SMB CYBERSECURITY ESSENTIALS

Address these 30 items as a minimum to help secure your organization.

Use this checklist to better understand privacy concerns and the policies and procedures critical to maintaining a secure organization and a culture of cybersecurity. For more information, see our summaries on the following pages.

PRIVACY PROGRAM

- ☐  01. Internal privacy policy
- ☐  02. Train employees on your privacy policy
- ☐  03. Internal policy for data retention

SECURITY PROGRAM

- ☐  04. Security awareness training of employees and contractors
- ☐  05. Phishing awareness training
- ☐  06. Clean desk policy
- ☐  07. Visitor program
- ☐  08. Identify digital assets
- ☐  09. Multi-Factor Authentication (MFA)

TOOLS

- ☐  10. Use Secure Networks
- ☐  11. Secure Wi-Fi / wireless networking
- ☐  12. Secure Email Gateway (SEG)
- ☐  13. System auditing
- ☐  14. Configure backup solution
- ☐  15. Test backup solution
- ☐  16. Domain Name System (DNS) and content filtering
- ☐  17. Endpoint Detection and Response (EDR)
- ☐  18. Security Incident and Event Management (SIEM)

SYSTEM HARDENING

☐ 

19. Clean up all unused programs on all systems

☐ 

20. Use group policies and active directory

☐ 

21. Secure Endpoint configurations

☐ 

22. Implement perimeter security

☐ 

23. Patch management plan

☐ 

24. Monitor and track behavior in cloud apps

VULNERABILITY AND RISK MANAGEMENT

☐ 

25. Define a vulnerability analysis and resolution strategy

☐ 

26. Vulnerability management program

RESPONSE

☐ 

27. Incident response policy

☐ 

28. Incident response procedures

☐ 

29. Identify roles and responsibilities

☐ 

30. Business continuity and disaster recovery

☐ 

31. Incorporate lessons learned

32. Trusted partners to manage and monitor

☐ 

Security is a shared responsibility. As attacks have grown in number and sophistication, small businesses no longer have the resources to deal with security issues effectively. SMBs are turning to trusted partners to bring enterprise-level skillset and expertise to their organization. In fact, in a recent study, 62% of SMBs believe their organization lacks the skillset to properly handle security incidents*. Partnering with Marco will allow you to address these critical issues.

* The State of SMB Cyber Security in 2019, Continuum, 2019

Ready to Learn More?
Check out the details below.

PRIVACY PROGRAM

01. Internal privacy policy
Your internal privacy policy should cover employee records, email and internet usage, client/customer usage, internal systems and access, mobile devices, laws and regulations, and consequences for violating the policy. Prepare for the need to have a public-facing privacy policy, if you do not already have one.

02. Train employees on your policy
After creating privacy policies, you need to train your staff to ensure they understand the content.

03. Internal policy for data retention
Creating a policy for data retention controls how long your company will retain data. This policy can reduce the impact of a security incident, exposure and data storage costs.

SECURITY PROGRAM

04. Security awareness training of employees and contractors
Implement security awareness training that is tailored to the needs of your organization. Such courses provide employees and contractors with a basic understanding of the physical and cybersecurity threats and how to respond.

05. Phishing awareness training
It is recommended to use a service to regularly test users on their ability to identify phishing emails to determine where additional training is needed.

06. Clean desk policy
A clean desk policy is designed to protect any information and data that may be found at a user's workstation. Requiring the removal or secure storage of sensitive information when employees or workforce personnel are away from their desks, the organization can ensure the confidentiality, integrity, and availability of data.

07. Visitor program
Having a clearly understood visitor policy and escort program is vital to the security of employees, clients, physical assets, and important data. The type of visitor policy needed depends on your office and workspace's type, size and location.

08. Identify digital assets
Conduct, at a minimum, an annual risk assessment that includes a complete digital asset inventory, a report of known threats and vulnerabilities, and an assessment of risk and impact to the business.

09. Multi-Factor Authentication (MFA)
MFA is a preventative authentication method which requires responses to a combination of prompts before allowing access to a system. These prompts may include something you know, something you have, and something you are. These prompts can take multiple forms including passwords, an app on your smartphone to allow/deny, text messages with a code, or biometric methods such as a fingerprint reader. At least two of the three prompt types are needed to achieve MFA.

TOOLS

10. Secure Remote Access
A VPN is an encryption-based communication method that connects a remote office or worker to an organization's private network over a shared or public network. The encryption effectively makes a tunnel within the public network that data can pass through without being read by eavesdroppers.

VPN technologies are a great way to protect your assets while users are outside your company network. More modern technologies such as secure application tunnels, network gateways, and virtual desktop and application tools have provided new ways to enable secure network access and streamline end user efficiency.

11. Secure Wi-Fi / wireless networking
Securing wireless at your organization is a vital component that protects data and ensures the security of critical business systems. At a minimum, ensure these three items are addressed: change the default passwords on access points, keep the firmware up-to-date, and use a separate wireless network for guest access.

12. Secure Email Gateway (SEG)
Email is the primary target hackers use to gain access to private company data. Email is often the least secure means of passing data into and within an organization. Modern methods of attacking email systems have grown in sophistication and the targeting of individuals. Ensure your SEG solution has modern anti-phishing, encryption, data loss prevention (DLP) options. DLP will detect sensitive data and take defined actions such as blocking the message entirely or ensuring data is encrypted. These are often premium features beyond anti-spam.

