**Seven Habits of Cyber Security for SMEs**

| Security Aspects | Control Rationale | Best Practices | Self-Assessment (Click all that applicable) |
|---|---|---|---|
| 1. Security Policy and Security Management | Security Policy is an important document in an organization. It dictates security requirements and attitude of senior management with respect to cybersecurity risk management. Senior management should setup a mechanism to maintain and disseminate the requirements of security policy to staff in a regularly basis. | ✓ Staff should be given a chance to read through the security policy, understand security requirements of the organization and acknowledge to conform when they onboard.<br>✓ The policy should be put in somewhere the staff can refer to easily.<br>✓ Policy should be updated and let the staff to re-acknowledge the policy regularly. | ☐ My organization does not have a security policy<br>☐ My organization has a security policy<br>☐ The security policy can be easily accessed by staff<br>☐ Staff needed to acknowledge the security policy when they onboard<br>☐ Staff needed to re-acknowledge the security policy regularly |

| | | | |
|---|---|---|---|
| 2. Endpoint Security | Endpoint refers to personal computers or notebook computers used by staff to access business information during work. Email communication, web browsing and other business applications are all run on endpoints. Attackers would like to compromise the endpoint since it can be used as an entry point to access valuable information assets of the organization. | ✓ Endpoint computers should be protected by security software like anti-virus and anti-malware software.<br>✓ Signatures and security software should be kept up-to-date to protect the endpoint from most recent threats.<br>✓ Security patches for endpoint computer operating system should also be kept up-to-date.<br>✓ IT staff should monitor the update status of the endpoints as well.<br>✓ User accounts on endpoint should be non-privileged (not Administrator)<br>✓ Proxy server used to filter malicious URLs during web browsing | ☐ My organization does not have any endpoint protection software installed<br>☐ My organization has endpoint protection software installed but don't know if signatures are up-to-date or not<br>☐ My organization has endpoint protection software installed and signatures are kept updated regularly<br>☐ IT staff regularly check the update status of endpoint protection software<br>☐ Security patches for endpoint computer operating system are not updated regularly<br>☐ Security patches for endpoint computer operating system are updated regularly |

| | | | |
|---|---|---|---|
| | | | ☐ Accounts used by user on endpoints are non-privileged<br>☐ Proxy server(s) is setup to filter malicious URL during web browsing |

| | | | |
|---|---|---|---|
| 3. Network Security | Most organizations would make use of Internet to facilitate business information exchange. Internet connection inherits network security risks that external attackers may intrude the organization network from outside. Firewall, Internet facing servers and other network devices should be configured properly to avoid intrusion. | ✓ Firewall should be configured properly that minimize network ports of organization network exposing to the Internet.<br>✓ Default rule on firewall should be "DENY". Only "ALLOW" certain traffic based on business needs<br>✓ Do not allow ANY from internal network to have access to Internet. Only allow approved IP addresses to have Internet access instead.<br>✓ Do not allow remote access (e.g. RDP) from Internet to internal servers<br>✓ Firewall rules should be reviewed regularly | ☐ My organization does not have a firewall to protect organization network<br>☐ My organization has a firewall to protect organization network<br>☐ Firewall(s) has a default "DENY" rule<br>☐ Firewall(s) does not allow ANY from internal network to access Internet<br>☐ Firewall(s) does not allow remote access<br>☐ Firewall rules are reviewed regularly |

| | | | |
|---|---|---|---|
| 4. System Security | Organizations make use of information systems to process business information. Some systems (e.g. web servers) are open to Internet to provide/collect information to/from the Internet. These systems are target of attackers since the information the systems contained are valuable. System security guidelines and practices should be developed for mission critical systems. | ✓ Password policy should be configured such that passwords of server should meet minimum length and complexity requirement<br>✓ Servers should be configured securely (called hardened) with security policies enabled and unused services disabled<br>✓ System patches should be updated timely to protect from recent threats<br>✓ Internet facing servers should avoid storing sensitive information. Sensitive information should be masked or encrypted when stored in servers<br>✓ Input from Internet users (e.g. web server forms) should be filtered properly in application to avoid SQL Injection type of attack<br>✓ For critical systems serving the public and performing critical | ☐ My organization has server password policy that passwords needed to meet minimum length and complexity requirement<br>☐ My organization has security guideline for servers that enable security features and disable unused services<br>☐ My organization has a process that update system patches regularly & timely<br>☐ Sensitive information is not stored in Internet facing servers.<br>☐ Sensitive information is masked or encrypted when stored<br>☐ Application(s) has built-in controls to filter user input to avoid SQL Injection type of attack |

| | | | |
|---|---|---|---|
| | | missions, periodical penetration test should be performed by professional parties | ☐ Periodical penetration test(s) is performed regularly by professional parties on mission critical systems |

| | | | |
|---|---|---|---|
| 5. Security Monitoring | There is no way to ensure 100% security of endpoints, servers and network. Organizations should setup mechanism to monitor and detect if something suspicious is happening in information systems. The earlier a threat is identified, the earlier actions can be taken. The potential damage of the threat can then be minimized. | ✓ Logging should be enabled in network devices (e.g. firewall) and servers<br>✓ Logs should be centralized somewhere within the organization for periodical review and monitoring<br>✓ Review of the logs should be timely such that detected issues are taken care properly<br>✓ Network traffic (e.g. Internet traffic) should be monitored to detect if any abrupt change in traffic pattern. | ☐ Logging is enabled in my organization's firewall(s) and servers<br>☐ Logs are collected in a centralized log server<br>☐ Logs are periodically reviewed by IT staff<br>☐ Mechanisms are setup to notify IT staff if something abnormal is detected<br>☐ Network traffic pattern is included in monitoring |

| | | | |
|---|---|---|---|
| 6. Incident Handling | System outages due to system issues or security incidents are not 100% avoidable. Organization should develop incident response plans for different kinds of scenarios including small incidents like malware infections all the way to big incidents that require system restoration. | ✓ Incident response plans (including different kinds of security incidents) are developed according to different scenarios<br>✓ Systems and data are backup regularly, the backups are taken offline (and even offsite)<br>✓ Restore procedures are drilled to make sure that the backup can be restored properly | ☐ My organization does not have any incident response plans<br>☐ My organization has incident response plans that handle different kinds of incidents<br>☐ My organization has backup plan for systems and data<br>☐ Backup data is kept offline<br>☐ Drills are done on restore plan regularly to make sure backups are restorable |

| | | | |
|---|---|---|---|
| 7. User Awareness | Users are the weakest links in cyber security. 95% security incidents involved human as a contributing factor. Organizations should ensure that staff understand their roles and responsibility in protecting information assets of the organization. | ✓ Staff should be reminded their roles and responsibility in protecting information assets of the organization regularly, e.g. by staff awareness training<br>✓ Drills (e.g. simulated phishing attacks) can be performed to test the readiness of staff against common cyber attack | ☐ My organization does not have any security awareness activity for staff<br>☐ My organization has periodical security awareness training for staff<br>☐ My organization performs simulated test to assess readiness of staff against common cyber attack |

**Self-assessment score calculation**

Score = number of ✓ in blue box - number of ✓ in yellow box

33 to 26: Robust and adequate security
25 to 18: Adequate security
19 to 10: Security to be strengthened
11 to 3: Vulnerable
2 to -5: Most vulnerable