VAUGHN INTERNATIONAL

Cybersecurity Solutions

Secure Today. Resilient Tomorrow.

Comprehensive cybersecurity capabilities designed to protect people, systems, networks and critical business data - while strengthening long-term cyber resilience.

A business-first cybersecurity approach

Assessment | Governance | Protection | Monitoring | Response | Recovery | Continuous Improvement

Capability Overview

Vaughn International Pte Ltd

CYBERSECURITY CAPABILITY

Building Cyber Resilience

Digital transformation creates opportunity, but it also increases exposure to cyber threats. Vaughn International supports organisations across the cybersecurity journey - from identifying risks and strengthening governance to protecting infrastructure, monitoring threats, preparing for incidents and maintaining business continuity.

How we position the service

Cybersecurity capabilities are delivered through Vaughn International and its specialist technology and cybersecurity ecosystem. Where formal certification or regulated specialist services are required, qualified providers can be engaged as appropriate.

Our cybersecurity capability areas

Cyber Assessment

Security posture reviews, gap analysis and prioritised remediation planning.

Governance & Risk

Policies, management accountability, asset identification and cybersecurity risk management.

Certification Readiness

Preparation aligned with recognised cybersecurity frameworks, including Cyber Essentials and Cyber Trust principles.

Managed Network Security

Firewall protection, network visibility, threat prevention and secure access controls.

Endpoint & Human Defence

Endpoint protection, malware defence, phishing awareness and employee cyber education.

Data Resilience

Backup, Microsoft 365 protection, recovery planning and business continuity.

Monitoring & Response

24/7 monitoring options, threat alerts, incident response and cyber recovery.

Sector Support

Cybersecurity readiness for organisations with sensitive data and sector-specific requirements.

Our operating philosophy

We look beyond individual security products. Our approach considers the organisation's business objectives, people, digital assets, infrastructure, data sensitivity, regulatory environment and existing cybersecurity maturity before defining appropriate controls.

01-02

Assessment, Governance & Risk Management

1. Cybersecurity Assessment & Health Check

Strong cybersecurity begins with understanding where an organisation stands today. Our assessment services evaluate existing security controls, technology environments, operational processes and potential vulnerabilities.

- Existing cybersecurity controls and IT infrastructure
- Hardware, software and digital assets
- Network architecture and access-control practices
- Data-protection and endpoint-security measures
- Malware and antivirus protection
- Software and security-update practices
- Backup and recovery capability
- Incident-response preparedness
- Cybersecurity policies, procedures and employee awareness

Outcome

A structured view of existing risks, identified gaps and recommended remediation priorities - tailored to the organisation's size, operations, digital complexity and risk exposure.

2. Cybersecurity Governance & Risk Management

Cybersecurity is not solely an IT responsibility. Effective resilience requires management accountability, clear policies and security practices that extend throughout the organisation.

Management Accountability

Establish responsibility, ownership and oversight for cybersecurity.

Cybersecurity Policies

Develop practical policies aligned with operational requirements.

Asset Identification

Identify the systems, hardware, software, data and people requiring protection.

Risk Assessment

Identify cyber risks and determine controls based on business impact and exposure.

Security Procedures

Structure access, backup, updates, incident management and related processes.

Cyber Awareness

Build employee understanding so people become an active part of the defence.

03-04

Certification Readiness & Network Security

3. Cyber Essentials & Cyber Trust Readiness

For Singapore organisations seeking to strengthen their cybersecurity posture, Vaughn International can facilitate specialist advisory and implementation support aligned with recognised cybersecurity frameworks, including the principles underlying Singapore's Cyber Essentials and Cyber Trust programmes.

- Cyber governance and management oversight
- Employee cybersecurity awareness
- Hardware and software management
- Information asset protection
- Secure access and secure configuration
- Malware protection and software updates
- Data backup and recovery
- Incident-response readiness and cyber resilience

Where certification is required, organisations can be supported in preparing for the relevant assessment and certification process through qualified specialist providers.

4. Managed Firewall & Network Security

The network is one of the primary gateways into an organisation. Managed firewall and network-security solutions can provide layered controls to monitor activity, control access and reduce exposure to malicious or unauthorised traffic.

