RANSOMWARE BEST PRACTICES
Checklist

□ **COMPLETE REGULAR IMMUTABLE BACKUPS**
All your data is backed up locally AND in the cloud. The backups are immutable, and cannot be deleted. Data is being backed up at least daily and better yet every two hours. The cloud storage is encrypted, secure, and cannot be deleted. The entire system is tested every month to make sure it is secure and working properly.

□ **EDUCATE YOUR ENTIRE TEAM ABOUT SECURITY**
I discuss best practices and examples of ransomware hacks that have been in the news. The more people know the more security-aware they are. You can start conducting security awareness training via a 3rd party that will “test phish” your team and provide cybersecurity education videos/testing.

□ **USE MULTI-FACTOR AUTHENTIFICATION (MFA)**
Phishing attacks are on the rise, make sure to enable MFA on all critical applications and software.

□ **INSTALL ANTI-VIRUS AND ANTIMALWARE**
Use something better than generic free anti-virus and make sure it’s running optimally, up to date, AND you’re actually using and learning from its reports.

□ **FILTER OUT AS MANY THREATS AS POSSIBLE**
Spam, spyware, malware, viruses, and phishing emails – Use an Email Security and Threat Prevention platform (Research one that’s a good fit for your organization) so most of the bad items never even make it to your email.

□ **PRACTICE GOOD IT HYGIENE**

- Ensure that your local machines DO NOT have administrator rights (so no rogue apps can be installed)
- Check that user access to servers is regulated/limited/reviewed
- Install updates at least weekly and critical security ones immediately
- Educate users regularly
- Review and test backups regularly
- Please make an accountable and proactive person is managing everything and NOT just handed to someone who does not want it and ignores it.

□ **HAVE A MANAGED DETECTION AND RESPONSE (MDR) RUNNING**
MDRs more fully protect your systems. Think of it as your personal AI that is monitoring your computer activity. If it finds something of concern, it will automatically block the activity. Even if you click on something you shouldn’t, this should prevent anything bad from happening.

□ **PREPARE AN INCIDENT RESPONSE PLAN BEFORE AN ATTACK**
This is a straightforward plan that helps you navigate through the landmine items if you have a cybersecurity fiasco. The internet has many examples to start building a working plan.

Are you sure your business is safe?

If not, contact us and we can help.

630.547.7000 | digdeeper@waident.com | waident.com