Threat Landscape — Small Retail & Service Businesses (1–25 employees)

Small retail and service businesses face a compact set of cyber threats driven by dependence on point-of-sale systems, cloud accounting, remote communication, and limited IT staff. The following list summarizes the most relevant threats, how they operate, common indicators, and the likely impact on a small business.

Phishing (Email & SMS)

How it works: Attackers send malicious emails or SMS pretending to be suppliers, banks, or delivery services to trick staff into revealing credentials or opening malware attachments.

Common indicators: Unexpected invoices, password reset links, spelling/URL mismatches.

Typical impact: Credential theft can expose email, accounting, or payment portals leading to fraud or data breach.

Ransomware

How it works: Malware infects systems and encrypts files or POS data, demanding ransom to restore access. Often delivered through phishing or unpatched software.

Common indicators: Inability to open files, ransom notes, unusual file extensions.

Typical impact: Business operations halt (no POS transactions), causing financial loss and expensive recovery.

POS Compromise & Payment Fraud

How it works: Malware or tampering targets POS terminals to capture card details or perform fraudulent transactions.

Common indicators: Unusual POS network activity, customer complaints, duplicate or invalid transactions.

Typical impact: Leads to financial loss, customer trust damage, and possible legal action.

Weak or Misconfigured Wi-Fi / Routers

How it works: Default passwords or weak encryption on routers allow attackers to access internal networks and sensitive systems.

Common indicators: Unknown devices on Wi-Fi, unchanged router credentials, no guest network.

Typical impact: Enables unauthorized access, network misuse, and potential data theft.

Unpatched Software & Weak Updates

How it works: Outdated operating systems or software vulnerabilities allow attackers to exploit and gain unauthorized access.

Common indicators: Old OS versions, missing updates, unsupported applications.

Typical impact: Increases risk of malware, ransomware, and remote code execution.

Business Email Compromise (BEC) & Supplier Fraud

How it works: Attackers impersonate business owners or suppliers to trick staff into transferring money or changing payment accounts.

Common indicators: Requests with urgency, bank detail changes, email address misspellings.

Typical impact: May cause major financial loss and strained supplier relationships.

Insider Error & Poor Access Control

How it works: Staff mistakes, password sharing, or poor privilege management expose sensitive systems and data.

Common indicators: Shared accounts, weak passwords, lack of access logs.

Typical impact: Leads to accidental data loss or unauthorized access escalation.

Third-party SaaS Misconfiguration & Supply Chain Risk

How it works: Improperly configured SaaS services or compromised vendors expose business data or enable attacker access.

Common indicators: Public file links, unknown admin accounts, vendor service downtime.

Typical impact: Causes data exposure, operational disruptions, and reputational harm.

References: NIST Cybersecurity Framework, MITRE ATT&CK;, Vendor Security Advisories