CLA Global TS
The Growth Strategist For Asia

Indus Value Consulting
Exemplifying Talent, Amplifying Value

Protect Your Organisation: Top Cybersecurity Risks – Prepare, Respond or React?

Where Expertise Meets Impact:
A Joint Article by CLA Global TS and CLA Global Indus Value Consulting

March 2026

Visuals designed by Freepik.

Cybersecurity is a critical component for all organisations and businesses, involving the use of technologies, processes, and practices to protect sensitive information from malicious threats and unauthorised access.

Why does Cybersecurity Matter to Businesses?

Regardless of the scale of the corporation, cybersecurity is crucial to the safety of the organisation, and the consequences of a breach increase as the company grows.

1. Small and Medium Enterprises (SMEs)
   SMEs are often seen as easier targets due to the lack of sophisticated security measures. A singular cyberattack could result in financial loss, reputational damage and even business closure.

2. Large Corporations
   Stakes are higher for larger corporations. Massive data breaches, regulatory penalties and loss of customer trust can all be results of a cyberattack.

Cybersecurity Landscapes - Regulatory Frameworks

To counteract and enforce security against malicious cyberattacks, comprehensive evaluation of all the potential and known cyber threats that exist must be thoroughly investigated. The findings lay the groundwork for establishing the Regulatory Frameworks that are now implemented:

1. Cybersecurity Act 2018

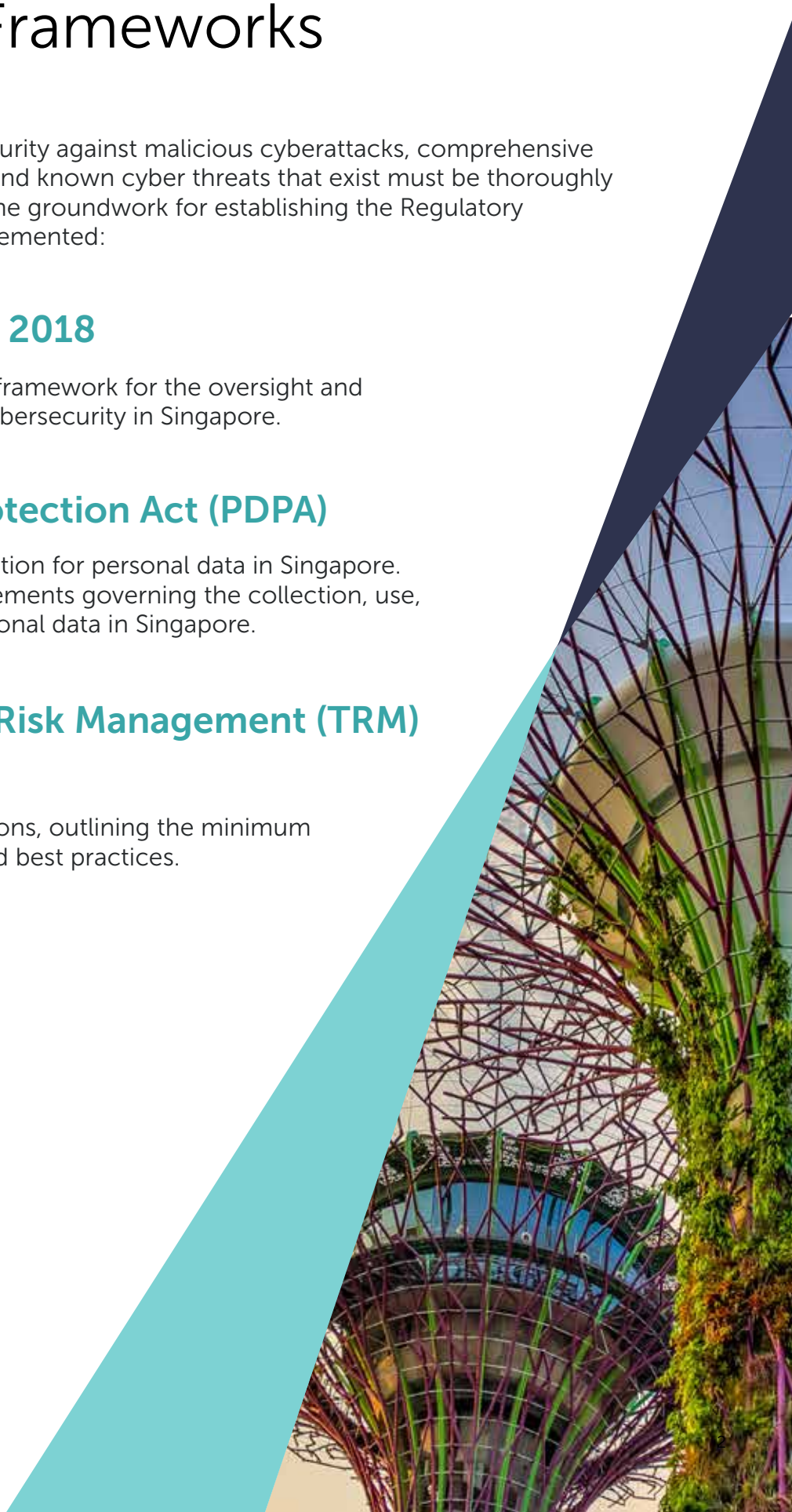
The Act establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore.