Unified Threat Management

Integrated controls that address multiple categories of cyber threat.

Network Monitoring

Visibility into network activity to identify unusual or potentially malicious behaviour.

Intrusion Prevention

Detection and prevention of potentially harmful network activity.

Advanced Malware Protection

Additional controls against malicious files, applications and emerging threats.

Web & Content Filtering

Policies that reduce exposure to dangerous websites and harmful content.

Access Control

Security policies defining who or what can access specific systems and information.

Real-Time Visibility

Monitoring and analytics that improve awareness of the network-security environment.

Scalable Deployment

Solutions can scale based on users, endpoints, locations and security requirements.

05-06

Endpoint Protection & Human Defence

5. Endpoint Protection

Every laptop, desktop, workstation, server and connected device can become an entry point for a cyberattack. Endpoint security should therefore operate as part of a layered defence model.

- Malware and ransomware protection
- Protection against malicious downloads and unauthorised applications
- Detection of suspicious endpoint or network behaviour
- Protection from compromised websites and emerging threats
- Integration with access controls, network monitoring and security policies

Layered protection

Endpoint controls are most effective when combined with network security, secure configuration, identity and access management, monitoring and employee awareness.

6. Phishing & Social Engineering Defence

Cybercriminals frequently target people rather than systems, using phishing emails, fraudulent links, impersonation and social engineering to obtain credentials or gain access to corporate environments.

- Cybersecurity and phishing awareness initiatives
- Social-engineering education
- Employee security training
- Recognition of suspicious communications and links
- Practical security best-practice guidance
- Organisation-wide awareness programmes

The objective is to make employees an active line of defence by improving their ability to recognise, question and report suspicious activity before it becomes a security incident.

07-08

Data Backup, Recovery & Microsoft 365 Protection

7. Data Backup & Business Continuity

Cybersecurity is not only about preventing an attack. Organisations must also be able to recover when systems, applications or information become unavailable.

Backup and business-continuity solutions can help protect mission-critical information and restore operations following cyberattacks, ransomware, hardware failures, accidental deletion, data corruption or wider operational disruption.

Automated & Scheduled Backup

Reduce reliance on manual backup processes and maintain repeatable protection.

Cloud & Flexible Storage

Support resilient storage strategies appropriate to operational requirements.

Recovery Planning

Define how critical systems and data should be restored following disruption.

Restore Testing

Validate that backups are recoverable rather than simply assuming they are usable.

Backup Health Checks

Monitor backup status and identify failures or protection gaps.

Business Continuity

Align recovery strategies with operational priorities and recovery objectives.

Core objective

Protect critical information and maintain a reliable path back to normal operations.

8. Microsoft 365 Data Protection

For organisations that rely on Microsoft 365, additional backup protection can provide an independent recovery capability for Exchange/email, Microsoft Teams, SharePoint and OneDrive data.

- Automated and scheduled backup
- Recovery from accidental deletion or corruption
- Protection against compromised or inaccessible cloud data
- Additional resilience for critical collaboration and productivity information

09-10

Continuous Monitoring & Incident Response

9. 24/7 Cybersecurity Monitoring & Alerts

Cyber threats do not operate according to business hours. Continuous monitoring can improve visibility and enable earlier identification of suspicious activity or security events.

- 24/7 security monitoring options
- Automated security alerts
- Threat detection and network monitoring
- Firewall and endpoint monitoring
- Security-event visibility and analytics
- Escalation of identified threats
- Specialist technical support

Why monitoring matters

Earlier identification of abnormal activity can improve the organisation's ability to contain threats and reduce potential operational impact.

10. Incident Response & Cyber Recovery

Even organisations with strong preventive controls must prepare for the possibility of a security incident. A defined response framework helps teams act with greater speed and confidence during a cyber event.

Identify
Recognise and validate potential cybersecurity incidents.

Contain
Limit the spread or impact of an identified threat.

Respond
Coordinate technical and organisational actions.

Recover
Restore affected systems, services and information.

Review
Understand what happened and strengthen controls to reduce recurrence.

Improve
Feed lessons learned into policies, controls, training and future preparedness.

