Checklist:

9 Defenses Against Ransomware

Strengthen defenses before your company becomes the next victim.

PEGASUS TECHNOLOGIES

Ransomware is a Serious Threat to Your Small Business

The ever-quickening cadence and expanding sophistication of ransomware attacks continues to wreak havoc with US businesses.

Many large companies have responded by overhauling their cybersecurity systems, leaving small-to-medium sized businesses as the low-hanging fruit.

It's time to step up your defenses—before your company becomes the latest victim.

Use this checklist to evaluate your defenses.

☐ Replace legacy antivirus software with next-generation Endpoint Detection and Response (EDR) solutions.

Legacy antivirus is a top vulnerability for many businesses. While it still protects against older types of computer viruses, it doesn't protect against modern and more significant threats like Ransomware.

EDR uses automated, AI-powered techniques to stop ransomware

Endpoint Detection and Response (EDR) looks for unusual patterns in computer behavior to isolate threats.

EDR can…

- Stop Trojans, worms, and other malicious computer software programs with traditional virus definitions
- Use robust static and behavioral Artificial Intelligence (AI) to reduce the risk of infection from fileless attacks, in-memory attacks, unknown threats, and modern attack vectors that leverage tools already in the environment.

	Legacy Antivirus	Managed Antivirus	Endpoint Detection and Response (EDR)
Definition-based threat detection	X	X	X
Automated threat removal attempt	X	X	X
Automated reporting		X	X
Automated alerting on failure to scan, update, and remove threats		X	X
Built-in escalation to manually remediate problems with scans, updates, and threat removal		X	X
Detection of fileless attacks, in-memory attacks, and unknown threats			X
Detection of attacks that leverage tools already in the environment			X
Now required to maintain most cyberliability insurance polices			X

☐ Be as restrictive as possible with computer and data access.

Once a hacker is in your system they will automatically seek to infect as much of your data and as many of your devices as possible. By being strategic about who has what access to your system, you significantly limit the damage one infected account or device can do.

Best Practices to Contain the Spread

- If a person does not need to access a folder, file, or computer—don't give them access.
- Limit equipment access for office visitors. Have a separate visitor WIFI.
- Service accounts (e.g. "scanner") should not be permitted access to entire drives or interactive login sessions.

☐ Don't Neglect Security Patches and Software Updates

New weaknesses in software are found daily, and companies fix these holes via patches. Old, unsupported products are no longer patched, but still have newly-found vulnerabilities.

Secure all your internet-enabled equipment, including computers, routers, switches, etc. by regularly updating with the latest software updates and patches.

☐ Activate **multifactor authentication** (aka MFA or two-factor authentication).

Even the strongest passwords are subject to compromise. MFA systems can prevent unauthorized access and block many attack vectors by requiring users to confirm their identity to gain access. If available, choose App-based authentication over SMS-based, as it's typically more secure.

☐ Add 24/7 Security Monitoring to your layered security system.

Hackers are smart—they know the best time to strike is when your defenses are down. And they can do a lot of damage while you're sleeping or enjoying your weekend.

Employing a security monitoring service means cybersecurity experts are personally monitoring potential threats all day and all night, so you can focus on your business and enjoy your free time.

☐ Off-line **and ransomware-resistant backups are critical.**

Modern attackers intentionally infect and destroy data from online backups first, which is why you need a backup system that's not accessible via USB port, your network, or the Internet (aka an 'air-gapped' backup).

Create a disaster recovery plan:

It's essential to have a plan in case your online backups are threatened:

- **Secure your data offline**. *Remember if it's an always-on backup—it's at risk.*
- **how you will efficiently restore your data** from offline backups to minimize downtime.
- **Test your backups regularly** to ensure they're functioning properly.

☐ Train employees on cybersecurity best practices.

Perhaps the biggest threat to your cybersecurity comes from inside your own ranks.

Regular cybersecurity awareness training is necessary to train and update staff on the latest security issues and reinforce good practices like using good passwords and avoiding clicking suspicious email links.

☐ Sync HR & IT Departments

Your HR and IT departments need to make a coordinated effort to ensure that the network is only accessible by authorized people and devices.

HR and IT Must Coordinate to Monitor "Hidden Threats"

- **Bring Your Own Technology** - ensure employee and contractor devices are properly equipped to protect against threats
- **Malicious Insiders -** monitor insiders like disgruntled employees, vendors, or contractors
- **Terminated Staff** - coordinate to immediately disable terminated staff accounts and ensure they are not forwarding information outside
- **Training** - enforce cybersecurity education so that it's required to gain and maintain access to resources

☐ Obtain Cyber Liability Insurance

Cyber liability insurance is an insurance policy that provides businesses with a combination of coverage options to help protect the company from data breaches and other cybersecurity issues.

You might have Cyber Liability Insurance—but is it the right coverage?

There are a range of policies that cover a variety of cybersecurity issues and situations. Make sure you understand what type of coverage you need and what the policy will pay for:

- Loss of income / business interruption
- Prior acts (Breaches before coverage started but exploited after coverage began)
- Labor to remediate problem and restore operations
- Ransom
- Damaged reputation/brand
- Legal response and defense
- Notification of affected people and parties
- Punitive / compensatory damages for affected people

Are you meeting your Cyber Liability requirements?

To ensure coverage, you must comply with all the requirements of the policy, answer the application questionnaire accurately, and keep the questionnaire up-to-date as your IT practices change.

Many businesses fail to meet the requirements of their policy and are found ineligible for coverage in the event of a cybersecurity issue.

Take Action to Protect Your Data—and Your Business

As ransomware attacks become increasingly prevalent for small businesses, leaders need to take steps to secure data from outside threats—before it's too late.

Upgrade Your Cybersecurity Defenses

Book a Security Consultation

PEGASUS TECHNOLOGIES