TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Morphing State of Cyber Security in APAC

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

The global cyber security climate is changing rapidly and dramatically as the digital interconnectedness amongst individuals and businesses continues to expand. And, the Asia-Pacific region is no different to get excluded from this shift.

Challenges like low cyber security investment, shortage of skills, and lack of security awareness are some of the contributing factors to the increased cyber intrusions targeting startups to popular business entities and critical infrastructures. According to recent research, over 80% of APAC organisations suffered a cyber attack in 2020. Ransomware, Clickjacking, Man-in-the-middle, Phishing, Social Engineering and Botnets are witnessed as some of the key threats to the organizations in APAC.

This diverse region greatly varies in terms of cyber security obligations and readiness. In the last few years, it is seen that organizations and governments have started speeding up their efforts in combating escalating cyber threats.

Let's have a quick look at how the whole picture is evolving in some regions of APAC.

TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

EMPHASIS ON CYBER REGULATIONS

India

As a result of the growing demands for regulatory developments in the ever-evolving cyber space, India is preparing to manage and drive the privacy and security of users' personal data with its Personal Data Protection Bill (or PDP Bill) that is presently under review. This new bill is expected to establish regulations and principles around how personal information should be managed, and create an independent Data Protection Authority of India.

Furthermore, the bill is also likely to propose some changes like the provision of consent at the time of requesting for data and consumer rights to revoke the same consent; and penalties in case of violation of the applicable laws.

Japan

In view of the increased regulatory oversight into data protection, Japan has made tremendous efforts to improve general privacy compliance and cyber security. It has drafted a revised version of the previous Act of the Protection of Personal Information (APPI), which introduces compulsory Breach Notification in the event of a data breach, and is likely to impose compliance requirements (e.g. users' consent) to organizations while gathering customers' personal information.

Also, the revisions have proposed to elevate the maximum fine to JPY 100 million in case any entity fails to comply with the applicable law.

Singapore

To stay on top of the increasing cyber threats and prevent the unauthorized disclosure of personal information, the Singapore government has enforced an effective Personal Data Protection Commission (PDPC). However, there are still some amendments that are pending, which upon approval will impose the following:

- Minimum fine of SGD 1 million or 10% of turnover if any entity fails to comply with the applicable law
- Obligations to report PDPC (within 3 days) and individuals affected in case of any security event
- Must conduct an assessment of any suspected data breached

Australia

In 2020 some changes were proposed to the Australian Privacy Act, including increased fines for breaches of the privacy act, extension of personal information (e.g. location data, IP addresses and device identifiers), changes in the consent notification (needs to be more concise, easily accessible and available in plain English), providing users with the right to bring actions against organizations (subjected to the Australian Privacy Principles (APPs) due to interference with their privacy, etc.

Greater China

The government has introduced an updated version of the previous Multi-level Protection Scheme (MLPS 1.0). This new version, MLPS 2.0, covers all organizations (including critical infrastructures) that operate a network wherein processing of data is involved. It defines 5 main levels of minimum security requirements based on the sensitivity of the industry and the type of information that the enterprise deals with. Each level calls for separate assessment requirement. Level 1 entities will only require a self-assessment, while all above Level 1 will need a third-party assessor.

Additionally, the financial penalties imposed can be RMB 1 million (maximum) in circumstances where highly sensitive data is breached. Also, this version will be applicable to all companies operating within Mainland China.

CYBER SECURITY MARKET
GROWTH IN APAC REGION

According to a recent survey from Mordor Intelligence, the APAC cybersecurity market was valued at USD 30.45 billion in 2019, and it is expected to register a CAGR of 18.3%, from 2020 to 2025. The contributing factors include:

- Increasing penetration of the internet into developing and developed countries
- Growing wireless network for mobile devices
- Increasing trend of malware and ransomware in the context of COVID-19

TOWARDS THE END

Businesses of all sizes worldwide must understand that they cannot ignore the threat of cyberattacks in this increasingly digital age. They should plan strategically in advance to surf against this rising tide of threats and start exploring and adopting more sophisticated cyber security solutions, imposing better security controls for personal devices and setting up communication policies in the event of a security breach.

References

https://www.welivesecurity.com/wp-content/uploads/2017/10/State-of-cybersecurity-in-APAC_Small-Businesses-Big-Threats.pdf
https://www.munichre.com/topics-online/en/digitalisation/cyber/evolving-cyber-regulations-in-asia-pacific.html
https://www.mordorintelligence.com/industry-reports/asia-pacific-cyber-security-market
https://securitybrief.co.nz/story/more-than-80-of-apac-organisations-suffered-a-cyber-attack-in-2020-study