A Note from the desk of:

Jason Venner, HR Manager

October is Cyber Security Month. It's a time when everyone, especially businesses, should be looking at their own data security and how they protect their information. The latest, and most frightening threat these days for companies is what's known as "ransomware." This is when a hacker gets into a company's networking system, shuts it down, and then demands payment in order to return to operational normalcy. Because nearly everything is done on an IT network and company issued devices these days, hackers know they can basically hold any Company hostage.

An easy Google search can illustrate this for us. Taken from analyticsindiamag.com:

1. American oil pipeline system Colonial Pipeline Company suffered a major ransomware attack in May this year. The cyberattack affected its computerized equipment managing the pipeline originating from Houston, Texas, disrupting the fuel supply to most of the US East Coast for days. With the FBI's help, the company paid $4.4 million in bitcoin, as demanded by the hackers. (Yikes!)
2. Taiwanese computer giant Acer was hit by a ransomware attack in March this year. The hackers demanded a whopping $50 million. They shared images of stolen files as proof of breaching Acer's security and the consequent data leak. These included images of financial spreadsheets, bank communications, and bank balances. (Double Yikes!)
3. Chicago-based CNA Financial Corp., one of the largest insurance companies in the USA, had noticed a breach in March this year. The ransomware attack is said to have led to the compromise of data of around 75,000 individuals. This data might have included names, health benefits information, and Social Security numbers of the company's present and former employees, contract workers, and their dependents. CNA agreed to pay $40 million in ransom. (Triple Yikes!)
4. Around the same time as the Colonial Pipeline Company cyberattack mentioned above, the group DarkSide targeted Germany-headquartered chemical distribution company Brenntag. DarkSide reportedly demanded $7.5 million, or 133.65 in bitcoin for gaining access to 150 GB worth of data. Additionally, DarkSide shared a data leak page consisting of a description of the data stolen and screenshots of a couple of files to prove its claims. The ransom was negotiated, and ultimately, Brenntag ended up paying $4.4 million. (Super Yikes!)
5. A subsidiary of Hyundai, Kia Motors, suffered ransom in February this year. Attackers DopplePaymer gang reportedly asked for $20 million for a decrypter and not leak the stolen data. As claimed by Kia Motors, the subsequent 'IT outage' affected the mobile UVO Link apps, payment systems, owner's portal, phone services, and internal sites used by Kia Motors America. (Super-Super Yikes!)

Even if you don't have access to company email or company information, issued devices, etc., you are still a potential target through your own, personal devices or home network. Create and utilize passwords on your personal devices and delete emails that look weird. Install some form of ant-virus on your personal computers, and ask Shauna and Paul if you have any questions regarding cyber security here. The one thing hackers don't have on Clampco is that we have the ability to stop and think before we click.

Our 14001 Environmental Audit went well. The auditor identified a few things for us to shore up, but on the whole, we did quite well. I wanted to thank those who helped prep for the audit, as well as those who were audited themselves. Nicely done!

Fred Fagan has stepped up to the task of absorbing Environmental Health & Safety tasks from Ian. We look forward to having Fred assist us with our safety initiatives going forward. Thank you Fred!

Positive Awareness Awards go to:

Jared Morgan	**Stacy Kemp**	**Steve Bushong**
Nick Beattie	**Jeff Shultz**	**DeNeyl Moore**
Katume Katende	**Yvonna Koch**	**Brenda Martin**
Amber Drayer	**Kelly Berryhill**	**Frank Kirby**