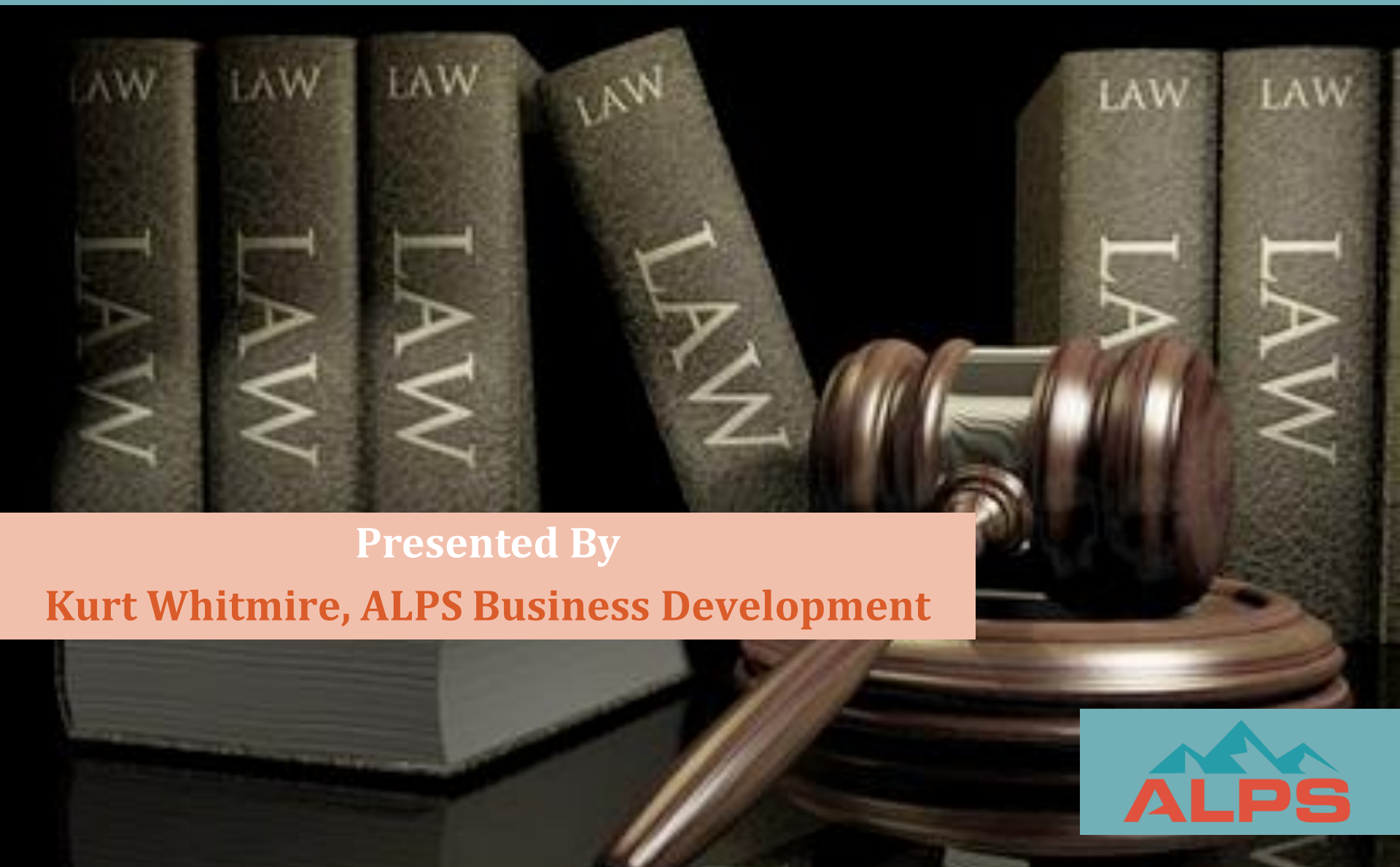
Cybersecurity:
How to Keep the Hackers at Bay

