Ransomware and the Increase of Cybersecurity Threats

by Patrick T. Copeland, CPA, Audit Manager

Posted on November 15, 2021

Over the past year, you may have heard about high profile cyber-attacks around the country. The year 2020 set many records on the number of cyber-attacks and with all likelihood, it does not appear to be slowing down in 2021. I am not a cybersecurity expert, however, it is always best to be prepared rather than having to react to a cyber-attack. In that vein, being aware of potential weak spots in your organization is essential to ensuring your business is up and running at all times. In addition, a direct effect of cyber-attacks is the high cost to an organization (i.e. the lost time of employees and the costs to restore business back to normal).

As ransomware is one of the fastest growing cybersecurity threats, I would like to focus on the specifics of this threat on an organization. What is ransomware you might ask? Ransomware is a malware (i.e. malicious software) that infects computers (and mobile devices) and restricts access to files, often threatening permanent data destruction unless the ransom is paid. How does a cybercriminal infect your organizations files? This is done in a number of different ways; however, a common way would be an individual in your organization clicks on a malicious link which downloads a file from an external website. The individual then clicks on the downloaded file not knowing it is ransomware. The malicious software will then start to propagate throughout the organization and subsequently encrypts the files.

This topic is a little dreary, but I would like to point out some best practices that might help your organization prevent a cyber-attack or accelerate your recovery if an attack occurs.

The National Institute of Standards and Technology (NIST) has a few recommendations to help prevent cybersecurity issues. They recommend that organizations use antivirus/antimalware software at all times and ensure that it automatically scans emails and removable media (i.e. flash drives) for malware. In addition, an organization keeps all computers patched with all the latest security updates. Finally, operating systems be configured to allow only authorized applications to run on computers and using security products to block access to known ransomware sites on the internet.

The NIST also has recommendations on how best to accelerate recovery from a cyber-attack. The first thing to do is to develop and implement a disaster recovery plan. This includes having defined roles and running through scenarios for what it would look like to resume operations. Another important aspect is to test the backup and restoration strategies to ensure that the malware cannot spread to the backed up files. Finally, they recommend that an organization maintains an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement.

NIST is just one organization with helpful information on cybersecurity protection and response. Another is the Cybersecurity & Infrastructure Security Agency (CISA) whose website also provides many good resources that might be beneficial to your organization.

If your organization has taken all of these steps, it will be necessary to ensure that the prevention process is reviewed and discussed on a regular basis to ensure it is up to date. As the world has moved to an even greater reliance on digital information, it's critical that your organization has taken the time to help prevent as best as possible a cyber-attack. I hope your organization never has to deal with one of these stressful situations. However, if you do, your organization should be resilient and able to resume operations as quickly as possible.