ABACUSNEXT®

ONE REALLY GOOD IDEA EVERY DAY
attorneyatwork@

Ransomware Checklist

Ten ways to protect your firm from the threat of ransomware.

With cyber criminals growing ever-more sophisticated, firms find themselves wondering how they can proactively prevent and, if needed, respond to a ransomware attack. Ransomware is a type of malicious software (malware) programmed to encrypt data and block access to a computer system until money is paid. And the effects it can have on a firm—including lost data, lost revenue, and lost trust—can be devastating. Be sure you've taken the following steps to keep your firm safe from the threat of ransomware:

1. Conduct Security Awareness Training

Of all the ways firms can protect themselves from ransomware, staff education and application of consistent security protocols are the most effective. Schedule regular security trainings and educational emails reminding employees how to spot spear-phishing attempts, email scams, and other cyberthreats. And be sure to have a written, frequently tested incident response plan in place.

2. Follow a "zero trust" model

Of course, you trust your employees, but why open your firm up to unnecessary security risks by giving everyone access to sensitive information? Start by giving employees minimum authorized access, then expand out as needed based on individual roles.

3. Use strong passwords

It seems simple, but a strong password goes a long way in keeping your accounts safe. Choose the longest most complex password permissible on a website or application, with at least 11 or more characters with random strings instead of common words.

4. Use a password manager

Password managers like LastPass and Keeper make it easy to store your login information, allowing for more complex passwords that require less typing each time you log in.

5. Enable multi-factor authentication (MFA)

Multi-factor authentication helps ensure that the only person who has access to your account is you. It requires two or three types of credentials to authenticate your identity and can easily be tied to your smartphone or watch with biometric authentication.

6. Deploy Endpoint antimalware

This new paradigm enhances protection against known malware by applying patches and updates from a central server. That design ensures consistency in protection and reduces the likelihood that any device would be unpatched or behind in its updates.

7. Virtualize your workstations and server

Cloud-hosted virtual workspaces and servers allow you to access remote instances of each computer in your network. Also, you'll be able to access all programs, tools, client information, and business-critical documents remotely, just as they existed before you lost access to your physical desktops. A virtual instance means you can quickly respond to a ransomware infection on one device or in one location by using an uninfected device to reconnect.

8. Create multiple, incremental, and verified backups

Being able to restore your backup means that the "last good state" of your environment is never far away. This gives you protection against ransomware, particularly when the next attack is often a never-seen malware variant. Multiple instances of your backup means you remove a single point of failure, incremental backups give you an efficient method of storing all data without needing to create multiple copies of the same files, and verification means your backups are tested and ready whether you need to restore a file or the entire database.

9. Conduct regular cybersecurity audits

Your firm should perform regular audits of your technology, hosting service, and employee awareness levels. By doing so, you can identify weak spots, remove single points of failure, and find opportunities to re-educate employees on security best practices.

10. Create incident response plan

Here's the good news: 96% of companies with a backup and disaster recovery plan survive a ransomware attack. It is important to create an action plan outlining the steps your firm would take in the event of an attack, including how you will identity and assess the threat, contain it, remove it, restore your network, and communicate to employees and clients.