Cybersecurity Toolkit for Small & Medium Businesses by

SECURING THINGS

FOR SMART & SAFER SOCIETY

Author: M. Yousuf Faisal

Global Threat Landscape for Small & Medium Businesses (SMBs)

SECURING THINGS

Cybercriminals / Attackers have been increasingly targeting SMBs globally in recent years; see below:

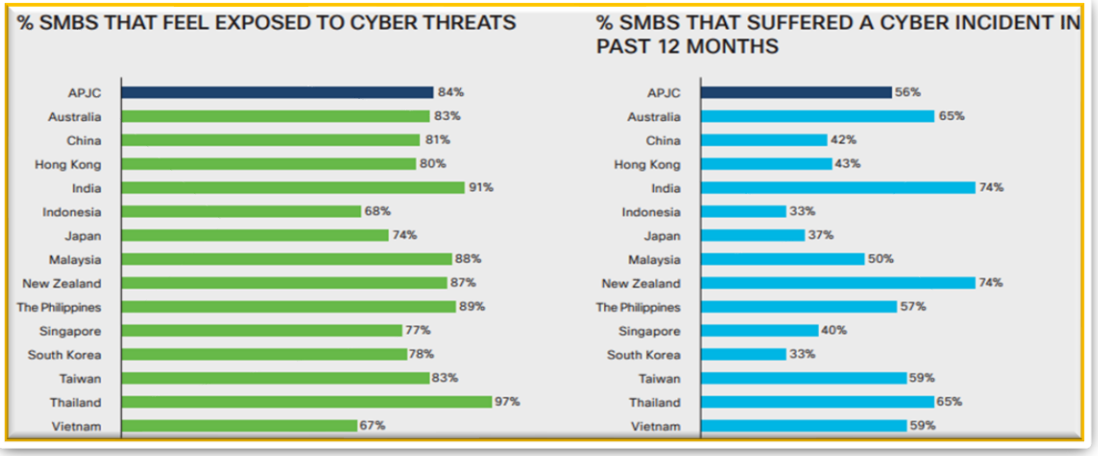
Industry Threat Landscape	• **2021 & 2022** saw nearly a **200% increase** in incidents for organizations with <1,000 employees)*. • **70%** of **Attacks** are targeted for Small & Medium Size Business* • **50% became unprofitable** within a month of being breached* • Average **cost of a data breach** for small businesses is **$383K** to **$2.98 million***. • **56%** of **SMBs in APAC** suffered a cyber incident *(per Cisco Asia Pacific Businesses Prepare for Digital Defense)*
Most common cybersecurity threats of 2023 include	Few key examples: • Ransomware • Security misconfigurations and unpatched systems • Credential stuffing • Social engineering • Phishing / Targeted Phishing Attacks • Malware infections • SQL Injections, Man-in-the-Middle, DDOS & others.
SMBs To Action ~	• **Identify** (Assets & Vulnerabilities/Risks) – Know what you have & why you need to protect it • **Protect (& Predict)** (Assets & fix vulnerabilities/Address Risks) – Know what you have & how you must protect it • **Detect** (Threats & Incidents) – Know what's happening in your environment • **Respond** (to Alerts & Incidents) – Know how to react to incidents • **Recover** (from Incidents) – know how to bring business back to normal operations. **See next few slides (After APAC Threat Landscape slide) for each of these actions:**