2. Personal Data Protection Act (PDPA)

Baseline standard of protection for personal data in Singapore. It comprises various requirements governing the collection, use, disclosure and care of personal data in Singapore.

3. MAS Technology Risk Management (TRM) Guidelines

Applies to financial institutions, outlining the minimum cybersecurity standards and best practices.



4. Computer Misuse Act

Designed to prevent unauthorized access to computer systems, cyber extortion, and other forms of computer misuse.

5. Sector-specific Cybersecurity Guidelines

- Infocomm Media Development Authority
- Ministry of Health

6. ISO 27001 – The Information

Structured framework to safeguard their information assets and information management security systems, covering risk assessment, risk management and continuous improvement.

Top Cybersecurity Risks in 2024-2025

Over the years many types of cyberattacks have made headlines. Analysing the threat and the frequency of such cyberattacks, it has been found that the top cybersecurity risks in **2024-2025** are:

- **Ransomware**
- **Phishing Attacks**
- **Insider Threats**
- **Advanced Persistent Threat**
- **Supply Chain**
- **Cloud Security**
- **DDOS**
- **Social Engineering Attack**

Visuals designed by Freepik.

Best Practices for Securing Systems

As cyber threats continue to grow in frequency and sophistication, securing systems is no longer optional, it is essential for business continuity, trust, and compliance. Strong cybersecurity practices reduce risk, limit damage during incidents, and help organisations operate with confidence in an increasingly digital environment.

Some of the best cyber practices that should be adopted to protect systems and defend against cybersecurity risks.

1. Establish Strong Access Controls

Uncontrolled access is one of the leading causes of security breaches.

Best practices

- Apply the **principle of least privilege**
- Enforce **multi-factor authentication (MFA)**
- Regularly review and revoke unused accounts
- Separate privileged and standard user accounts

Benefit

Limits attacker movement even if credentials are compromised.

2. Keep Systems Patched and Updated

Outdated software often contains known vulnerabilities actively exploited by attackers.

Best practices

- Implement automated patch management
- Prioritise critical and internet-facing systems
- Track end-of-life software and replace it promptly

Benefit

Closes security gaps before attackers exploit them.

3. Protect Endpoints and Networks

Every device connected to your environment is a potential entry point.

Best practices

- Use endpoint detection and response (EDR) tools
- Segment networks to contain breaches
- Secure remote access with VPNs and zero-trust principles
- Disable unnecessary services and ports

Benefit

Reduces attack surface and improves threat containment.

4. Strengthen Email and Web Security

Email remains the primary delivery method for malware and phishing attacks.

Best practices

- Deploy advanced spam and phishing filters
- Block malicious links and attachments
- Use domain protection (SPF, DKIM, DMARC)
- Educate users to identify suspicious messages

Benefit

Prevents social engineering attacks before they reach users.

5. Encrypt Data Everywhere

Data is valuable to all in the organisation and to attackers as well.

Best practices

- Encrypt sensitive data at rest and in transit
- Secure backups with encryption and access controls
- Protect encryption keys using dedicated key management

Benefit

Protects data even if systems are compromised.

6. Implement Regular Backups and Recovery Testing

Backups are your last line of defence against ransomware and system failure.

