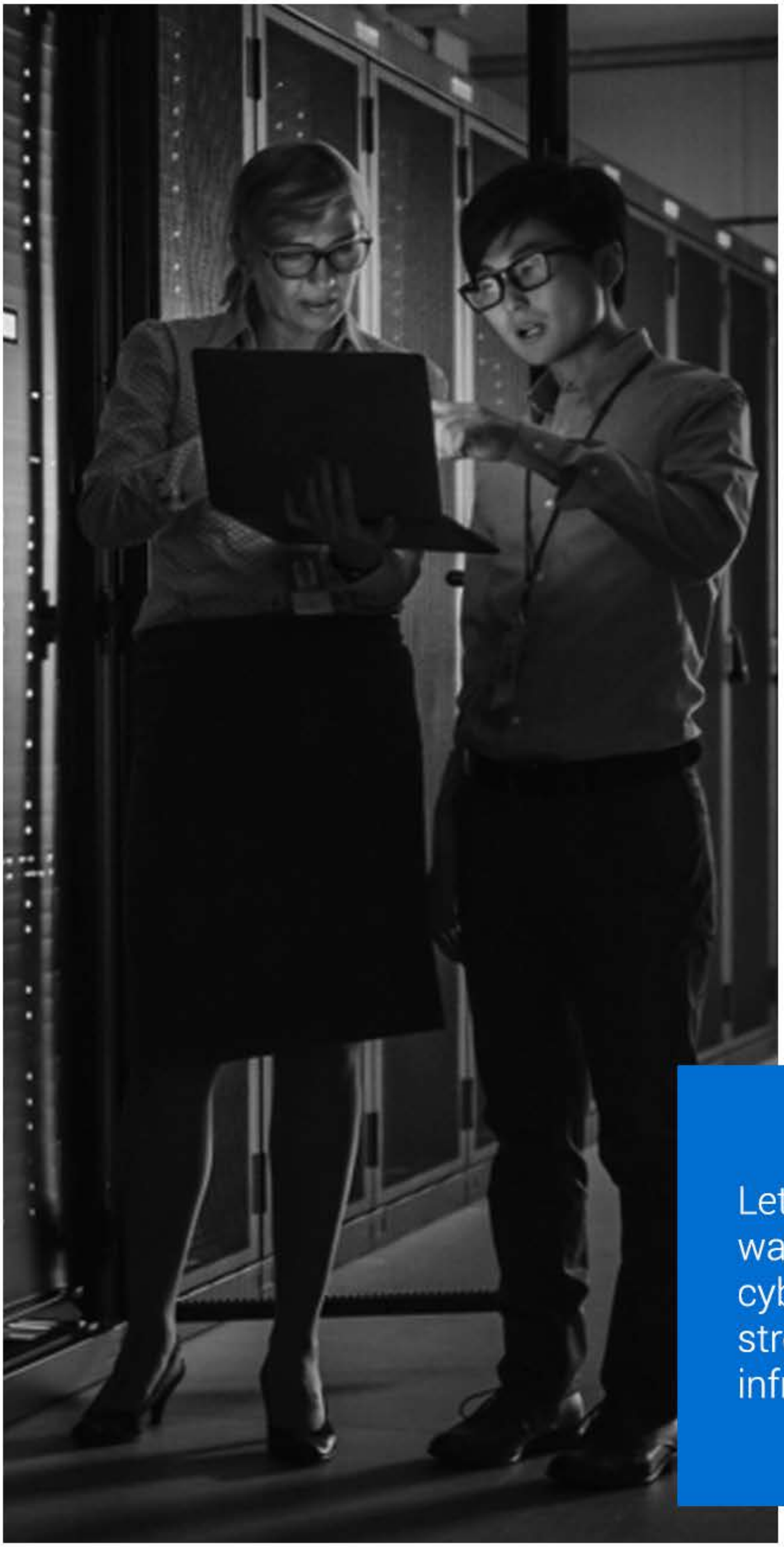
PLAN NOW TO CONFRONT FUTURE CHALLENGES

www.tataadvancedsystems.com

TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE



As 2021 has come close to our doors, it is an opportune time for companies to relook and set an effective strategy to navigate through the cybersecurity challenges in the coming year. All the C-level executives must brainstorm to effectively deal with concerns such as meeting regulatory compliance, keeping pace with emerging trends and technologies, preparing a strong incident response and remediation plan, and creating policies to securely manage critical data throughout its lifespan. All these tasks need to be accomplished while keeping in mind the security of sensitive digital assets, which becomes even more difficult when we all are in the midst of a pandemic. It is important for organizations to set their goals and priorities regarding the cybersecurity challenges right from the beginning of the new year.

