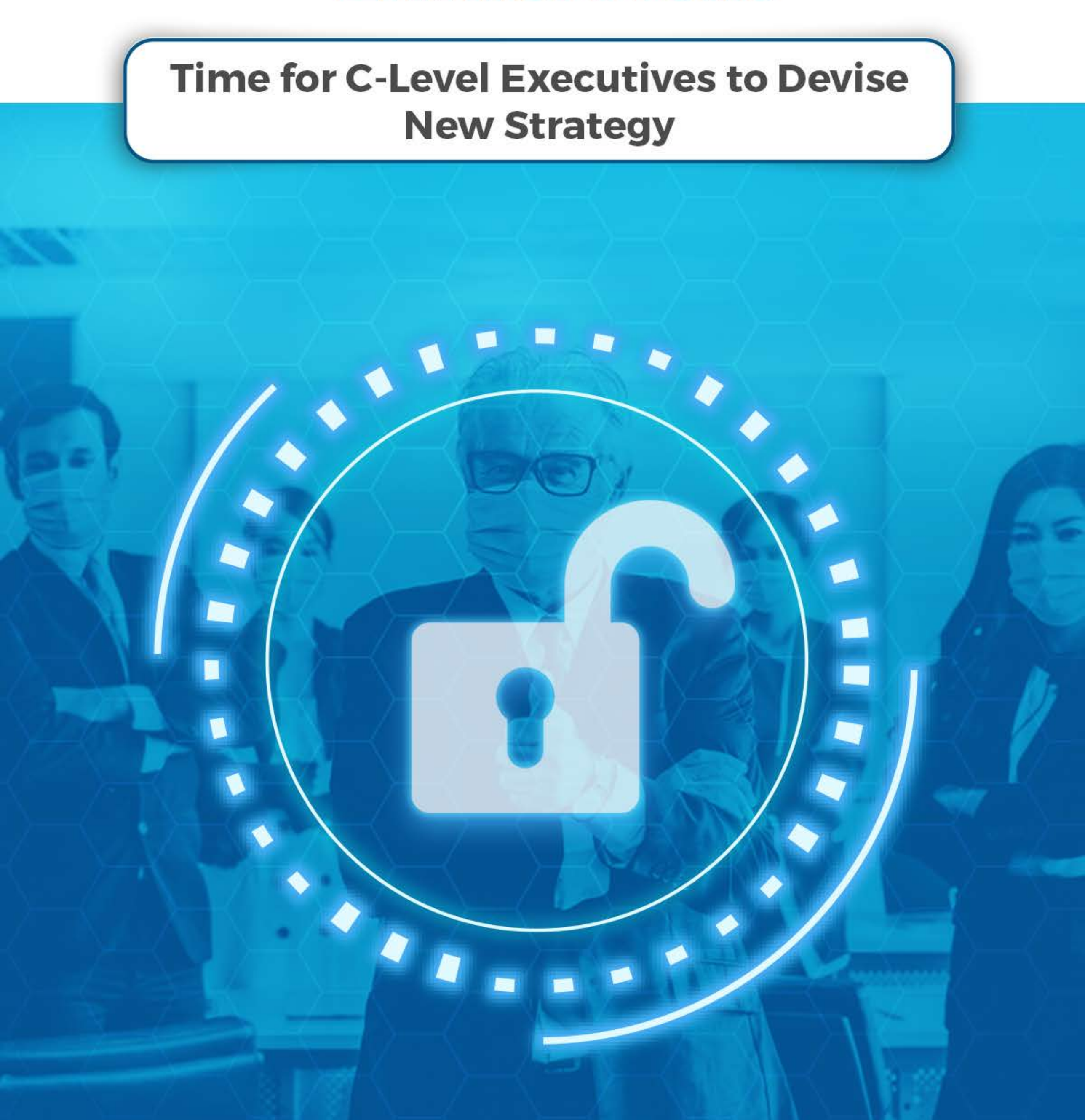
TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Cybersecurity in Post-COVID Environment

Time for C-Level Executives to Devise New Strategy



TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

As COVID-19 restrictions have started slackening, people are transitioning back to their offices and social calendar. Unfortunately, this shift is expected to introduce an increased threat of malicious activities. The risk is comparatively higher for those organizations who have not provided their remote employees with adequate VPN and regular software updates. Employees of such organizations exposed to a variety of threats as they were connected to their home network, which lacks required security measures.

