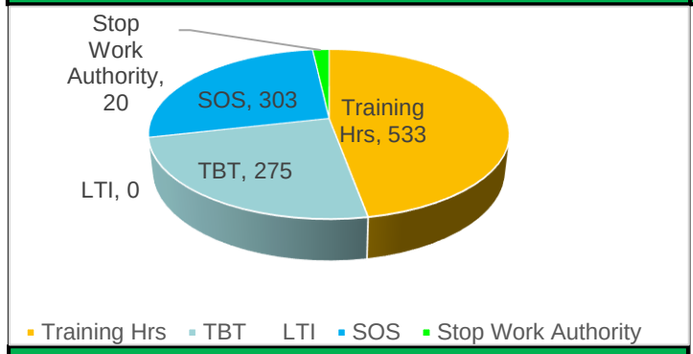
Sep HSE Bulletin 2021

HSE Statistics Report Aug 21



Spetco Aug 21 Winners

Awards	Name	Remarks
Best Drivers	Vishal Chhetri 2472	WS
	Gurpal Singh 2555	GSF
	Munawar 2988	NK
Best SOS	Mathew 1390	GSF
	Alex 1564	WT
	Anas Ali 2763	JPF
	Johnson 1292	EPF

For more information on "Security tips for working remotely" please visit:
https://youtu.be/n9yYprpKoKM

Spetco HSE Motivational Programs

*SOS- Safety Observation System

Cyber Security & Chemical Operations

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 you can do?

- Ensure your firewalls and other network software are up to date and turned on.
- Make sure to backup your systems and data regularly.
- Do not save passwords on browsers & don't allow strangers to use your system.
- Don't click on links or attachments in emails sent from someone you don't know.
- Change your passwords whenever such employees are leaving the company.
- Equipment or part replacements shall only be purchased from reputed suppliers.
- Use strong passwords for all access. Do not share passwords or accounts and change passwords regularly.
- Always verify software update requests with IT before following through and install approved updates in a timely manner.
- Never install unapproved software on any company computer; make sure access keys and other physical security devices are 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.
- Restricting & control usage of USB device (including smartphones) to corporate device. Does everybody need this access?
- Do not allow third party engineers connect to the control system with their laptop or USB. Ensure such engineers are buddied all the time.

On 05 Feb 2021, a water treatment plant employee in Florida, noticed that the cursor was moving strangely on the control computer screen. Initially, there was no concern; the plant used remote-access software to allow staff to share screens and troubleshoot IT issues. 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 rechanged the settings.

On 07 May 2021 for one of the largest US pipelines which carries refined gasoline and jet fuel from Texas up the East Coast to New York, was forced to shut down after being hit by Ransomware in a vivid demonstration of of the vulnerability of energy Infrastructure to cyberattack resulting loss of more than 4.4million

Our systems are also 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.