Cybersection

Cybersecurity Spotlight – *Ransomware*

What is Ransomware?
Ransomware is a form of malware, which is software designed to damage or disable computers and computer systems. Ransomware targets your critical data and systems for the purpose of extortion.

Ransomware is frequently delivered through "spear phishing" emails, which are emails sent by criminal hackers that appear to be from an individual or business known to your or your employees.

Once enabled, the ransomware locks the legitimate user out of their data or system, and the criminal hacker demands a ransom payment. After paying the ransom, you will purportedly regain access to your system or data.

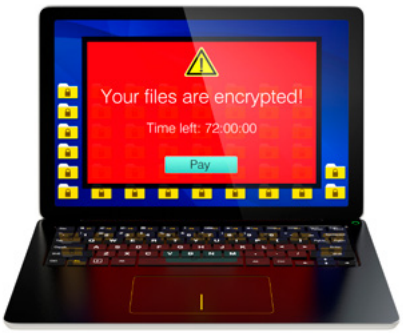
The Ransomware Threat
Ransomware is the fastest growing malware threat, targeting users of all types—from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300-percent increase since 2015.

However, businesses can take steps to prevent these attacks as well as plan responses to attacks that can significantly mitigate the risk posed to your business. The U.S. Department of Homeland Security's **Alert TA16-091A** (Ransomware and Recent Variants) provides important information on this threat. You can also:

- Educate your staff – constantly remind employees about the basics, such as "think before you click."
- Be proactive – put in place, and maintain, software, hardware, and training measures.
- Review business continuity plans – make sure they address cybersecurity contingencies.
- Review industry and regulatory cybersecurity best practices and guidance, which is available **here.**

Where to Report Ransomware Attacks?
- Federal Bureau of Investigation, **here**.
- Internet Crime Complaint Center, **here**
- United States Secret Service Electronic Crimes Task Force, **here** and Local Field Offices, **here**

Source: **"How to Protect Your Networks from Ransomware"**



Department Closes First CornerStone Bank

Source: Lance Knickerbocker, montco.today

On May 6, the Department of Banking and Securities closed the $103.3 million-asset First CornerStone Bank, King of Prussia. The FDIC entered into a purchase and assumption agreement with First-Citizens Bank & Trust Company, Raleigh, NC, to assume all of the deposits of First CornerStone Bank.

The cost to the Deposit Insurance Fund was estimated to be $10.8 million. This failure was the third bank failure of 2016 and the first bank failure in Pennsylvania since 2014.