Process Safety Beacon
Messages for Manufacturing Personnel
www.aiche.org/ccps/process-safety-beacon

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

This issue sponsored by
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Cyber Security and Chemical Operations

July 2021

Figure 1. Oldmar, Florida water treatment plant

On February 5, 2021, a water treatment plant employee in Oldsmar, Florida, noticed that the cursor was moving strangely on his computer screen, Initially, there was no concern; the plant used remote-access software to allow staff to share screens and troubleshoot IT issues. The supervisor often connected to his computer to monitor the facility's systems too. A few hours later, the operator noticed the cursor moving and clicking through the water treatment plant's controls. Within seconds, the intruder was attempting to change the system's sodium hydroxide setpoint from 100 parts per million (ppm) to 11,100 ppm. The operator quickly spotted the intrusion and returned the sodium hydroxide to normal levels. Fortunately, there was no impact on the water quality.

A recent ransomware attack on the Colonial Pipeline shut down the supply of gasoline to the US East Coast for several days.

Your company's systems are probably connected to the internet and need protection from cyber threats. There are many strategies used by companies to deter cyber threats such as: firewalls, anti-virus software and policies to protect against malware and computer viruses .

More people are working remotely; this has increased the opportunities for cyber attacks.

Did You Know?

- Cyber criminals use sophisticated malware to take advantage of multiple vulnerabilities and accomplish their goals.
- Ransom-ware attacks are increasing with organized criminals using it as a money-making tool.
- According to a recent study, a cyber attack occurs every 39 seconds. (Ref. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- Phishing is sending emails, supposedly from reputable companies, to induce individuals to reveal personal information. These attacks are a primary entry method for malware.
- Cyber threats can enter the company's systems through emails, attachments and from portable storage devices, such as thumb drives or other portable storage devices.
- Ninety-five percent of cyber security breaches are caused by human error. (Ref. https://www.cybintsolutions.com/employee-education-reduces-risk/)

What Can You Do?

- Always verify software update requests with IT before following through, and install approved updates in a timely manner.
- Ensure your firewalls and other network software are up to date and turned on.
- Make sure to backup your systems and data regularly.
- Use strong passwords for all access. Do not share passwords or accounts and change passwords regularly.
- Do not save passwords on browsers.
- Don't click on links or attachments in emails sent from someone you don't know.
- Never install unapproved software on any company computer; make sure access keys and other physical security devices are properly secured.
- If you use remote access, follow the company's requirements. Be especially vigilant if using public internet sites.
- If something on your computer seems odd or different, ask for help! It could be a hacker trying to gain access.

Cyberattacks are real. You are a vital part of the defense.