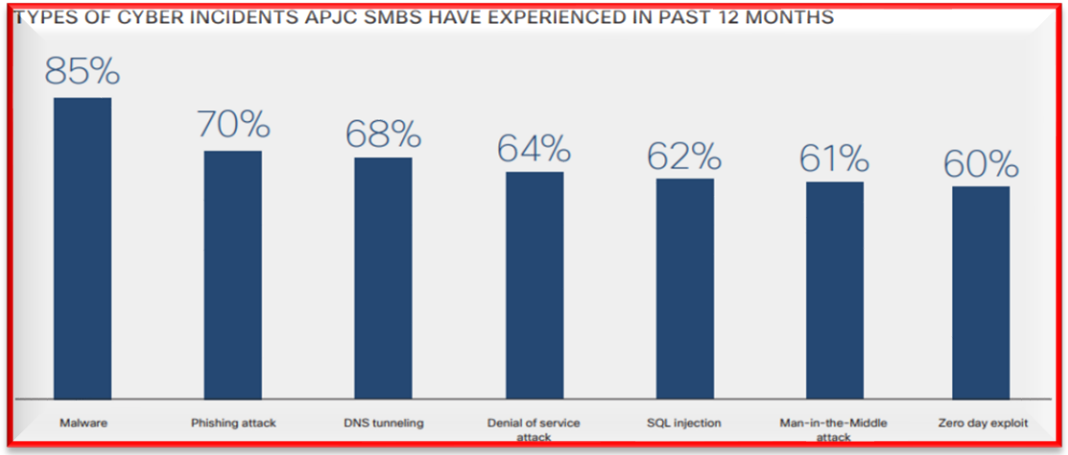
* References – Forbes | Tech Republic | Better Business Bureau | Forbes. Most Common Cyber Security Threats In 2022. August 2022 | Verizon Data Breach Investigation Report | Forrester Study | Cisco.

APAC Threat Landscape for Small & Medium Businesses (SMBs)

SECURING THINGS

Source: Cisco Asia Pacific Businesses Prepare for Digital Defense Report 2021





ESCALATION OF IMPACT DUE TO LENGTH OF DOWNTIME

	APJC	Australia	China	Hong Kong	India	Indonesia	Japan	Malaysia	New Zealand	The Philippines	Singapore	South Korea	Taiwan	Thailand	Vietnam
Amount of downtime before your organization's operations are severely impacted															
Under one hour	15%	10%	21%	11%	17%	18%	10%	13%	17%	16%	7%	10%	21%	18%	8%
One to two hours	29%	25%	28%	21%	32%	35%	18%	32%	39%	28%	23%	29%	28%	31%	30%
Amount of downtime before your revenue is severely impacted															
Under one hour	13%	8%	16%	12%	12%	25%	7%	16%	9%	15%	10%	14%	14%	14%	9%
One to two hours	24%	20%	26%	21%	24%	27%	17%	23%	19%	27%	20%	19%	34%	28%	20%
Amount of downtime before you may face regulatory or legal implications															
Under one hour	13%	7%	16%	14%	13%	19%	6%	17%	8%	13%	11%	13%	18%	14%	12%
One to two hours	22%	19%	24%	18%	24%	32%	15%	23%	20%	19%	24%	21%	25%	22%	17%

% SMBS AND LENGTH OF TIME TAKEN TO DETECT AND REMEDIATE AN INCIDENT

	APJC	Australia	China	Hong Kong	India	Indonesia	Japan	Malaysia	New Zealand	The Philippines	Singapore	South Korea	Taiwan	Thailand	Vietnam
The average length of time it took to detect an incident															
Under one hour	15%	8%	13%	11%	17%	17%	16%	17%	24%	9%	8%	11%	25%	13%	8%
One to two hours	30%	28%	36%	28%	34%	31%	18%	32%	28%	28%	16%	34%	16%	33%	33%
The average length of time it took to remediate the incident															
Under one hour	10%	6%	8%	3%	12%	12%	9%	12%	11%	9%	5%	4%	16%	7%	3%
One to two hours	23%	20%	31%	26%	23%	27%	13%	21%	17%	22%	21%	18%	21%	26%	24%

FINANCIAL IMPACT OF CYBER INCIDENTS OVER PAST 12 MONTHS (US$)

	APJC	Australia	China	Hong Kong	India	Indonesia	Japan	Malaysia	New Zealand	The Philippines	Singapore	South Korea	Taiwan	Thailand	Vietnam
$500,000 or more	51%	64%	41%	39%	62%	43%	49%	32%	62%	28%	51%	58%	27%	47%	30%
$1 million or more	13%	33%	3%	10%	13%	12%	6%	6%	18%	10%	11%	10%	2%	28%	4%

Cybersecurity Toolkit for Small & Medium Businesses (SMBs)

SECURING THINGS

Mapped to Industry best practices – NIST Cybersecurity Framework Concept – For Illustrative Purposes Only.

