Micro Technology Solutions, Inc.
The Computer Systems People ™

Cyber Security Primer for SMB Leaders

Cyber Security is critical for any business, but the technology is complex and fastmoving. Since understanding your security posture is so important and so difficult for business leaders, we created this bookmarkable guide for you to refer back to.

Why do you need Cyber Security? A data breach or ransomware event can expose your organization to losses including Business Interruption, Regulatory Fines, Civil Liability and more. Significant data loss could even cause a business to fail.

Key considerations when developing your cyber security strategy:

- Types of data collected (and stored)
- Industry regulations
- Local regulations
- Cost of business interruption
- Value of Intellectual property
- Business reliance on technology

Cyber Technology Terms you'll see:

- Vulnerability Scan
- Cyber Insurance
- MFA
- Firewall
- Patch Management
- Anti-Virus
- EDR
- MDR
- DNS Security
- Security Awareness Training
- Backup / Disaster Recovery
- Pen Testing
- Incident Response Plan
- NIST Framework

Micro Technology Solutions, Inc.
The Computer Systems People ™

Let's take them one at a time…

Vulnerability Scan

What is it? This is an automated process using a tool to scan your devices for known vulnerabilities (often from inside your network).

Who needs one? Everyone should do this periodically. It quickly identifies gaps in your cyber preparedness. A vulnerability scan should be followed by a remediation effort to fix the issues found during the scan! It is important to look for systemic issues to prevent future vulnerabilities from cropping up.

How expensive is it? Cost varies with the number of locations and devices, but a typical vulnerability scan is not expensive for a small business. If you have not done (or not recently done) a vulnerability scan, this is a high value, low-cost tool to help prevent cyberattacks.

How difficult is it to deploy? Very simple. Your provider will need some basic questions answered and access to your network.

Cyber Insurance

What is it? Cyber insurance covers the costs associated with a cyber breach including business interruption, regulatory fines, civil liability, legal fees, remediation costs, etc.

Who needs it? Businesses with significant exposure above, should consider cyber insurance. Carriers who specialize in cyber liability will have resources to help in the event of a breach. Riders are available but typically don't offer much coverage and the carrier may offer little help if you are breached.

How expensive is it? Cost varies. It is important to consider coverage for the realistic costs of a breach including public relations and emergency remediation to restore normal operation of your computer network.

How difficult is it to deploy? The key difficulty with cyber insurance is making sure to answer questions on the application accurately. Incorrect answers can change your pricing and potentially invalidate your insurance if you have a claim.

Multi-factor Authentication (MFA)

What is it? MFA is an added layer of security after logon to ensure a user is who they claim to be. This prevents hackers from gaining access to your network with stolen login credentials. The second factor of authentication could be something they are (biometric), something they have (iPhone or token), or something they know (answer).

Who needs it? Most cyber insurance carriers require MFA because it adds a significant layer of protection. MFA is highly recommended because it is effective.

How expensive is it? Some M365 licenses include MFA. Otherwise, a per user subscription for a product like Cisco DUO will be needed.

How difficult is it to deploy? MFA is fairly easy to deploy for qualified technology firms.

Firewall

What is it? A device that inspects traffic coming from one network to another, usually located at the edge of a network where it connects to a data carrier. (Verizon, Comcast, etc.) A firewall acts like curtains in your home, blocking visibility to things you want to keep private inside your network.

Who needs it? EVERY BUSINESS.

How expensive is it? Firewalls can be as inexpensive as $500 depending upon the speed of connection they interface with. It is critical to have a qualified engineer set up your firewall so it works effectively. A poorly configured firewall can be as insecure as having no firewall. Also, some firewalls require a subscription. Make sure to manage your subscription renewal so your protection keeps working.

How difficult is it to deploy? Difficult. Depending upon the complexity of your network and your security needs firewall configuration can be very complex. Hiring a professional is highly recommended.

Patch Management

What is it? A process using automated tools to review and apply fixes software vendors make to their products. Most of these are for security purposes.

Who needs it? EVERY BUSINESS. This is a critical task that is neglected in many firms. This is one of the least expensive and most important cyber security protections you can employ.

How expensive is it? Not very. A good MSP can perform patch management very inexpensively.

How difficult is it to deploy? Easy (with the proper tools).

Anti-Virus

What is it? A tool that scans files for known viruses.

Who needs it? We do not recommend anti-virus because it is obsolete. (See EDR). Threat actors can circumvent anti-virus products.

How expensive is it? Inexpensive relative to EDR.

How difficult is it to deploy? Easy.