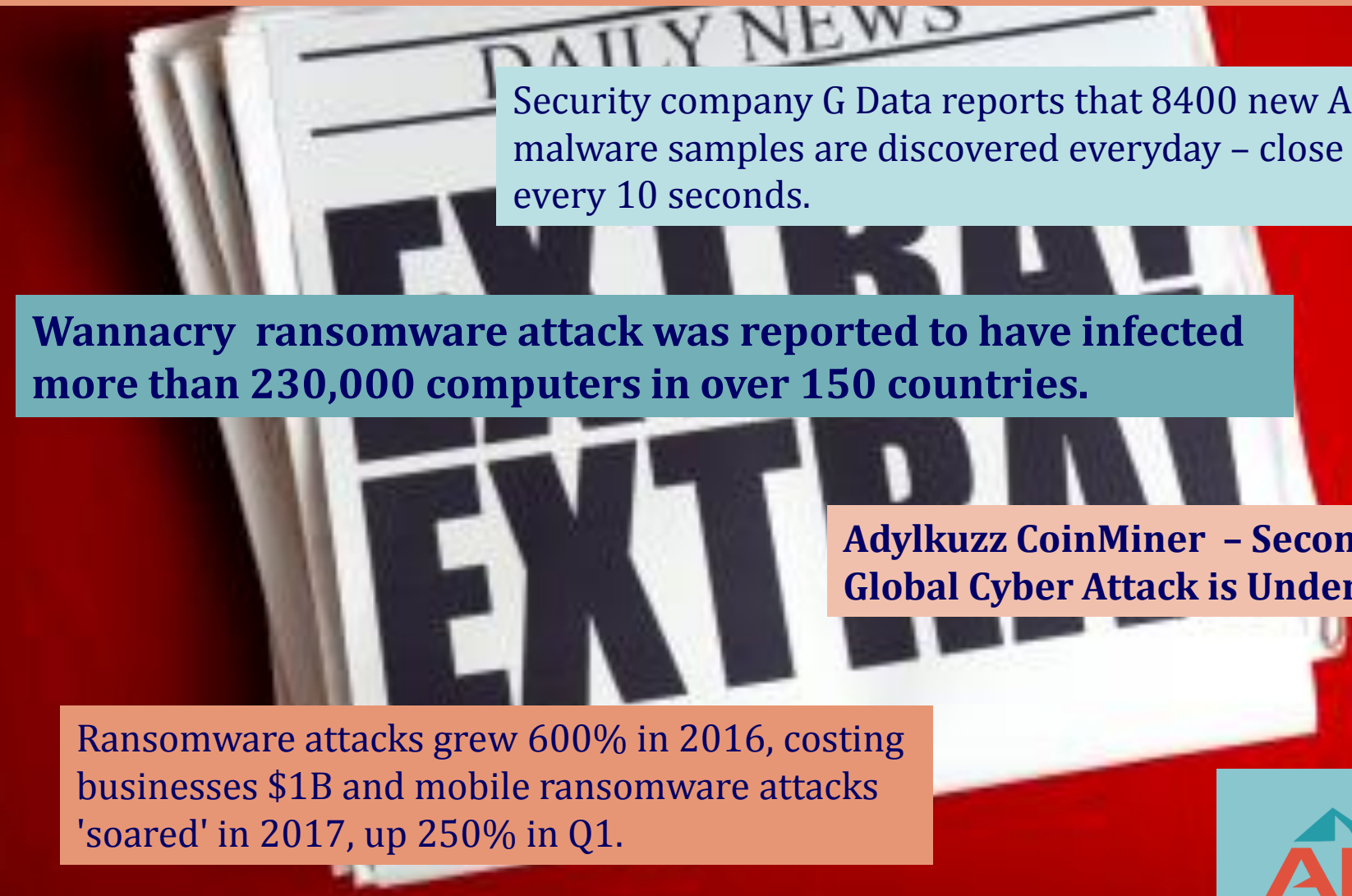


Presented By

Kurt Whitmire, ALPS Business Development

ALPS

A Sampling of Recent Cyber Crime Headlines



Security company G Data reports that 8400 new Android malware samples are discovered everyday – close to one every 10 seconds.