13. System auditing
Ensure that logging is enabled and that the logs are periodically reviewed by assigned staff to identify potential patterns that may indicate a compromise or ongoing attack.

Many vendors provide or include built-in reporting solutions. Set aside time to periodically review reports including security and access logs.

14. Configure backup solution
One of the best known and least implemented security controls is data recovery, or specifically data backups. An organization may have many processes and utilities for backing up critical information.

A robust backup solution should follow the 3-2-1 backup rule: 3 copies of your data, 2 types of storage and 1 copy off-site.

Sophisticated, modern ransomware attacks are routinely targeting backup environments first to ensure an organization can't recover by simply restoring systems. Consider an air-gap backup solution where a copy is maintained in a disconnected or secured state from the production network. There are various solutions to protect the integrity of your backup data.

15. Test backup solution
Regularly test backup restoration procedures. This process involves testing backup media for reliability and testing the recovery procedure to ensure that the process has been verified. Testing procedures ensures that data can be restored quickly and with minimal issues during a disaster.

16. Domain Name System (DNS) and content filtering
Use the Domain Name System (DNS) layer to filter content based on IP addresses to control web use and reduce infections by blocking sites known to pose a high risk of containing malware. While most firewalls have this capability, once the user leaves the office (remote workforce) they need an agent installed on their laptop or wireless device.

17. Endpoint Detection and Response (EDR)
Endpoint Detection and Response (EDR) is a cybersecurity technology that addresses the need for *continuous monitoring* and *response* to advanced threats. It is a subset of endpoint security technology and a critical piece of optimal security posture. Attackers do not work 8 am to 5 pm, so you need 24x7x365 protection for effective detection and response.

18. Security Incident and Event Management (SIEM)
Security-related logs from all network devices should be collected and stored centrally to provide the ability to correlate events in order to aid in investigations and help identify potentially malicious behavior.

SYSTEM HARDENING

19. Remove unused programs on all systems
Every program installed on an endpoint or server operating system is another potential avenue of potential attack for a hacker.

Removing unnecessary or unneeded programs helps to limit the number of ways into a system.

20. Use group policies and Active Directory
It is recommended to clearly define what groups can access and manage Microsoft Active Directory groups and rules. Occasionally, simple user error can create issues that create opportunities for a successful cyber-attack. Use Group Policy Objects, or GPOs, to push and enforce consistent settings across network devices.

21. Secure Endpoint configurations
This includes reducing the attack surface, strengthening user account controls, enforcing device host firewalls, and implementing secure policies while maintaining reasonable user efficiency. Close unused ports.

22. Implement perimeter security
Properly configure and implement firewalls, routers, VPNs, and Intrusion Detection and Prevention systems (IDS/IPS).

23. Patch management plan
A regular component of the security routine should involve planning, testing, implementing, and auditing patches through automated patch management software.

24. Monitor and track behavior in cloud apps
Detect abnormal user behavior like impossible travel, unfamiliar sign-in properties, or suspicious inbox manipulation rules within cloud-based apps such as Microsoft 365 and Azure AD to prevent attacks like business email compromise and ransomware. Vulnerability Management and Assessment

25. Define a vulnerability analysis and resolution strategy
Identifying vulnerabilities and determining the viability is a crucial component to understanding your organization's overall risk. Your organization needs to develop a plan to track vulnerabilities, assign severity, and address them accordingly.

26. Vulnerability management program
At the core of any vulnerability management program lies the fundamental process of software management. Most vulnerabilities are software "bugs" that can be exploited and possibly compromise confidentiality, integrity, or availability. As such, the organization should take the time to understand all the software used within their environment. Vulnerabilities affect all devices that run software (sometimes referred to as firmware), not just desktops and laptops, it includes Internet of Things (IoT) devices, like HVAC controls, door readers, and other network connected devices.

RESPONSE

27. Incident response policy
Policies set the standard of behavior for activities; such examples include:

- Purpose and Objectives of the Policy
- Statement of Management Commitment
- Scope of the Policy
- Organizational Structure and Definition of Roles, Responsibilities, and Levels of Authority
- Severity Ratings of Incidents
- Performance Measures
- Reporting and Contact Forms

28. Incident response procedures
Procedures are the specific step-by-step instructions to execute individual processes as part of a plan specific to incident response. Incident Response is not the same as business continuity or disaster recovery.

29. Identify roles and responsibilities
Know the key stakeholders and critical roles within the organization who should be involved in a security incident. The responsible stakeholders and roles may change depending on the type of incident and the targeted resources of the organization.

Conduct simulated tests or tabletop exercises with key stakeholders and critical roles to ensure all required parties are accounted for.

VULNERABILITY MANAGEMENT AND ASSESSMENT

30. Business continuity and disaster recovery
Establish, review and test business continuity and disaster recovery plans. These plans should include each major functional area to keep your business operating. This goes beyond IT and includes Finance, Human Resources, Operations and other functions essential to your business. Test plans at least annually.

31. Incorporate Lessons Learned
Whether it is a real incident or a simulated walkthrough, we identify weak areas in our plans. It is critical to take lessons learned through experience and incorporate them into your plans going forward.