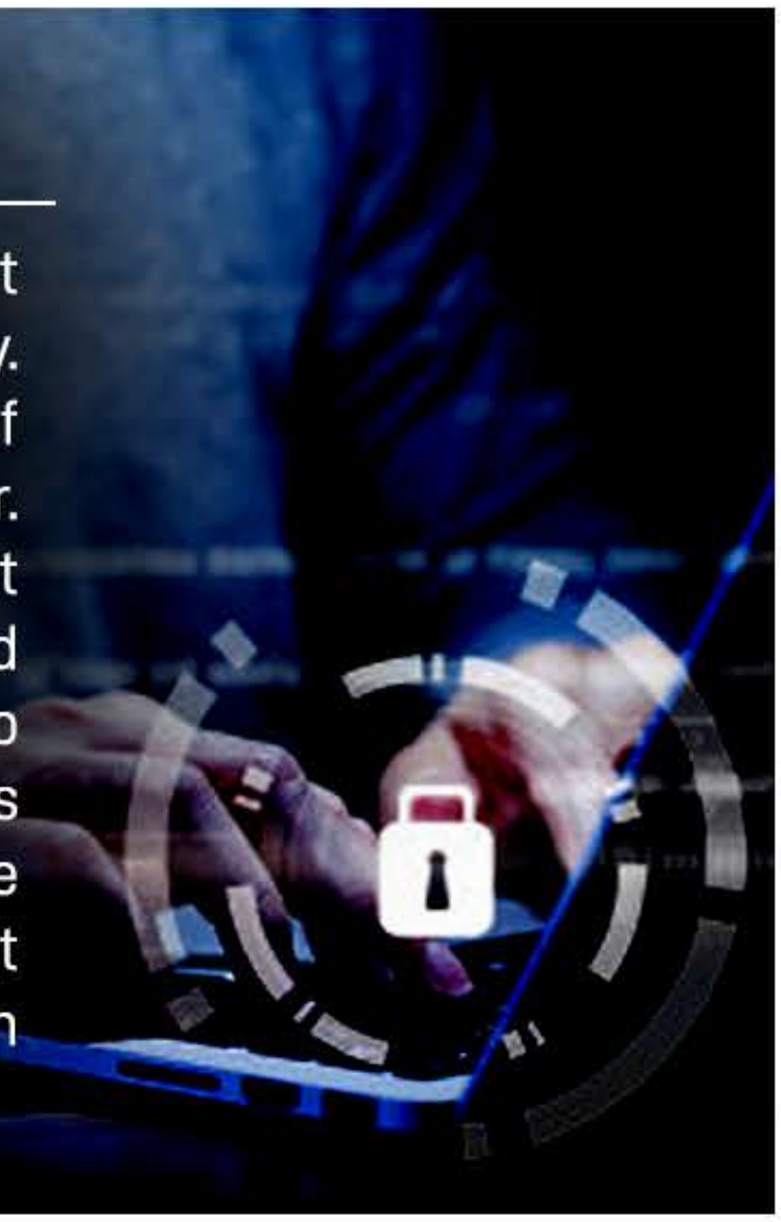
Glance through some common risks that employees may have experienced while working from home.

Risk of Dormant Malware

Threat actors have largely exploited the remote workforce during the lockdown with COVID-themed phishing emails containing malevolent URLs and attachments to get access to victim's sensitive personal and corporate information. They have also infected systems with different strains of malware that have stayed dormant and may get active once those systems are reconnected to the office networks. Post successful execution, such malware may trigger dreadful cybersecurity incidents and cause massive loss to an organization, both financially and reputationally.

Improper Security Configuration

Lack of proper security configuration is another element that has fueled the growing momentum of cyber-attacks globally. For several organizations, the remote management of employees' computer systems has been challenging so far. For instance, providing VPN to such a great extent was not feasible for every organization. Also, it cannot be overlooked that employees may not have given sufficient attention to update their work devices or install required security patches while working from home. Linking those devices back to the corporate network may permit malicious activists to exploit the security loopholes in the systems and bring an organization to its knees.



TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Ransomware, data breaches, social engineering, phishing and malware attacks have surged exponentially during COVID times and impacted organizations globally, irrespective of their vertical. Now, when the employees are returning to the offices, all the C-level executives and security teams must collaborate and work closely to define a new strategy to use technology, tools, people and processes smartly. Gartner has also predicted that cyber-physical security incidents will result in personal liability for 75% of CEOs by 2024. So, they need to remain more cautious than ever before while defending the digital assets of their organization.

Here, we will look at some important steps that can be employed to address potential cyber threats and reduce the chances for threat actors to infiltrate.

Security Assessment of IT Infrastructure

The first step towards resumption of work from offices should be a thorough assessment of the entire IT infrastructure. The C-level executives, including CISOs and CIOs, must have a clear understanding of the organization's current cybersecurity posture as the prolonged inactivity may have surfaced some unpatched vulnerabilities.

Expand Cybersecurity Budget

Spending on information security and risk assessment will help organizations to create a robust and resilient infrastructure, repel complex cyber-attacks and minimize the chances of data breaches and leaks. Not long ago, Gartner has also predicted that information security spending is expected to grow 2.4% to reach $123.8 billion in 2020.

Examine Employees' Devices for Vulnerabilities

A majority of organizations have provided their employees with laptops and desktops to continue work from home during the lockdown. It is possible that those systems may get infected with some virus or trojans since they were not connected to the office network. This could be potentially dangerous when those devices will be reconnected to the corporate network as threat actors might exploit the hidden vulnerabilities to cause damage to the organization. Ideally, all such devices should be submitted to the IT team for virus scan and security patches before usage.

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Allow Sufficient Resources Only

Organizations can identify and allow resources that have privileged access to critical business data and are at increased risk of being exploited by the cybercriminals to resume work from offices. This can help in removing pressure from IT teams working to patch employees' work devices and mitigating the risk of cybersecurity incidents.

Conduct Security Awareness Training

Security awareness training is supposed to be the most important practice towards ensuring cybersecurity as employees have been accustomed to certain habits while working from home, which may pose risks to an organization's security. Such awareness programs will help in educating employees about the security obligations that they need to follow at the workplace and in staying aware of the new emerging cyber threats.

Implement a Zero Trust Model

Zero Trust model is based on the principle – Trust no one, verify all. Since the number of endpoints has continued to rise, it is increasingly becoming difficult to define a security perimeter. An ideal approach would be to adopt a Zero Trust model which ensures that the business-critical applications and information are accessible only to authenticated users and devices.

In the post-COVID environment, organizations, especially their C-level executives need to remain vigilant to different complex cyber threats and vulnerabilities that could arise when employees start working from the workplace. Security teams need to take the opportunity to recheck the efficacy of existing security controls and implement good cyber hygienic activities like virus scans and network traffic monitoring to prevent unauthorised users from accessing the company's network.

To redefine the cybersecurity infrastructure of your organization, connect with us at

contactcs@tataadvancedsystems.com