GTS Is on a Cybersecurity Roll

By Tiffany Marchi

Systems locked. Operations crippled. Orders delayed. Data compromised and held for ransom. Reputations tarnished. After their systems were hacked, manufacturers like Merck Pharmaceuticals, Taiwan Semiconductor (the maker of computer chips for Apple products), and Saint-Gobain (a plastics/polymer manufacturer) had to address issues they never thought would happen to them.

Why? Our industry – manufacturing – is a prime target for digital threats. According to a 2018 study from the Engineering Employers' Federation, **"*Half* of manufacturers have been the victim of cybercrime, with the sector now *the third most targeted* for attack."**

This is true for several reasons:

1. Manufacturers like APS have tons of intellectual property, plans, and trade secrets that hackers would love to get their hands on (to sell to our competition, or to extort money by attempting to sell our data back to us).

2. Hackers know that the manufacturing industry as a whole is seriously behind the times when it comes to data security – we're easy prey.

3. In addition to stealing the employee and customer information, online criminals can completely shut down production operations (and hold us hostage for ransom) if they hack an assembly line machine or an industrial robot.

GTS is aware of all of this and is increasing data security with the following initiatives:

- **User Education.** The GTS Stream channel features educational content to increase awareness about email phishing, since this is the primary way that hackers gain access to company systems and info. [1]
- **Threat Analysis**. GTS has conducted some initial testing to assess how secure we are at APS and will continue to do so – because the best way to stop hackers is by finding the chinks in our armor and welding them shut ourselves before online criminals can find their way in.

"Email phishing is the primary way that hackers gain access to company systems and info."

- **Office 365 Migration**. Rolling out Office 365 is a crucial part of data security. Once all APS data is in OneDrive and SharePoint, we can increase protection by adding additional encryption, redacting data (so that info can't be seen by hackers), and using Microsoft's Advanced Threat Protection tools to stop attacks before they start.
- **Spotlight on APS GTS**. Since APS GTS is leading the way in technology among manufacturing companies in Ohio, our very own Scott Farris has been selected as a featured speaker at the MCPc Annual Sales and Marketing Meeting. Scott will present a case study of how technology changes are rippling through our company, and how other businesses can follow APS' example.

Hacking attacks are a concern that affect us personally and professionally – they happen online every 39 seconds[2] **and 95% of cybersecurity breaches are due to human error.**[3] GTS will continue to keep APS completely secure and we appreciate your willingness to help our entire company stay safe.

1 Source: Verizon, *2017 Data Breach Investigations Report,* (2017).

2 Source: Daniel Ramsbrock, Robin Berthier, and Michel Cukier, *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks,* "Profiling Attacker Behavior Following SSH Compromises," (2007).

3 Source: IBM, *X-Force Threat Intelligence Index 2018,* (2018).