MATURITY LEVEL 1

20 WAYS TO PROTECT YOUR BUSINESS FROM A CYBER ATTACK!

Security Assessment

Take the first step on your security journey: establish your security baseline and identify existing vulnerabilities. When was your last assessment?

Date: _____

Unified Network Monitoring & Alerting

Respond to security threats and alerts with 24x7 network monitoring to quickly detect and fight against cyber-attacks or data breaches.

Advanced Endpoint Detection & Response

Protect your data from malware with advanced endpoint security. This modern technology replaces your outdated anti-virus solution and protects against complex threats- it can even rollback a ransomware attack!

SIEM/Log Management

(Security Incident and Event Management)
Log, monitor and analyze your network security to protect your data and meet cybersecurity compliance requirements. SIEM enables you to detect files entering and leaving your network, administrator password changes, and log potential security risks using big data engines.

Web Filtering

Worried about Internet safety and productivity? Web Filtering allows you to customize what website content your users can (and cannot) access to support your Information Security policies and reduce the risk of web-based threats.

SPAM Filtering

Secure your email! Most cyber-attacks originate in your inbox. Choose a service designed to reduce your company's exposure to harmful e-mail messages.

Password and Security Policies

Apply security policies on your network that protects critical data. You should enable enhanced password policies, set user screen timeouts, limit USB file storage access, and have user access permissions in place.

Security Awareness

Train your users on security threats – often! By teaching your employees about data security, email threats and your security policies, you reduce the "human factor" threats. We offer a web-based training platform for your employees, simulated phishing attempts, and "best practice" Security Policy consultation.

Multi-factor Authentication

Use multi-factor whenever you can, including on your local network, banking and financial website, and even social media to confirm your identity more than once. This adds an additional layer of protection in case your password is stolen.

Physical Security Cameras

Using security cameras to control and monitor building locations where your server and networking assets are located, as well as sensitive documents, will protect your data and reduce the risk of a physical data breach.

DID YOU KNOW?

1 IN 5 Small businesses will suffer a cyber breach this year.

81% Of all breaches happen to small & medium sized businesses.

97% Of breaches could have been prevented with today's technology.

Physical Access Control

Building access control restricts employee access to critical network infrastructure, data storage and confidential documents, and keeps track of "who went where?" to further protect your data. If you lock your car at night, shouldn't your company's data have the same protection?

Computer Updates and Patches

Automate your computer and system updates with the latest patches for better security. Using a monitored, automated "critical update" service keeps software and Operating Systems secure and protected from malicious attacks.

Dark Web Monitoring

Knowing in real-time if your passwords have been posted on the Dark Web lets you act fast to prevent a data breach. Use a reputable Dark Web scan to protect your business from stolen credentials that could get posted for sale.

Web Gateway Security

Internet Security is a race against time. Cloud-based security detects web and email threats as they emerge on the Internet and block them on your network within seconds – before they reach your users.

Mobile Device Security

Protect your data from cyber criminals by limiting mobile access to your network, requiring passcodes and screen locks, and controlling access to company data stored on mobile devices in case an employee's phone is lost or stolen.

Advanced Firewall Protection

Turn on your Intrusion Detection and Intrusion Prevention features first, and then send the log files to a managed SIEM. And if your IT team doesn't know what these things are, call us today!

Encryption

Encrypt data when sending and transporting files to avoid potential data breaches. Using encryption technology when storing files (on your servers or back-ups) or sending files (like sending email, or USB file sharing) prevents unauthorized access to your sensitive data.

Data Back-Ups

Back-up locally. Back-up to the Cloud -even if you're "in the Cloud"! Have an offline back-up for each month of the year. Test your back-ups often, and make sure you have a working disaster recovery plan in the event of a failure or data loss. If you aren't convinced your back-ups are working, call us ASAP.

Third Party IT Management

Companies with or without onsite IT departments are required to use a 3rd Party IT Provider for security compliance. Partner with a reputable Managed Service Security Provider who understands security risks and objectively audit your security practices.

Cyber Insurance

If all else fails, protect your income and business with cyber damage and recovery insurance policies.

ONE2ONE
ONE2ONEINC.COM ▪ 717.393.7403 ▪ 617 SOUTH WATER ST. LANCASTER, PA 17603