Best practices

- Maintain offline or immutable backups
- Follow regular backup principle
- Regularly test restoration procedures

Benefit

Ensures fast recovery with minimal data loss.

7. Monitor, Detect, and Respond Quickly

Early detection significantly reduces the impact of cyber incidents.

Best practices

- Centralise logs and security monitoring
- Define alert thresholds for suspicious behaviour
- Maintain a documented and tested incident response plan

Benefit

Enables faster containment and recovery.

8. Educate and Empower Employees

Human error is a major contributor to cyber incidents.

Best practices

- Conduct regular security awareness training
- Simulate phishing attacks
- Clearly define reporting procedures for security incidents

Benefit

Turns employees into a strong line of defence rather than a weakness.

9. Secure Third-Party and Supply Chain Access

Your security is only as strong as your weakest vendor.

Best practices

- Assess third-party security posture
- Limit vendor access to required systems only
- Monitor third-party activity continuously

Benefit

Reduces indirect attack paths into your organisation.

10. Adopt a Continuous Improvement Mindset

Cybersecurity is not static as it evolves with threats and technology.

Best practices

- Perform regular risk assessments
- Conduct penetration testing and vulnerability scans
- Review incidents and near misses to improve controls

Benefit

Builds long-term cyber resilience.

Meticulous practical approaches to tackling these cybersecurity risks are essential to keep corporation systems safe. Practicing safe and secure measures will strengthen internal systems and will allow companies to be less susceptible to future occurrences of such threats.

1. Comprehensive Cybersecurity Policy and Framework

Policy Development: Establish clear policies for data protection, incident response, and acceptable use.

Frameworks: Use frameworks like NIST or the Cybersecurity Framework from the Singapore Cyber Security Agency (CSA).

2. Enterprise-Wide Cybersecurity Policies, Processes, and Controls

Integration: Ensure policies are integrated across all departments and business functions.

Processes: Implement standardised processes for risk management and incident response.

3. Cybersecurity Tools and Technology

Firewalls and Antivirus Software: Essential for basic protection.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): Monitor and prevent suspicious activities.

Security Information and Event Management (SIEM): Singapore's Government Technology Agency (GovTech) uses SIEM for monitoring and threat detection.

Cloud Security

4. Cybersecurity Training and Awareness Programs

Regular Training: Conduct training sessions on recognizing phishing attempts and secure practices.

Simulated Attacks: Use phishing simulations to test employee responses. Cybersecurity Tools and Technology.

5. Periodic Comprehensive Cybersecurity Audits

Regular Audits: Example - Singapore's Personal Data Protection Commission (PDPC) conducts audits to ensure compliance with data protection regulations.

6. System Hardening Mechanisms

Patch Management: Regularly update and patch systems to fix vulnerabilities.

Configuration Management: Apply security configurations to reduce exposure.

7. Cybersecurity Certifications

ISO 27001: International standard for information security management systems (ISMS).

ISO 42001: International standard for AI Management systems.

ISO 22301: 2019 - Business continuity management and recovery from disruptions.

ISO/IEC 27701: Enhances privacy protection by extending information security management.

Through the forementioned practices, it is important that corporations secure and protect key aspects such as:

- **Information Assets** - Use encryption to protect sensitive business data.
- **External Stakeholders** - Ensure secure communication channels with partners and clients.
- **AI Programs** - Protect AI systems from tampering and data poisoning attacks.
- **Cloud Systems** - Implement strong access controls and encryption for cloud data.

Identifying the Threats

To prevent cyberattacks from occurring, staff within the corporations can take precautionary measures to prevent the threats before they happen.

Unusual Network Traffic

Look for sudden spikes in traffic or data transfers to unfamiliar locations, which could indicate DDoS attacks or data exfiltration.

Phishing & Social Engineering

Be aware of suspicious emails or messages with urgent requests, links, or attachments. Phishing often precedes larger breaches.

Unfamiliar Logins

Monitor for logins from unusual locations or devices, particularly from foreign IP addresses or at odd hours. Use geolocation monitoring.

Failed Login Attempts

Repeated failed logins, especially for privileged accounts, can signal brute force attacks. Implement multi-factor authentication (MFA) for added security.

Unauthorized Software or Changes

Watch for unapproved software installations or sudden configuration changes, which may indicate malware or insider threats.