Wannacry ransomware attack was reported to have infected more than 230,000 computers in over 150 countries.

Adylkuzz CoinMiner – Second Major Global Cyber Attack is Underway.

Ransomware attacks grew 600% in 2016, costing businesses $1B and mobile ransomware attacks 'soared' in 2017, up 250% in Q1.

ALPS

When it comes to cybercrime…

Some of the risks you face by not doing enough…

- ✓ Legal liability to others (employees and clients) for the loss, theft or unauthorized disclosure of PI Information
- ✓ Legal liability for the loss of client funds
- ✓ Legal liability for the loss of 3rd party corporate information
- ✓ Being subject to regulatory action for the failure to comply with state breach notification laws
- ✓ Having to cover the costs of responding to and recovering from a breach
- ✓ Damage to your reputation
- ✓ Loss of revenue due to a breach

ALPS

Cyber security is the goal and remember the RPCs are in play!

- ✓ Rule 1.1 Competence
- ✓ Rule 1.6 Confidentiality of Information
- ✓ Rule 5.1 Responsibilities of Partners, Manager, and Supervisory Lawyers
- ✓ Rule 5.3 Responsibilities Regarding Non-lawyer Assistants

Cyber Secure = All data is protected

Personally identifiable information:

- ✓ Names
- ✓ Social security numbers
- ✓ Birth dates
- ✓ Place of birth
- ✓ Addresses

Client confidences and property

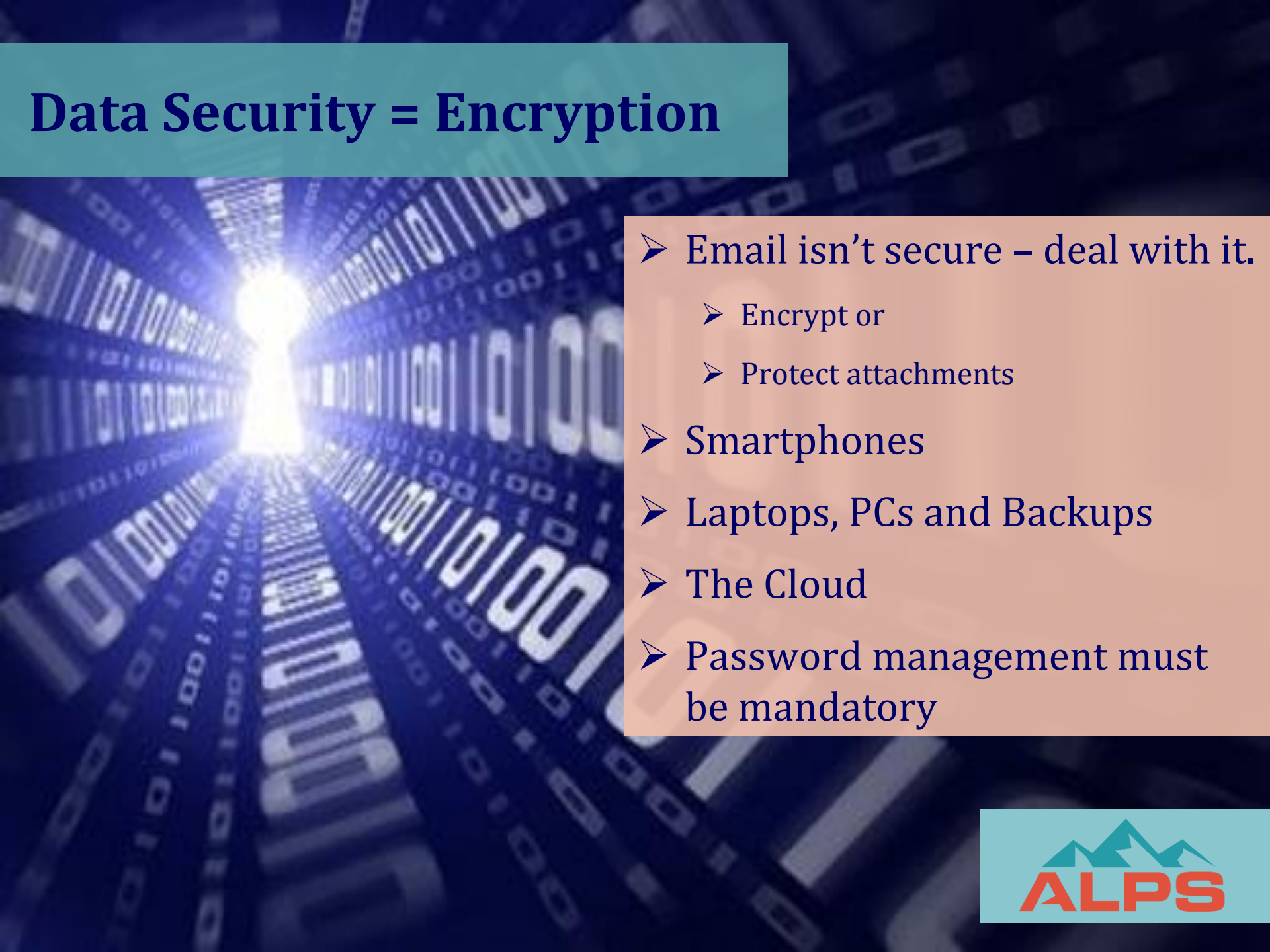
Financial and medical too!