Endpoint Detection and Response (EDR)

What is it? EDR replaces Anti-virus. It scans files, but also monitors the behavior of active processes on a device. EDR can see an attack occurring and stop a process and even remove the device from the network to protect other devices. EDR is a significant upgrade from anti-virus and will detect many threats that anti-virus does not.

Who needs it? Everyone.

How expensive is it? About double the price of Anti-virus.

How difficult is it to deploy? EDR is fairly simple to deploy, but it is critical to have a knowledgeable team in place to monitor alerts and respond to them.

Managed Detection and Response (MDR)

What is it? MDR is designed to detect a ransomware attack before the attack is triggered. It hunts for persistence mechanisms (back doors) in your environment and signs your data is being altered by a threat actor.

Who needs it? Firms concerned about Ransomware

How expensive is it? Similar to EDR.

How difficult is it to deploy? Moderately difficult. It is critical to have trained engineers installing and monitoring MDR for alerts.

DNS Security

What is it? DNS is how your computer finds files and web sites on the Internet. DNS security systems broker requests coming from your users and are able to block them from reaching malicious sites.

Who needs it? DNS Security is highly recommended because it can protect your team from emerging attacks.

How expensive is it? DNS Security is priced per client and is less expensive that EDR or MDR.

How difficult is it to deploy? Easy. Like EDR and MDR, it is important to have a team ready to assist when sites are blocked. Users may complain about not reaching a site that is being blocked because it has been compromised. Allowing users to visit such sites gives threat actors an opportunity to attack.

Security Awareness Training

What is it? Training to help users identify Phishing attacks and other security threats. It works by employing a combination of training and simulated attacks to improve overall security.

Who needs it? Firms concerned about cyber security. Security Awareness Training is especially helpful for unsophisticated user groups. Firms handling credit card data can benefit from training on the handling of Personally Identifiable Information.

How expensive is it? Very inexpensive. Usually an annual subscription.

How difficult is it to deploy? Easy. Phishing attacks are delivered via email. Some firms like KnowBe4 have a customer success team that is extremely helpful setting up training and monitoring progress.

Backup / Disaster Recovery

What is it? System to store system configuration and data. In the event of a disaster or an attack this system should allow restoration of data and the ability to replicate any servers affected, ideally in an off-site location if necessary.

Who needs it? Everyone. Everyone needs to test their DR solution!

How expensive is it? Varies with the amount of data the customer is willing to lose in an emergency and the amount of time they are willing to wait to restore operation after a failure.

How difficult is it to deploy? Varies with goals for data restoration and tolerance for data loss. Most small businesses fall short on testing the backup and developing an adequate plan for emergency situations.

Penetration Testing (Pen Testing)

What is it? Penetration testers target a network and attempt to gain access. Some may even test physical security by trying to get inside your buildings. This is a more in-depth test than a vulnerability scan and is driven by experienced professionals.

Who needs it? Firms very concerned about security.

How expensive is it? Pen Testing is significantly more expensive than a vulnerability scan. Cost varies with the expertise of the firm.

How difficult is it to deploy? Easy. The process is driven by the selected vendor. Results depend on the skillset of the vendor and the amount of time they are engaged for.

Incident Response Plan

What is it? A plan that documents everything needed and actions to be taken in event of a disaster or ransomware attack. Key data like contacts is imperative if automated systems are not available.

Who needs it? Firms concerned about cybersecurity. An incident response plan is immensely valuable in an emergency and table top exercises are recommended to walk through the plan periodically.

How expensive is it? Complexity of plans vary. Cost will vary based on the expertise of individuals developing the plan.

How difficult is it to deploy? Plans can be very difficult to implement based on the complexity of the environment. It is key to test these plans with tabletop exercises as technology in the environment will change and so, the plan also needs to be updated. Plans obviously should be on paper and include contact information for everyone likely to be involved in recovery.

NIST Framework

What is it? This is not a tool used in cybersecurity, but a framework developed by the National Institute of Standards and Technology. It outlines best practices to help organizations manage cybersecurity risk.

Who needs it? Business leaders need only be aware of what it is. The vast majority of providers follow the NIST framework.

How expensive is it? Free.

Our team at MTSi deploys and manages these technologies on a daily basis. If you'd like to know more about anything discussed here, reach out to our sales team.

If you are concerned your firm is lagging in cybersecurity, a quick conversation is a great place to start. We can help you understand your cyber security posture and if needed, perform a vulnerability scan or an audit to help determine where your defenses could use fortification.

Micro Technology Solutions, Inc.
132 Alden Rd.
Fairhaven, MA 02719
Sales@mtsolutions.net
(508) 324-9475 Option 1