System Slowdowns

Performance issues or crashes may signal malware, ransomware, or crypto-mining activities. Investigate unexplained resource use.

Data Access Irregularities

Track unusual access to sensitive data, especially by employees or systems not usually involved with that data. Use Data Loss Prevention (DLP) tools.

Vendor or Third-Party Risks

Regularly assess your supply chain security. A breach at a vendor can compromise your systems. Ensure vendors follow strong cybersecurity practices.

Frequent Security Alerts

Don't ignore repeated alerts from security software or tools. They may indicate an ongoing or imminent attack. Review logs regularly.

Anomalies in Privilege Use

Monitor for unusual admin activities, such as privilege escalation or access to restricted systems without a valid reason.

Top Cybersecurity Dos and Don'ts

In order to effectively ensure the cybersecurity measures are capable of properly preventing cyberattacks from occurring, proper practice of the precautionary measures are to be observed to minimise potential loopholes in its defences.

Do's	vs	Don'ts
► Encrypt data in transit and at rest ► Enforce strong IAM and access Controls ► Monitor cloud activity continuously	Cloud Security	► Store sensitive data without encryption ► Allow public or excessive access
► Encrypt data in transit and at rest ► Enforce strong IAM and access Controls ► Monitor cloud activity continuously	Personal Data Protection	► Collect or retain unnecessary data ► Share data without consent
► Review contracts & SLAs regularly ► Embed cybersecurity & data protection clauses ► Validate vendor security controls	Agreements & Compliance	► Rely on outdated agreements ► Assume vendor compliance
► Keep devices patched and protected ► Enforce MFA for system access	Endpoint Security	► Ignore security alerts ► Rely only on passwords
► Train staff on phising risks ► Verify requests via secure channels	User Awareness	► Click suspicious links or attachments ► Act on urgency or fear
► Independently verify caller identity ► Educate staff on deepfake risks	AI & Voice Based Fraud	► Trust unsolicited calls ► Ignore AI-driven fraud threats

Example of Singapore's Cyber Fraud Handling Process

Immediate Response: 24 - 48 Hours

- Isolate the Incident
- Alert Internal Teams
- Secure Evidence
- Engage a Cybersecurity Specialists

Engage Law Enforcement & Relevant Authorities

- Report to the Singapore Police Force (SPF)
- Notify the Cyber Security Agency (CSA)
- Involve the Monetary Authority of Singapore (MAS)

Internal Investigation & Forensic Analysis

- Identify the Entry Point
- Access the Extent of the Damage
- Engage a Forensic Team

Legal and Financial Considerations

- Legal Counsel
- Review Insurance Policies
- Potential Liabilities
- Work with the Board

Communication Strategy: Internal & External

- Internal Communication
- External Communication
- Work with PR Communication

Recovery & Restoration

- System Restoration
- Data Recovery
- Strengthen Defences

Post-Incident Analysis & Reporting

- Conduct a Post-Incident Review
- Implement Security Training

Prevention: Strengthening Cyber Resilience

- Regular Security Audits
- Cybersecurity Awareness Programme
- Engage with a Professional Organisation

Cyber Fraud – How is it dangerous?

Cyber Fraud is one of the most well-known cyber threats in the world of cybersecurity and one that may cause significant risks to a company. Through deceptions or theft via the internet, Cyber Frauds can lead an organisation to financial, reputational and operational risks.

In the case for Singapore, being a financial hub, it is highly exposed to cyber threats. In order to counter these attacks, policies such as the PDPA and Cybersecurity Act 2018 have been put in place in order to govern the occurrence of such threats.

Visuals designed by Freepik

Contact us

CLA Global TS Business Advisors – Data Governance

Pamela Chen
Director, Head of Risk Advisory
Data Governance,
Sustainability & Climate Change
pamelachen@sg.cla-ts.com

Maria Teo
Director, Risk Advisory
Data Governance,
Sustainability & Climate Change
mariateo@sg.cla-ts.com

CLA Global Indus Value Consulting Business Advisors

Kartik Radia
CEO
kartik.radia@claivc.com

Vikas Kumta
Director, Cyber Security
vikas.kumta@claivc.com

Xavier Sahaya
CISO
xavier.sahaya@claivc.com

T: (+65) 6534 5700
connect@sg.cla-ts.com
cla-ts.com

CLA Global TS
The Growth Strategist For Asia