- ✓ Credit card numbers
- ✓ Health records
- ✓ Health benefits account data
- ✓ Bank account numbers
- ✓ User names and account passwords

Staff and Attorneys included

ALPS

Data Security = Encryption



- Email isn't secure – deal with it.
  - Encrypt or
  - Protect attachments
- Smartphones
- Laptops, PCs and Backups
- The Cloud
- Password management must be mandatory

Passwords Make My Head Hurt

- Require strong passwords and periodic changes
  - Combination of upper & lower case characters, numbers, and special characters
  - Be at least 15 characters in length if possible
  - Strong passwords are not…..
- Enforce the policy
  - No sharing
  - Always decline “Remember Password”
  - No writing them down
- Maintain a master list
  - Personal or enterprise level password mangers
  - Encrypted file with limited access

ALPS

A specific example: Wire fraud.

How to Not Become Yet Another Victim of Ransomware

- ✓ Robust Internet security software suite installed on all servers, PCs, laptops and mobile devices to include remote (e.g. home) computers
- ✓ Effective patch management coupled with current software versions
- ✓ Attorney and staff training on insider negligence to include social engineering attacks and how internal systems work.
- ✓ Establish a protocol for the secure use of Wi-Fi networks
- ✓ Use of strong passwords with policy enforcement
- ✓ Regular backups of all critical data
- ✓ Robust security hardware

Safe Browsing Basics

- ✓ Don't let anyone take you anywhere
- ✓ No unauthorized downloads
- ✓ Never give out information unless you initiated the contact
- ✓ Only Open an attachment from a known and trusted source
- ✓ Never click on a pop-up
- ✓ Never allow your browser to save passwords or other information

- ✓ Don't respond to unsolicited junk mail
- ✓ Visit only reputable sites
- ✓ Don't use public computers
- ✓ Don't disable firewalls
- ✓ Use VPNs
- ✓ Use two factor authentication on any service/software that offers it
- ✓ And….

ALPS

Develop written policies, provide training, and then enforce them.

Should address as a minimum:

- ✓ Participation in social media
- ✓ Remote access
- ✓ Personal use to include streaming, downloading, and email
- ✓ Use of Bluetooth
- ✓ Use of personal devices for work
- ✓ Backup expectations
- ✓ Physical security of devices
- ✓ Data security
- ✓ Email preservation

THANK YOU. ARE THERE ANY QUESTIONS?

Please feel free to contact our ALPS Risk Manager anytime to discuss this presentation or any other risk concerns.

Mark Bassingthwaighte

- mbass@alpsnet.com

ALPS Website

- www.alpsnet.com

ALPS 411 Blog

- www.alps411.com