11-13

Access, Configuration & Data Protection

11. Access Control & Secure Configuration

Protecting information requires ensuring that the right people have access to the right systems - while preventing unnecessary or excessive access.

- User-access and role-based access management
- Privileged-access controls
- Password and authentication policies
- Device and network configuration
- Firewall rules and application-security settings
- System permissions and secure-configuration standards

12. Software Updates & Vulnerability Reduction

Unpatched or outdated software can expose organisations to vulnerabilities that attackers may exploit. A mature cybersecurity programme should include repeatable processes for maintaining supported and secure systems.

- Maintain current software versions
- Apply security updates and critical patches
- Identify unsupported or obsolete software
- Review technology assets periodically
- Reduce unnecessary applications and exposed services

13. Data Protection

Information is one of an organisation's most valuable assets. Data-protection practices should support confidentiality, availability and protection against unauthorised alteration or loss.

- Identification and classification of critical information
- Access controls and permissions
- Secure storage and transmission
- Backup and recovery
- Information-handling policies
- Protection against unauthorised access, accidental loss and malicious activity

14-15

Sector Cybersecurity & Remediation

14. Cybersecurity for Healthcare Organisations

Healthcare organisations operate in an environment where cybersecurity is especially important because of sensitive patient, clinical and operational information. Specialist support can help strengthen cybersecurity readiness across both technical and organisational controls.

- Patient-data and healthcare IT protection
- Access management and secure configuration
- Cybersecurity policy development
- Backup and recovery
- Incident-response planning
- Security assessment and gap analysis
- Remediation planning
- Employee security awareness
- Cybersecurity and compliance readiness

For organisations operating in Singapore's healthcare environment, specialist support can also help teams understand cybersecurity and data-security requirements relevant to their systems and operations.

15. Cybersecurity Remediation

Finding a vulnerability is only the beginning. Following an assessment, organisations need a practical remediation roadmap that prioritises gaps according to severity, business impact and operational importance.

- Strengthen access controls and policies
- Implement or improve endpoint and firewall protection
- Improve backup arrangements and recovery readiness
- Update software and reduce known vulnerabilities
- Strengthen network-security architecture
- Establish or enhance incident-response procedures
- Improve employee cybersecurity awareness
- Introduce monitoring, alerting and stronger data-security practices

From assessment to action

Identify gaps -> prioritise risks -> implement improvements -> validate controls -> monitor -> continuously improve.

INTEGRATED MODEL

An End-to-End Cybersecurity Approach

Effective cybersecurity requires multiple layers of defence working together. Vaughn International considers six essential areas when helping organisations strengthen their security posture.

ACCOUNTABILITY
Management ownership, policies, awareness and clearly defined responsibilities.

ASSETS
Understand and manage people, hardware, software, networks and data.

PROTECT
Apply malware protection, firewalls, endpoint controls, secure configuration and access controls.

UPDATE
Keep operating systems, applications and critical software appropriately updated.

BACKUP
Maintain secure, recoverable copies of important business information.

RESPOND
Prepare to detect, manage, contain and recover from cybersecurity incidents.

Why Vaughn International?

Business-Focused Cybersecurity
Security measures designed to protect the organisation without unnecessarily restricting operations.

Specialist Technology Ecosystem
Access to established cybersecurity expertise, solutions and professional support through a specialist ecosystem.

Scalable Solutions
Support for SMEs beginning their cybersecurity journey through to organisations with more complex digital operations.

End-to-End Approach
Assess -> Identify -> Protect -> Monitor -> Respond -> Recover -> Improve.

Security Around Your Organisation
Solutions shaped by industry, users, endpoints, infrastructure, regulation, data sensitivity and risk exposure.

Practical Remediation
Prioritised improvement plans that turn assessments into actionable security enhancements.

Build a more cyber-resilient organisation
Whether strengthening existing infrastructure, protecting critical information, improving business continuity or preparing for recognised cybersecurity standards, Vaughn International can help establish the security foundation required for a more resilient digital future.

PROTECT YOUR PEOPLE | PROTECT YOUR SYSTEMS | PROTECT YOUR DATA | PROTECT YOUR BUSINESS

Talk to Vaughn International about your cybersecurity requirements.