Cybersecurity Lifecycle Stage	**Identify – Know what you have & why you need to protect it ~**
To-Do (Actions to take) – ***(Implement a combination of Administrative & Technical Controls)***	**1(a) – Identify all Assets and build an Asset Inventory (maintain and keep it up-to-date) :** ▪ Devices (desktops/laptops/smart phones, tablets, printers, IOT, routers, cctv etc.) ▪ Applications (/Accounts) (email, website/web/SaaS apps, software, social media etc.) ▪ Data (business plans, client/personal info, financial, etc.) ▪ In addition, also identify all suppliers/service providers that may impact the security of your business. **1(b) – Identify Risks -** Discover Vulnerabilities, Threats, and associated Risks across your CIA triad (note: don't forget risks related to compliance/regulations, natural events, and or attacks in terms of fines/damages) & forecasting likelihood, impact & consequences.
Additional Remarks on Asset Inventory & Risk Management	For # 1 (a): • Without knowing what you've; you can't protect it. • Knowing what assets you have is the first step, so you can secure them. • Inventory serves as a guide or a checklist for the rest of your cybersecurity journey. • Use both manual or automated means to perform Asset Discovery (Scans) and or Management Tools (local or SaaS based)* For # 1 (b): • Discover cyber risks to the business (for your brand & operations) across CIA triad (confidentiality, integrity & availability) needs • Build Risk Management Framework & maintain Risk Register (start with basic and continue expanding to document risks & treatment).

* Both Free & Commercial tools options are available to address your cybersecurity needs *(contact SecuringThings for more details)*

Cybersecurity Toolkit for Small & Medium Businesses (SMBs)

SECURING THINGS

Mapped to Industry best practices – NIST Cybersecurity Framework Concept – For Illustrative Purposes Only.

Cybersecurity Lifecycle Stage	**Protect (& Predict) – Know who & how you must protect it**
To-Do (Actions to take) – ***(Implement a combination of Administrative & Technical Controls)***	• **2 – Cybersecurity Education & Awareness –** Subscribe to industry news, security advisories/email alerts from vendor neutral sources / vendor products/solutions used and ensure continued security awareness trainings for staff (start with general awareness & move to role specific trainings). • **3 – Patch & Configuration Management** – Keep your devices and applications up to date & secure via regularly updating/installing latest software security patches / version upgrades. Follow industry/vendor suggested configuration hardening standards / security settings. • **4 – Network Security Controls** – Build, design & maintain secure network & wireless architecture, Apply ZTNA, & VPNS for remote access • **5 – Secure your Digital Presence** – secure your DNS, websites, web/mobile apps, internet browsers, VPNs & Social Media Accounts • **6 – Encrypt Your Data** – both at rest (local, removable media, cloud storage) & in-transit (use only secure means to transfer or exchange data btw systems or networks) • **7 – Go Beyond Simple Passwords** – Use strong password policies, use Multi-factor authentication (MFA) for admin, remote network access, and externally exposed applications) • **8 – Email (Antispam, Phishing) & Malware Prevention** – Harden your email defenses following best practices (SPF/DMARC) & use an updated anti-malware/endpoint protection • **9 – Physical Security Controls** – locks & control entry points/sensitive areas via Access Control / Guards
Additional Remarks	• For #2: Train staff on latest security threats & threats specific to your business via Online/In-person security awareness trainings.* • For #3: Most to all devices (Windows, MAC, IOS, Android)* can be set to Auto-Update themselves – uplift your resilience against attacks. Change all vendor defaults & follow security configuration guidelines • For #4: Network Segmentation/Zones, Secure Wireless architecture/mechanisms, Zero Trust Network Architecture & use VPNs* • For #5: Digital certs, DNS filters/Sec, Ad-blockers, browsers, VPNs, Social Media accounts etc.* • For #6: Data in motion (VPN/HTTPS via internet during transfer)* & at Rest (Native OS/other encryption on hard disk, USB, Cloud storage)* • For #7: Use password managers & / strong AD group policy enforcement* & Use MFA / Privilege Access Management (PAM) tools* • For #8: Use DKIM, SPF, DMARC, Anti-spam, Blacklists, and AV / Endpoint protection tools* • For #9: Keep visitor access logs and or physical access control systems (Proximity Cards / Keys), and your cabinets locked/secured.

