Office of Risk Management
RISK ALERT
No. 2017-07

RE: Ransomware Attacks **March 22, 2017**

It has come to our attention that another parish in our archdiocese has been the victim of a ransomware attack. All of the parish's files were encrypted and the hacker has demanded a ransom in order to restore the files. This is becoming a more common form of attack, and it is PREVENTABLE. Please review protocols with your IT personnel or contractors and take immediate steps to prevent this from happening to your network.

What is Ransomware?

There are different types of ransomware. However, all of them will prevent you from using your PC normally, and they will all ask you to do something before you can use your PC. They can target any PC users, whether it's a home computer, endpoints in an enterprise network, or servers used by a government agency or healthcare provider.

Ransomware can:

- Prevent you from accessing Windows
- Encrypt files so you can't use them
- Stop certain apps from running (like your web browser)

Ransomware will demand that you pay money (a "ransom") to get access to your PC or files. We have also seen them make you complete surveys. There is no guarantee that paying the fine or doing what the ransomware tells you will give access to your PC or files again.

How to Prevent Ransomware

- **BACKUP YOUR FILES.** The best advice for prevention is to ensure that confidential, sensitive, or important files are **securely backed up. Backups should be set up in such a way that they are separate from your computer. This is critical.** Back up all of your computers and mobile devices on a daily basis to both external hard drives AND cloud-based backup services. Then, if your files are locked up by ransomware, you can restore files from the backups. Caution: some ransomware encrypts backup drives. It's best to disconnect or switch off backup drives after each backup.
- **UPDATE YOUR SOFTWARE AND OPERATING SYSTEMS**. Keep your operating system and other software fully updated and patched. In Windows, go to Windows Update in the Control Panel, or Update & Security in the Settings menu, and make sure that updates are set to install automatically. On a Mac, go to Settings, then App Store, and make sure "Automatically check for updates" and "Install system data files and security updates" are checked.

- **INSTALL ANTI-VIRUS SOFTWARE.** Make sure your systems are running robust, self-updating antivirus software. Firewalls don't always protect against infiltration, and they cannot stop you from opening email attachments.
- **REMEMBER:** Most forms of ransomware are recognized and blocked by antivirus programs, and most exploit software vulnerabilities for which fixes have long existed. People who don't patch their systems and don't run antivirus software get infected first.
- **CLEAN HOUSE!** A cyber security audit recently conducted by the Office of Risk Management discovered that multiple locations are still utilizing Operating Systems that are "end of life," such as Windows XP, Server 2003 and Server 2000. **These unsupported operating systems represent significant risk as Microsoft is no longer developing and providing security patches and updates for them. It is important that you disable or update outdated computers and servers ASAP.**

If You Think You Have Been Infected

- Disconnect the infected computer from the network, but do not turn it off.
- Immediately look for newly-created login accounts on your system
- Alert law enforcement and the Office of Risk Management (617-746-5740)
- Hopefully, you will have an external backup of your files and will be able to restore the files via the backup.

PLEASE REMEMBER: As noted, your very best defense against ransomware is a recent backup from which you can recover lost or encrypted files. Confirm your backups are in place and appropriately configured to run on an automated and scheduled basis. Test a full recovery at least once or twice a year to make sure the file restore process works as expected.