SMALL BUSINESS CHECKLIST
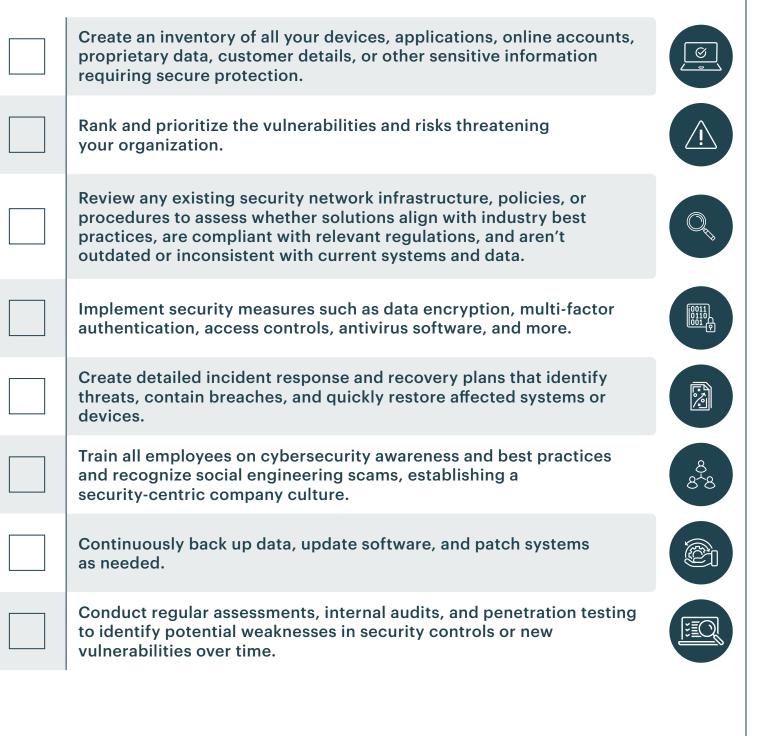
- [ ] Create an inventory of all your devices, applications, online accounts, proprietary data, customer details, or other sensitive information requiring secure protection.

- [ ] Rank and prioritize the vulnerabilities and risks threatening your organization.

- [ ] Review any existing security network infrastructure, policies, or procedures to assess whether solutions align with industry best practices, are compliant with relevant regulations, and aren't outdated or inconsistent with current systems and data.

- [ ] Implement security measures such as data encryption, multi-factor authentication, access controls, antivirus software, and more.

- [ ] Create detailed incident response and recovery plans that identify threats, contain breaches, and quickly restore affected systems or devices.

- [ ] Train all employees on cybersecurity awareness and best practices and recognize social engineering scams, establishing a security-centric company culture.

- [ ] Continuously back up data, update software, and patch systems as needed.

- [ ] Conduct regular assessments, internal audits, and penetration testing to identify potential weaknesses in security controls or new vulnerabilities over time.

RAMPxchange