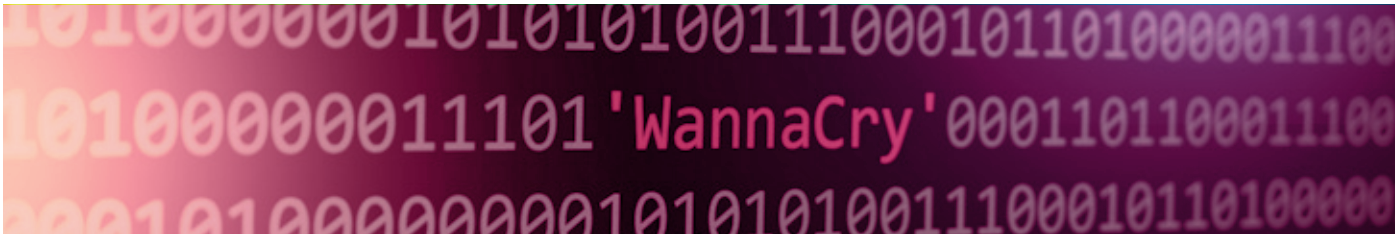
'Wanna Cry'?

Tips for protecting your school district against ransomware



This spring, organizations around the world were attacked by a particularly virulent form of ransomware ("WannaCry") that exploited vulnerabilities in the Microsoft Window's operating systems. The attack impacted hundreds of thousands of organizations. It was a stark reminder that the threat of ransomware is real, important and growing.

What Is It?

Ransomware is a type of malicious software that infects a computer and then holds the data hostage by encrypting the files until victims pay to have them unlocked. It comes in two major types: cryptors and blockers.

- **Cryptors:** Encrypt valuable data on a computer or a computer network so that a user cannot access them.
- **Blockers:** Deny access to an infected computer device so the device is unusable.

Ransomware isn't new — criminals have long sought to extort payment from victims. What is new, however, is its dramatic increase in popularity. In 2016, Microsoft detected a 400 percent increase in the number of ransomware encounters. It is often spread in one of three ways:

- Through phishing emails that include malicious attachments.
- Through a user visiting a website from which malware is downloaded without the user's knowledge.
- Through social media applications.

The consequences to a victim company can be significant, including loss of access to data, disruption of normal business activities and loss of revenue, as well as the costs of restoring data/files, paying the ransom and damage to reputation.

What Can an Organization Do to Mitigate the Threat?

Evaluate Data Back-up Procedures. Recreating digital assets from an uninfected backup is often the quickest and most effective solution.

Provide Training to Employees. Train employees to detect phishing emails. Phishing emails which appear to be sent from a person or organization you trust, but they are really hackers trying to access your computer. Some signs of phishing emails are:

- Sender is asking for your network username or password;
- Email appears to be sent from your human resources or information technology department;
- Email has grammatical errors;
- Contains email addresses that do not match the header or body of the email; and
- Include links that show a different destination when you hover over them.

Purchase Cyber Insurance Coverage

Ensure your policy includes the following key coverages.

- **Cyber extortion:** Covers payments and fees to respond to and terminate a threat.
- **Digital asset restoration:** Covers costs to determine if assets have been altered and to restore, recreate or repair them.
- **Breach response services:** Covers costs to respond to a cyber-attack including a privacy attorney, data forensics investigator and public relations firm.

Unfortunately, not all "off-the-shelf" cyber policies have these key coverages and it is important to consult with an insurance professional. Arthur J. Gallagher & Co has an established team of insurance professionals with cyber insurance expertise to assist our clients in responding to this growing worldwide problem. ■

Nancy Moon PWCA is area vice president for Arthur J. Gallagher & Co, an endorsed agency through the WASB Insurance Plan. For more information, visit wasb.org.