TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

MANAGING CYBER RISKS IN ENERGY SECTOR

A KEY CHALLENGE

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

A recent cyber-attack on the US popular fuel pipeline operator demonstrated that why cybersecurity professionals worldwide see ransomware as one of the biggest threats to public safety. This attack is a clear indication of how the frequency and complexity of cyber threats targeting critical infrastructures have amplified over the years. Earlier this year, anonymous hackers somehow got access to the Florida water treatment facility and altered the sodium hydroxide levels to an extremely hazardous level.

In short, these incidents showed that essential services providers are on the list of threat actors and more vulnerable than ever before. It would not be an overstatement if the growing digitization of such infrastructures is considered as one of the reasons behind the spike in cyber-attacks. Undoubtedly, modern digital elements have significantly optimized the effectiveness of energy systems. But, at the same time, the chances of cyber intrusions have increased manifold. Other reasons may include (but not limited to) legacy infrastructure and systems, nation-backed actors for cyber espionage, high returns for cybercriminals, etc. In a recent survey done by World Economic Forum, 49% of respondents reported that cybersecurity failures are one of the medium-term risks facing the world.

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Security Practices to Keep Critical Energy Infrastructures More Secure

In order to mitigate potential risks and harness the full benefits of digitalization, organizations must work in accordance with the governments and redefine the security strategies of the critical infrastructures. New practices should be embedded to shape up the overall security.

Following are a few suggestions for critical organizations to ramp up their cybersecurity without hampering business productivity:

- **Build a strong cybersecurity governance model**

  Organizations must adopt a forward-looking approach, instead of following reactive measures, to ensure security. Establishing a robust cybersecurity governance model containing a comprehensive risk management approach, along with a complete set of management tools and a security awareness program, will assist organizations to address all of their cybersecurity needs.

- **Increase the visibility of third-party risks (safeguard the supply chain)**

  Marginal flaws in third-party software or products may turn into critical vulnerabilities for your organization. Threat actors may target third-party vendors to penetrate your organization's security infrastructure. Third-party risks may involve (but not limited to) operational risks, compliance risks, reputational risks, etc. Organizations must check and ensure that their supply chain vendors meet all necessary cybersecurity requirements. They should implement an effective defence plan that includes risk assessments and appropriate mitigations.

- **Test your response plans**

  Creating an incident response plan is key to mitigate the potential damage. But to check their effectiveness, organizations must conduct regular drills and exercises to look for security loopholes (if exists). Perform a detailed vulnerability scan to determine the potential systems likely to be targeted by the cybercriminals. Such practices help in identifying exactly what your critical weaknesses might be and what actions various personnel will need to take in the event of a breach.

- **Collaborate with other stakeholders in the industry**

  Industry-wide collaborations can help organizations to address the increasing cyber risks to a great extent. Sharing information regarding attackers and their tactics can reduce the potential risks and help other companies to prepare in advance to thwart them. Conveying data also builds trust among organizations, and sustaining such practices foster confidence in optimizing cybersecurity.

- **Educate Workforce**

  Companies must educate employees about the most common methods through which different malware, trojans or viruses are delivered. They must conduct security awareness programs, wherein the workforce should be made aware of the common phishing attacks and the steps to look and inspect anything that appears suspicious. Employees must be trained to counter any adverse situation to avoid any data breach or other malicious intrusion.

Towards The End

The cyber threat landscape for power generation companies has been rapidly evolving and expanding with more frequent cyber-attacks leveraging complex and sophisticated malware and other tools. One of the most challenging vulnerabilities to address is the supply chain risk. Organizations must prepare themselves in advance to address the ongoing wave of attacks. They should remain mindful of what is happening in cyber security and persist to work in order to reduce the potential vulnerabilities in their critical systems.