



665 Rodi Road Suite 305
Pittsburgh, PA 15235
Phone: 412.244.0440
Fax: 412.244.9090
www.HMAmembers.org

A chat with the Pros about your Security

Keeping property and confidential information 'secure' requires a lot more than an annual facility inspection and a locked file cabinet. At HMA's 2018 National Conference and Expo, Doug Hoyle and Ross Moore, Pennsylvania Lumbermens Mutual Insurance Company (PLM) associates, provided multiple security measures via their presentation, "**Protecting Your Operations: Cyber/Information Security & Physical Security.**"

Physical Security

Taking the microphone first and discussing 'physical' security methods was PLM Loss Control Director, Doug Hoyle. He told attendees that in 2017, nearly 10 percent of businesses suffered a burglary or theft. Entry was usually through a door or window and 75 percent of the incidents occurred when the premises were unoccupied.

- Hoyle's suggested **exterior** security measures included dusk-to-dawn lighting, warning signage, fencing/gates, surveillance cameras, physical barriers, restricted access, and establishing a police/security presence. **Interior** security measures included monitored security cameras, window/door alarms, motion detectors, off-hours lighting and securement of high value targets.
- Regarding the **human element**, "Good employees are hard to find," Hoyle said. So do your due diligence! Employee background checks are essential. Keep keys to buildings, vehicles, and equipment in 'non-obvious' places. Change/Monitor access codes regularly. Also test/calibrate camera and alarm systems on a regular basis. Conduct walk-around audits, inside and out.

Hoyle's Bottom Line: Be an active participant in the physical 'policing' of your businesses and holdings.

Cyber Security

IT Security Analyst, Ross Moore, took the podium to discuss data protection measures and staying 'safe' online. "The threat of data breach is real," Moore said. "To secure it, apply the basics of safety to technology." Just as locks, alarms, law enforcement experts and other measures protect physical assets. Data can be secured in much the same way.

- Have **people** who know what they are doing, run/manage your technology.
- **Know what you are protecting** - Computers, phones, other electronic devices, Personal/Customer/Employee information, identity, credit/banking data
- **Know the Threats** - Links/attachments in emails, internet and web (anything that starts with www is suspect), Hackers/Crackers, Competitors, Thrill Seekers

- **Adopt/Implement IT Best Practices** – Passwords should be unique, changed every 90 days, and not shared. Backups should be done daily. Protect Servers (antivirus). Protect Workstations (install endpoint protection and set to auto-update). Educate employees to STOP clicking on 'things' and how to recognize a phishing email.
- Insure yourself with **Cyber Insurance**.

Moore's Bottom Line: Hackers want personal information and will go to great lengths to get it!

The PowerPoint and audio portion of the entire session are available in the **Members Only** section of www.HMAmembers.org.