PLANT OPERATIONS

Cyber Security Steps to Mitigate Risk

*by **Dan Laurencelle**, Arctic Glacier, Inc.*

Cyber risk is increasing. In 2021, cyber risks were ranked the #1 concern. This is up 105% from the cyber ranking of #25 in 2009 *(Aon 2021 Global Risk Management Survey)*.

In 2020, the FBI Internet Crime Complaint Center received a record number of complaints from victims of cyber crime: 791,790; losses exceeded $4.1 billion (*https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf*).

Ben Franklin once said, "An ounce of prevention is worth a pound of cure." He was referring to the fire threat in Philadelphia in the 1700's; suggesting that preventing a fire is better than fighting a fire. The same analogy is true for cyber threats.

Most often, small to mid-sized businesses (SME) are targeted by cyber criminals as they may not be as sophisticated as big business, and often do not have in-house I.T. experts on staff. The damage that a cyber event can cause a SME could potentially mean bankruptcy, therefore, it is prudent to understand what proactive steps you can take to prevent cyber events now.

Below are some cost-effective ways to address the two most common root causes of a cyber event:

Human Error

Employees are the front line of defense against cyber criminals as one wrong click can take down an entire I.T. system. Businesses can prevent losses from occurring by training employees on Social Engineering risks. Cyber criminals rely on inexperience and people's natural curiosity and their desire to help.

Teach employees to consider the following with respect to email:

- Is the email address suspicious or from a misspelled familiar name? Compare the spelling of the email address to the display name - scammers use slight differences and can impersonate others with only a slight variation.
- Is the email from someone you know but the message is unusual? Does it create a sense of urgency or mention consequences? Is the email unsolicited?
- Is it a business email but it's sent from a Gmail, Yahoo or Hotmail domain?
- Does the email use bad grammar or have spelling errors?
- Are you being asked to clink on a link or open an attachment? Hover over the hyperlinks (DO NOT CLICK!) and verify if the domain name is spelled correctly. Look for any details that do not match.
- If the email is suspicious, delete the unopened email and do not respond.

Inadequate I.T. Security Measures

- Cyber criminals target poorly secured systems. Practice good Patch Management:
  - Ensure all software is up to date with the latest version, especially those programs requiring security patches. This includes all devices on your network (laptops, desktops, servers, networking equipment) and the IoT (Internet of Things) such as personal mobile devices and iPads. It is important that firmware is up to date and that security patches pushed down from the manufacturer are installed as they are received.
- Introduce effective password policies:
  - Ensure passwords are changed frequently.
  - Ensure employees are forced to choose a password that contains a combination of capital and lower-case letters, numbers and/or symbols.
  - Don't allow them to reuse passwords or variations of old passwords. Train employees not to reuse passwords across multiple websites.
  - Avoid guessable passwords.
- Set up Multi-factor Authentication on VPN and remote access as well as personal devices. Free apps like Google Authenticator and Microsoft Authenticator work with Android and iOS devices.
- Backup your data often to ensure the ability to recover from data corruption or loss. Schedule your devices to backup automatically and ensure that you have redundancy. Use USB Drives, external hard drives, virtual servers or cloud backup solutions. (There is free backup software available - Google Drive is one option.)

All businesses, no matter the size, should perform a risk assessment of the information stored in their system, the electronic programs required to continue working and any potential vulnerabilities before a loss occurs. If a cyber attack is not prevented, a SME must understand exactly what the impact may be to their business and their customers. If your system was unavailable for a period of time, could your business continue working? Can you still operate your equipment and machinery manually? Can you track your assets and manage supply chain?

- What do you need to protect so you can continue to operate through a cyber event/breach or disruption? Is all your banking information online? How will you contact the bank and make payments or receive funds without your device and your fob? Are all your insurance policies electronic? How will you contact your broker or insurer to make a claim? Do you have that information at your fingertips?
- Can customers continue working in the event your SME is the target of malware or ransomware? What systems are critical to your clients?
- Engage your Business I.T. Solution services to help in the assessment to choose the best ways to protect your business and your investments.

Below are some links to free cyber awareness websites in Canada and the USA that may be useful as you manage cyber risk:

Canada - GetCybersafe.ca
www.getcybersafe.gc.ca/en

USA - CISA Cybersecurity Awareness Program
www.cisa.gov/about-stopthinkconnect

Sources: CISA (cisa.gov), GetCybersafe (getcybersafe.gc.ca), AON Report (2021 Global Risk Survey)