* Both Free & Commercial tools options are available to address your cybersecurity needs *(contact SecuringThings for more details)*

Cybersecurity Toolkit for Small & Medium Businesses (SMBs)

SECURING THINGS

Mapped to Industry best practices – NIST Cybersecurity Framework Concept – For Illustrative Purposes Only.

Cybersecurity Lifecycle Stage	**Detect (Threats & Incidents) – Know what's happening in your environment**
To-Do (Actions to take) – ***(Implement a combination of Administrative & Technical Controls)***	• **10 (a) – Enable Logging & Monitoring –** Enable audit logs on all key assets/devices/apps, collect & monitor events and alerts for incidents. (also explore and use services to monitor dark web / threat intelligence gathering). • **10 (b) – Physical Security Monitoring –** monitor sensitive areas of your offices, data centres etc. via CCTV & guards and protect them through physical access control systems and keep your devices secure. • **10 (c) – Supplier/Vendor/Service Provider Security & Monitoring** – monitor the suppliers/services providers for compliance
Additional Remarks	• For #10(a): Use key security technology solutions like Firewall, IPS, Endpoint protection, Log Management / SIEM (local / Hosted) solution*. Also subscribe and or use dark web / threat intelligence services to monitor activities related to your brand/business operations. • For #10(b): Use Physical Access Control System on entry/exist and key sensitive areas in offices (e.g., Server room/Data centers, document storage), practice keeping sensitive physical records in locked cabinets & have them covered under CCTV surveillance/recordings. Use proximity badges/card readers or keys or a combination of these. Also, keep your devices secure and insight all the time. • For #10(c): Review and include security provisions in supplier/vendors/service providers contracts, ensure processes are in place to monitor their conformance / compliance to your policies and make contract / process adjustments as and when required.

* Both Free & Commercial tools options are available to address your cybersecurity needs *(contact SecuringThings for more details)*

Cybersecurity Toolkit for Small & Medium Businesses (SMBs)

SECURING THINGS

Mapped to Industry best practices – NIST Cybersecurity Framework Concept – For Illustrative Purposes Only.

Cybersecurity Lifecycle Stage	**Respond (Alerts & Incidents) – Know how to react to incidents ~**
To-Do (Actions to take) – ***(Implement a combination of Administrative & Technical Controls)***	• **11 - Incident Response (IR) Readiness –** Ensure to develop and document an IR Plan & procedures/playbooks are in place. Perform interna IR tabletops (optionally participate in any local community exercises as well), plus engage a third party IR & cyber insurance contract.
Additional Remarks	• For #11: IR Tools* (EDR, forensics tools, evidence collection, native commands etc.) via staff, 3rd party or Cyber insurance provider • Perform IR tabletop exercises at-least once a year • Have a plan in place to notify local government / sector specific regulators (per local/international notification requirements) and also to consumers, customers, employees and partners who's data maybe at risk. • Report attacks to law enforcements and other relevant authorities.

Cybersecurity Lifecycle Stage	**Recover (from Incidents) – know how to bring business back to normal operations**
To-Do (Actions to take) – ***(Implement a combination of Administrative & Technical Controls)***	• **12 - Data Backup and Recovery –** Take regular backups of all important business data and routinely perform backups of your important personal digital life and test recovering them at-least once a year.
Additional Remarks	• For #12: Local, Network and or Cloud based Backups & Recovery tools (On-prem & Cloud based services option)* • In case of performing recovery from incidents, Keep your customers and employees, informed about the recovery activities/status.

