Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

# A Strategy to Get Started with a Cybersecurity Program: Are you prepared with a Data backup?

***Published October 9, 2020 - In the spirit of October being Cybersecurity awareness month, Dopkins & Company is launching a monthly blog on IT Security topics. October should be spooky; your IT Security should not be. These blogs will introduce various topics, related terms, importance of reviewing the topic and hopefully raise some questions you should be asking. We hope to use Cybersecurity awareness month as a catalyst for year-long and continuous awareness.***

This month we will be discussing data backups. Backups are a copy of data stored in a different location than the source data. They allow for the data to be restored in case it is permanently lost. Data can be lost in many ways, including user error, fire, hardware failure, data corruption, or malware.

Data loss due to hardware failure can occur when a drive fails, or even begins to fail. Typically, the only chance at recovering this data is through a forensic recovery service. These services can be costly and will take a considerable amount of time. Even then recovery is not guaranteed. This is not the situation that you want your most important data to be in. One configuration that is vital to have configured correctly on critical systems is RAID (Redundant Array of Independent Disks). Disk mirroring is a form of RAID. RAID can be configured many ways depending on the size of the data and the performance required from the drives. RAID allows for drive failure, and replacement, without data loss. However, RAID is **not** a backup. Multiple drive failures can still result in data loss where a backup will be needed. If RAID is the only configuration in your environment you will still need to configure a data backup.

It is also possible for data to become corrupted. Sometimes data corruption is an early sign of hardware failure. Mechanical failures can cause parts of a drive to become unreadable. It is also possible for software to cause corruption. Corruption can occur if a program does not install correctly. Any disruption in software installation has the potential to cause that program to function incorrectly or even to make unintentional changes to system files and settings. This is especially true with updates, including firmware and regular Windows Updates. Powering off a computer while updates are being applied can leave the system in a state of change where it will not operate correctly or sometimes it will not even boot. When data corruption occurs, there is frequently not much that can be done to fix the corruption. Some websites offer software that can be purchased; but, just like with recovering data after a hardware failure, there is no guarantee that it will be successful.

Another cause of data loss is malware. Malware can come in many forms and effect data in various ways. An increasingly common form of malware is ransomware. Ransomware encrypts data to render it unusable. Data will not be recoverable due to the complexity of the encryption. The attacker has the key that would allow the data to be decrypted and requires payment before providing the key. Even after payment there is no guarantee that they provide the correct key and that it works.

No matter which way data is lost the common answer is having a reliable backup. In every scenario it is less expensive in both time loss and actual cost to have an effective and recent backup ready to restore. The key to determining whether you have effective backups is to ask yourself several questions: What

damage am I trying to protect against? How much data am I willing to lose (need to reconstruct) if something goes wrong? What systems need backing up? Can my backup be effectively and efficiently restored (have you tried)? For example, if you want to restore your systems after a fire, the backup should not be stored where it would be affected by the fire (off-site). If you want to restore a file that someone mistakenly erased, you should be able to access the backup file quickly.

You could have several different backups of different data with different processes and timeframes, based on the risk that you are trying to protect. For example, a backup of accounting records for compliance purposes may need to be done monthly and kept for years and not be over-written; but a database backup is done hourly and overwrites the previous one.

**The answer to the question "Do you have a backup" may not be so simple. We'd love to help you evaluate your backup needs and implement an effective backup process. If you would like to have a conversation and review your backups check out our STARTegy page for more information about our Strategy for Getting Started with Information Security.**

**Dopkins was recently featured in the *Business First of Buffalo cybersecurity executive forum*. Bill Prohn, Dopkins Systems Consultants Managing Director, participated in a panel discussion covering a broad spectrum of IT security issues, including data backups. Watch the full program here.**

## For more information, contact Patrick M. Rost at prost@dopkins.com.