**Technology Department**
**April 2018**

## Cyber/Network Security

As mentioned last month, Browning has partnered with the Multi-State Information and Sharing Center (MS-IASC), a non-profit that works with the Department of Homeland Security (DHS) working with government organizations including school districts to establish new tools, review existing tools and monitor these systems for our cyber security efforts. One of the benefits is MS-IASC provides a network monitoring service.

During the March 25 through April 7, 2018 - just a short 2 weeks, Browning's defense mechanisms performed well stopping:

- 4,329 port scans on our firewall - this is where the bad guys scan routers and firewalls (very possibly the one in your home) looking for vulnerabilities and points of entry to attack our network. A properly configured firewall denies these illegitimate port scans and is transparent to our end users.
  Browning 4,329 Bad Guys 0
- 3 DoS (Denial of Service) Attacks - this is where the bad guy sends a flood of data at our defense mechanisms looking for weaknesses and all around just trying to slow us down so we don't have use of our network connections. All 3 were stopped by our firewall defense although 1 of the DoS attacks stopped our traffic for approximately 5.8 seconds. Along with our own firewall protections, internet service providers around the world play a key part in preventing/slowing down these types of attacks.
  Browning 2.999998 Bad Guys 0.0000002
- 28,000+ phishing attacks - this is the attack where the bad guy sends emails with various links trying to get the user to click links and give up personal details such as their passwords, banking information, social security numbers and other information potentially devastating to the user. A few of these phishing attack emails are bound to get through the defense mechanisms but 99.91% of them were caught in our spam filters courtesy of Google hosting our email services.
  Browning/Google 27,974 Bad Guys 26
  This attack is considered to be one of the lowest risk attacks to our network and infrastructure although could be quite devastating to an individual if they inadvertently give out their personal information. Many of our users already know to just delete the email or give us a call to ask about it.

We will be able to continue moving forward with some great additional cyber defense tools as well as expanding our library of known attack methods to monitor to keep our network and data safe.

## E-Rate

Just a quick update, our Form 471's have been filed for our internet and the last of our telephone eligible services as we enter the 10% funding year where we will feel the additional financial hit on our 3 Rivers telephone bill.

**META (Montana Educational Technologists Association)** is the consortium of many of the Technology Directors from around the state. We met in Helena for our annual meeting this past March where much of the discussion centered around our cyber security in light of the Columbia Falls incident this past September. The good news for BPS is that the weaknesses exploited on the Columbia Falls network attack have long a go been secured in our environment. BPS has taken advantage of some of the discussion such as implementing the MS-ISAC alliance agreement for alerts and network monitoring.

At the annual meeting I was nominated for the President-Elect position in META and now that the electronic voting is complete have been elected to that position. We'll have a seat at the forefront of the technology discussions in the state and legislature over the next 6 years as I fulfill the next 2 years as President-Elect, 2 years as President and 2 years as past President.