* Both Free & Commercial tools options are available to address your cybersecurity needs *(contact SecuringThings for more details)*

Resilient Cybersecurity Strategy for Small & Medium Businesses (SMBs)

SECURING THINGS

People, Process & Technology Mapped to NIST & Cyber Defense Matrix Concept – For Illustrative Purposes Only.

Pre Event – Structural Awareness (Proactive) | Post Event – Contextual Awareness (Reactive)

	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
PEOPLE (User)	• Asse Acce • AM: • GV: • RA: HK+	• Policy USB, C harde securi	• Polic Mon – P1	• Incid Docu • Data temp	• Recov Recov
TECHNOLOGY (Apps Devices Networks)	• AM: buil or n • AM: & er	• Email: • Centra • Securi • WAP F • MS 36 • Access • Encryp File va • DLP =	• Setu P1 • Cent Senti P3 • Cons • Exter P3	• Use I cons futur loggi supp – P2 • cons	• Select backu backu files/f
PROCESSES (Data Flows / Stages)	• AM: • AM: • GV: D Archi & cor • GV: D build • GV: T each • Incor the o	• Define manag encryp manag users a activati harden	• Audit • Admi – P1 • 12-24	• IR – D • IR – T year • Brea • Repo	• Reco Docu RP p • IR Ta insu • RP – Eval

Hidden Text

DEGREE OF DEPENDENCY

TECHNOLOGY ✸ — **PEOPLE** ✸

PROCESSES ✸

✸ People, Processes and Technology effort or dependency mapped to each stage of Identify | Protect | Detect | Respond | Recover.

SECURING THINGS
FOR SMART & SAFER SOCIETY

SME/SMB Cybersecurity Toolkit – Summary

1 Slide – For Retention

Cybersecurity Toolkit for SMBs – Summary

SECURING THINGS

Mapped to Industry best practices – NIST Cybersecurity Framework Concept - One Page Summary – For Illustrative Purposes Only.

Cybersecurity Lifecycle Stage	To-Do (Actions to take) - Implement a combo of Administrative & Technical Controls	Additional Remarks
Identify – Know what you have & why you need to protect it ~	**1 (a) – Asset Inventory (build & Keep it updated) to Identify:** ▪ Devices (desktops/laptops/smart phones, tablets, printers, IOT etc.) ▪ Applications (/Accounts) (email, software, website/web/SaaS apps, etc.) ▪ Data (PII, Credit Card #s, product designs, business plans, client/personal info, $$$, etc.)	• Without knowing what you've you can't protect it. • Knowing what you have is first step so you can secure them. • It serves as a guide/checklist to rest of cybersec journey. • Asset Discovery (Scans)/Management Tools (local or SaaS)*
	1 (b) – Identify Risks - Discover Vulnerabilities, Threats, and associated Risks across your CIA triad (note: don't forget risks related to compliance/regulations, natural events, and or attacks in terms of fines/damages) & forecasting likelihood, impact & consequences	• Discover cyber risks to your business (brand & operations) across CIA triad (confidentiality, integrity & availability) needs • Risk Management Framework & Risk Register
Protect (& Predict) – Know what & how you have to protect it	**2 – Cybersecurity Education & Awareness** – Subscribe to industry certs/your vendors security advisories/email alerts & train staff on security policies/procedures & best practices	• Train staff on latest security threats & threats specific to your business via Online/In-person security awareness trainings.*
	3 – Patch & Configuration Management – Keep your Devices and Applications up to date & secure via regularly updating/installing latest SW security patches/versions & follow industry/vendor suggested security settings	• Most to all devices (Windows, MAC, IOS, Android)* can be set to Auto-Update themselves – uplift your resilience against attacks • Change all vendor defaults & follow security config. guidelines
	4 – Network Security – Design secure network architecture / ZTNA & remote access, wireless	• Network Segmentation, Wireless Security, ZTNA & VPNs*
	5 - Secure Digital Presence – DNS Security, website, web/mobile apps, browsers, Social Media	• Digital certs, DNS filters/Sec, Ad-blockers, browsers, Secure SMA**
	6 - Encrypt Data (Confidential/Sensitive) – both at rest (local, removable media, cloud storage) & in-transit (use only secure means to transfer or exchange data btw systems or networks)	• Data in motion (use secure means to transfer, VPNs/HTTPS/SFTP)* • Native OS/other encryption tools (local disk, USB & Cloud storage)*
	7 - Go Beyond Simple Passwords – Use strong password policies, use Multi-factor authentication (MFA) for admin/remote network access and for all externally exposed apps.	• Use password managers & strong AD group policy enforcement* • Use MFA / Privilege Access Management (PAM) tools*
	8 – Email (Antispam, Phishing) & Malware Prevention – Harden your email defenses following best practices (SPF/DMARC) & use an updated anti-malware/endpoint protection	• Use DKIM, SPF, DMARC, Anti-spam, Blacklists, and AV / Endpoint protection tools*
	9 – Physical Security – locks & control entry points/sensitive areas via Access Control / Guards	• Visitor & Access Control (Proximity Cards / Keys), locked cabinets.
Detect (Threats & Incidents) – know what's happening in your environment	**10 (a) – Enable Logging & Monitoring** – Enable, collect & monitor logs/alerts on all key assets. **10 (b) – Physical Security Monitoring** – monitor sensitive areas & access control systems **10 (c) – Supplier/Vendor/Service Providers** – monitor contracts and compliance with policies.	• Firewall, IPS, Endpoint protection, Log Management / SIEM Tools* • Physical Access Control System & use CCTV surveillance/recordings • Security Requirements in contracts & monitoring compliance.
Respond (Incidents & Alerts) – Know how to react to incidents	**11 – Incident Response (IR) Readiness** – Ensure IR Plan & procedures are in place. Perform internal tabletops & participate in community exercises, plus 3rd party IR & insurance contract.	• IR Tools* (EDR, forensics tools, evidence collection, native commands etc.) via staff, 3rd party or Cyber insurance provider
Recover (from Incidents) – know how to bring things back to normal operations	**12 – Data Backup and Recovery** – routinely perform backups and test recovery (know & document restore procedures in advance)	• Local & Network based Backup & Recovery tools (On-prem & Cloud based services option)*

