SECURE YOUR FIRM’S DATA: Best Practices for Data Backup and Verification
More and more, there are new reports of the destruction that cyber criminals have caused with a data breach or ransomware attack on a different company, hospital, or school. Recovering from these attacks can be expensive for the company whose data was leaked, and their reputation can be compromised. In 2021, it is not a matter of “if” your company will see a data breach or ransomware attack, it is a matter of “when.” That means it is time for your business to fortify your company with precautions, safety nets, and contingency plans for recovery. Where can you start today?

**End-User Education**

The leading cause of ransomware attacks, according to Datto’s State of Ransomware Report for 2021, is phishing email attempts, followed by poor user practices and their own gullibility. Your Firm’s security training should extend beyond education about phishing emails to improving your employees’ habits, such as, password strength, RDP access, and other vulnerabilities at the user level.

**TIP:** Conduct regular mock phishing attacks to teach your employees best practices in case of actual attempts. After educating your employees on the proper response to a phishing email, unannounced fake attacks can help your Firm remain sharp on best practices.
Secure Your Firm’s Data: Best Practices for Data Backup and Verification

Cyber Security

Common ransomware prevention tools can help protect your Firm from an attack. Things like antivirus platforms, email filtering, pop-up blockers, and endpoint detection systems can significantly help protect from basic attacks. However, ransomware and cyber criminals can evade these measures with more and more ease, so it should not be considered a comprehensive solution. Criminals have adapted and now produce very sophisticated dupes that can trick even the most trained user, so a multi-layered approach is best for your Firm’s security.

TIP: Establish and document a thorough cyber resiliency plan. It should document what to do before, during, and after an attack, including all steps and points of contact. This plan should be reviewed and updated regularly.

Business Continuity

Breaches can often result in considerable downtime and negative attention, since ransomware attacks are rarely limited to a single computer. The virus crawls for larger areas to compromise, such as servers and SaaS applications. Without a recovery and business continuity plan, nearly 20% of MSPs reported resolving to paying the ransom just to be able to return to business. Instead, your Firm’s business continuity plan should include preparations such as:

- Hybrid cloud-based backup
- Automated backup processes
- Image-based backup processes
- Virtualization capabilities

TIP: Invite an IT Managed Service (ITMS) provider to audit your security system. Many ransomware attacks succeed because of unpatched systems, incorrect set-up in cloud systems like Microsoft 365, and a lack of user education. An ITMS provider can identify these weaknesses and develop a cost-efficient, scalable solution to holistically audit your security posture.

Have concerns or questions about your cybersecurity practices or your Firm’s system?

Contact Frontline Managed Services for an audit and a discussion.