Let's discover some promising ways that can help in mitigating cybersecurity risks and strengthening the IT infrastructure in 2021.

TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Focus on Cloud Security

Cloud migration has increased incredibly in 2020. As per a report from the Synergy Research Group, global spending on cloud infrastructure services increased 33% in Q2 2020 over the same period in 2019 to $30 billion. During this pandemic, the velocity of creating digital-native business applications and services has greatly enhanced as enterprises are preparing themselves for survival in the post-pandemic period.

In 2021, organizations must look for misconfigurations and human errors, implement strong practices for container security, and meet compliance with industry regulations such as PCI, HIPAA, GDPR, etc. Companies should adopt and execute such a cloud security strategy that accelerates significant workplace transitions, to incorporate constantly increasing remote workforce. They can also prioritize Privileged Access Management (PAM) & Identity Access Management (IAM) to provide the least privilege access to the confidential data. Also, investment in Zero Trust Policy and Micro-segmentation will be a good option for cloud security.

Look for Insider Threats

Insider threats are one of the biggest drivers of the security risks faced by organizations as an insider has all the necessary rights required to assess the company's critical assets. Identification and detection of malicious insider activities is a daunting task as companies often lack the ability to detect such unusual activities within their premises. According to a report by Forrester, it is expected that internal incidents will be accounted for 33% of data breaches in 2021.

Organizations should consider insider threat defence in order to prevent such incidents while being cautious not to degrade employees' privacy, company's culture and standards for labour practices. They can follow the below-mentioned security procedures to mitigate insider threats:

- Conduct regular risk assessments
- Create and document security policies such as account management, user monitoring and password management policies
- Invest in security software like endpoint protection, intrusion detection and prevention and traffic monitoring
- Strengthen the network security

TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Add Multi-factor Authentication (MFA)

Throughout 2020, data breaches remained at the top of the headlines across the globe. Malicious activists have gained incredible success in stealing sensitive business data with the help of stolen usernames and passwords, which are now easily available on underground marketplaces like Dark Web. Threat actors take advantage of the fact that most of the users still do not select strong and unique passwords for their accounts.

MFA reduces the risk by providing additional security methods, apart from username and password, such as One-Time Passwords (OTPs) that you often receive via emails & SMS. It is expected to be a crucial factor in protecting a user's identity and preventing unauthorised account accesses. As per a recent report from MarketWatch, the global Multi-Factor Authentication (MFA) market size is expected to reach USD 32110 million by the end of 2026, with a CAGR of 19.6% during the forecast period (2021-2026).

Keep an Eye on Human Vulnerability

In 2021, enterprises must keep a sharp eye on the security of their workforce against the growing and evolving social engineering and phishing attacks. CISOs and other security leaders need to focus on and improve the casual attitude of employees towards cybersecurity in order to reduce the occurrences of data breaches and cybersecurity attacks.

It will be vital for organizations to look into cybersecurity education and training of their workforce, particularly when remote work is being followed globally. Employees should be made aware of the basic practices such as the creation of a strong password and double-check the URLs (embedded in emails) before clicking on them.

Review Data Security & Privacy Policies

In 2021, the data privacy landscape will remain in the spotlight. With the increasing focus on compliance with industry regulations, organizations will be looking forward to the security and privacy of data more seriously than ever. Classifying data as public, private and confidential is not sufficient enough to avert data breaches. Companies often provide employees with access to data that they do not need, and hence they are more likely to face a data security incident.

Strong data access controls and policies should be considered as one of the top priorities in 2021 in order to ensure the security of critical business data. Solutions, like email security, can be viewed and implemented to keep a check on what data is being transferred or received to/from outside the organizational perimeter. Companies must regularly review policies to track how their critical information is being stored and update authorizations on a regular basis.