* Both Free & Commercial tools options are available to address your cybersecurity needs *(contact SecuringThings for more details)* | ** SMA – Social Media Accounts / Online Accounts

Free References for Small & Medium Businesses (SMBs)

SECURING THINGS

Plenty of Free Resources Available online – a few key examples listed below (not an exhaustive list)

Guidance for Businesses	• CISA Cybersecurity Awareness Program Small Business Resources • CISA's Cybersecurity Guidance for SMBs • CISA's Free Cybersecurity Services & Tools • CISA Cross Sector Cybersecurity Performance Goals (CPGs) report • 10 Steps to Cyber Security NCSC – National Cybersecurity Centre • Small Business Guide – National Cybersecurity Centre • Small and Medium Business Resources by NIST • NIST Small Business Cybersecurity Corner • Cybersecurity for Small Business by Federal Trade Commission • PCI DSS Guidance for Small Merchants • CIS Controls Implementation Guide for SMEs • Cybersecure My Business (Stay Safe Online) by National Cybersecurity Alliance • ACSC (Australian Cybersecurity Centre) Small Business Cybersecurity Guide • UK Cybersecurity Essentials • Canadian Centre of Cybersecurity • & many more..
Trainings	• NCSC Certified Training – National Cybersecurity Centre • HHS Cybersecurity Awareness Training and Security Awareness Trainings • SANS Free Training ACE • Cyber Training Series & many more..
Educational	• YouTube (e.g. https://www.youtube.com/results?search_query=Free+Cybersecurity+Awareness+Training+for+SMBs) • Ted Talks (e.g. 12 Must Watch Cybersecurity Ted Talks) • LinkedIn Learning Trainings, Coursera, Edx and other commercial awareness training offerings. • & many more..

Thanks & wishing all a Great 2023 & beyond

It’s a great day to start …

SECURING THINGS

For Small & Medium Businesses

Contact: info[at]securingthings[dot]com

Author: M. Yousuf Faisal (Founder STL)