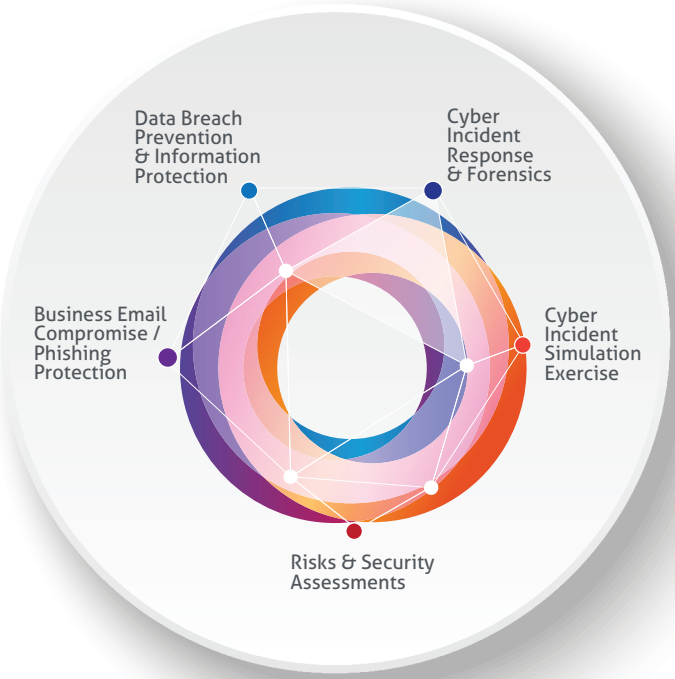
RAJAH & TANN

CYBERSECURITY

A member of Rajah & Tann Technologies group



R&TCYBERSECURITY

Safeguarding your Digital Assets

Rajah & Tann Cybersecurity is uniquely placed to help clients protect, mitigate against attacks, minimise disruptions from a security breach and effectively deal with a data breach.

COMPREHENSIVE SUITE OF SERVICES

We offer end-to-end services that cover the entire risk management lifecycle in your operations and ensure they maintain a robust cybersecurity solutions strategy.

PROFESSIONAL DOMAIN EXPERTS

Led by highly experienced technical experts in the field of security services and consultancy, we are a market leader in providing comprehensive pre and post incident security services.

BEST-OF-BREED CYBERSECURITY SOLUTIONS

We partner with other solution experts who will implement appropriate security solutions to improve your security posture.

A Member of Rajah & Tann Asia

Cambodia | China | Indonesia | Lao PDR | Malaysia | Myanmar | Philippines | Singapore | Thailand | Vietnam

OUR SERVICES

Data Breach Prevention & Information Protection
Develop and implement data breach prevention strategy to identify, monitor and protect your valuable business information.

Business Email Compromise / Phishing Protection
Provide advice on phishing protection, prevention of malware or ransomware intrusion, and domain name spoofing.

Cyber Incident Response & Forensics
Assist in setting up a Cyber Incident Response System with processes based on ISO standards. Provide staff training, conduct regular table- top exercises and develop a Cyber Incident Response playbook per scenario for each system.

Cyber Incident Simulation Exercise
Designed to be as realistic as possible, participants are engaged through immersive and engaging exercises to assess your organisation's ability to prevent, detect and respond to cyberattacks. These exercises also prepares your organisation in responding to cybersecurity incidents.

RISKS AND SECURITY ASSESSMENTS

Configuration Audit
Assess the system hardening configurations against industry-accepted security standards.

Personal Data Protection
Advise organisations using our DEFICIT© framework to minimise the risk of data leakages from your internal network or from publicly accessible web servers more effectively.

Incident Response and Investigation
Set up Incident Response (IR) capability with processes based on international standards, develop Incident Response playbooks for common attack scenarios, design IR team structure and conduct regular table-top or cyber-range exercises.

Privacy Impact Assessment (PIA)
Identify the effectiveness of your organisation's personal data protection and compliance with privacy laws.

Information Security Risk Assessment
Identify, understand and prioritise risks in your IT systems to determine measures to mitigate, reduce, remove or transfer risks.

Source Code Security Review and Training
Conduct independent security review of source codes (including Java and .Net) and secure coding awareness training for your development team.

IT Architecture Security Review
Improve your security posture to ensure greater confidentiality, integrity and availability of your critical IT services.

Vulnerability Assessment and Penetration Test (VAPT)
Provision of network, operating system and web application VAPTs, including HTTP / SMTP Distributed Denial of Service (DDoS) assessments.

PRE-INCIDENT

- (Technical) Privacy Impact Assessment (ISO/IEC 29134)
- Architecture Review (NIST 800-53r4/CSF/CIS Controls)
- Log or Security Information Event Management (SIEM) Review
- Development of Incident Response Plan and Playbooks
- Vulnerability Assessment
- Penetration Testing (by CREST-accredited and ISO/IEC 27001-certified parties)
- Source Code Security Review
- Incident Response Simulation Exercises
- Provide Dark Web Intelligence
- Compliance Review and Audit
  Review gaps and identify areas of improvement against regulatory standards such as MAS TRM and Cyber Hygiene Notices

POST-INCIDENT

- Incident Response (remote and onsite)
- Identification, Containment, Eradication
- Forensic Imaging and Analysis
- e-Discovery and Investigation
- Malware Reverse Engineering
- Threat Hunting
- Technical Advisory Support for Responses to Regulators
- Lessons Learnt Workshops.
- Post-Incident Controls Verification
- Dark Web Monitoring for Post-Mortem Transmission