Economic Stability and Cyber Security

Economic stability-whether in the utility industry or others industries-relies on a solid cyber security program. Cyber policies and protocols can help us maintain a sense of normalcy, safety and privacy in relation to the cyber world that we all interact with.

According to the National Institute of Standards and Technology (Department of Commerce), a cyber-attack is “an attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.”

In short, a cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general.

Cyber-attacks and threats have increased over recent years to where all agencies, organizations (and even individuals) should be planning for breaches and similar attacks in order to protect personal identifiable information (PII) and prevent interruption of business operations.

Seven common types of cyber security threats include the following:

- Malware
- Emotet
- Denial of Service
- Man in the Middle
- Phishing
- SQL Injection
- Password Attacks

Malware is a contraction for “malicious software.” Examples of common malware includes viruses, worms, trojan viruses, spyware, adware, and ransomware.

Emotet is a trojan virus that is primarily spread through spam emails (malspam).

Denial of Service (DoS) is a cyber-attack in which the bad actor seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network.

Man in the Middle is a form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.

Phishing is a type of social engineering attack often used to steal user data, including log-in credentials and credit card numbers.

SQL Injection is a type of cyber-attack in which a hacker uses a piece of Structured Query Language (SQL) code to manipulate a database and gain access to potentially valuable information.

Password attacks refer to any of the various methods used to maliciously authenticate into password-protected accounts.

Unlike some common threats to business operations like natural disasters, cyber security attacks are similar to terrorist attacks in that you do not see them coming or anticipate them. Cyber breaches can be brought on both intentionally by a bad actor or unintentionally by an end user not using strong passwords (or sharing passwords) or by an organization, as a whole, by not properly planning.

Some best practices are:

- Utilizing strong passwords
- Using Multi-function Authentication (MFA)
- Education. It's much easier to prevent a hack than it is to recover from a hack.
- Safe and Secure Wi-Fi
- Backup systems regularly
- Install Anti-Virus Software
- Secure Physical Devices
- Update Software and Firmware

It is never too early to begin planning for cyber threats. Start planning this spring for a strong cyber defense. Afterall, a strong defense is the best offense.

Submitted by:

Luke Mitchell, Risk and Insurance Analyst I, West Virginia Board of Risk & Insurance Management