Protecting Your Operations

PHYSICAL SECURITY & CYBER SECURITY

Pennsylvania Lumbermens Mutual
INSURANCE COMPANY

HMA
Agenda

Physical Security
- Why you should remember physical security
- Securing the premises and the interior
- The human element

Cyber Security
- Security is a mindset
- Knowledge and fundamentals
- Reasonable security
- Employee education
PHYSICAL SECURITY: STATISTICS

- 9% of businesses suffered a burglary or theft in 2017
- Forcing a door or window is the most common entry technique
- 75% of incidents occur when premises are unoccupied
- The more isolated the area, the higher frequency of incidents
- Burglaries often lead to other losses (arson)
PHYSICAL SECURITY: THE PREMISES

- Dusk-to-dawn lighting
- Fencing/Gates
- Posting signs
- Police presence
- Security (firm or employees)
- Low profile shrubs & trees
- Surveillance cameras
- Physical barriers
- Restricted access
PHYSICAL SECURITY: INTERIOR

• Monitored security cameras
• Local/Central station alarms
  ➢ Door/window contact
  ➢ Motion detection
  ➢ Sound/glass breakage
• Fortify skylights
• Lights during off hours
• Conceal/Secure high value targets
PHYSICAL SECURITY: HUMAN ELEMENT

- Background checks
- Minimize cash
- Key control program
  - Building
  - Vehicles
  - Equipment
- Change access codes
- Test/calibrate systems
- Pre/Post operating hours check

POLICE PERSPECTIVE
CYBER SECURITY
Consider how you do other things safely and correctly...

...then apply that to technology
Security is a Mindset
Rapid technological advancements won’t stop

The basics of safety still apply...and work
Know What You’re Protecting

WHAT
▲ Physical Assets
▲ Digital Assets
▲ Financial Assets

WHY
▲ Your Reputation
▲ Continuity of Your Operations
▲ Protecting your Assets

HOW
▲ Know Your Threats
▲ Know Your Technology & Risks
▲ Adopt Some Basic Best Practices
▲ Educate Yourself and Your Employees
▲ Insure Yourself with Cyber Insurance
Know The Threats

▲ Links/attachments in emails (90%)
▲ IoT
▲ Internet and web – they’re both vulnerable
▲ Ne’er-do-wells to be concerned about
  ▪ Hackers/Crackers
  ▪ Competitors
  ▪ Hacktivists
  ▪ Thrill Seekers
▲ Hear of the Dark Web or Deep Web?
  ▪ Anything that starts with www is suspect
Know Your Technology

Outer Boundary-Virtual e.g., Firewall

Middle Endpoints- Physical e.g., Antivirus

Inner Passwords-Data e.g., Files

Internet Firewall Home or Business Network
Know Your Technology

Outer
Boundary-Virtual
e.g., Firewall

Middle
Endpoints- Physical
e.g., Antivirus

Inner
Passwords-Data
e.g., Files
The Importance of Fundamentals

“The minute you get away from fundamentals – whether it’s proper technique, work ethic or mental preparation – the bottom can fall out of your game, your schoolwork, your job, whatever you’re doing.”
Michael Jordan

“Gentlemen, this is a football.”
Vince Lombardi

“Everything in life goes back to the basics.”
Kron Gracie, BJJ

“It all comes back to the basics. Serve customers the best-tasting food at a good value in a clean, comfortable restaurant, and they'll keep coming back.”
Dave Thomas, Wendy’s

“…if you do this type of work long enough you realize that the mastery of the basics is the true objective.”
James Hamilton, VP of Gavin De Becker and Associates
The Puzzle of Information Security

- Backups
- Contract
- Review
- Trusted Advisor
- Patching
- Passwords
- Education
- Cyber
- Endpoint Protection
- Liability
- Reasonable Security
Best IT Security Practices

Passwords
- At least 8 characters, with a number, symbol, uppercase, lowercase
- Change at least every 90 days
- Don’t share your password with anyone

Backups
- Backup to the cloud every day
- Test by restoring at least every 90 days
- Backup any data that you believe needs backed up

Protecting Your Servers
- Patch critical updates within 2 weeks; others at 3-4 weeks; don’t auto-update
- Servers get antivirus protection
- Only a certain few get to work on servers

Protecting Your Workstations
- Set OS patches to auto-update
- It’s best if employees can’t install programs on their own
- Install endpoint protection and set to auto-update
- Beware of phishing

Education
- Search online for “10 things you need to do to be secure”
- Tell everyone consistently
Spot a phishing email

1. Fake sender domain.
   (not service@paypal-australia.com.au)

2. Suspicious Subject and content.

3. Bad grammar

4. Hovering over link reveals suspicious URL.
Contact Information

Doug Hoyle
Loss Control Director
Direct: (267) 825-9128
dhoyle@plmins.com

Ross Moore
IT Security Analyst
Direct: (317) 875-3770
rmoore@plmins.com

WWW.PLMINCS.COM
Further Education

- https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/small-businesses
- How the journalist was hacked: https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/
- https://www.us-cert.gov/ccubedvp/smb
- Big Security For Small Business
- https://www.cyberessentials.ncsc.gov.uk/advice/
- Sign up at: https://haveibeenpwned.com/ to be notified if your account has been compromised in a data breach
- Lists and reviews of software at https://www.av-test.org/en/
- Free course on Creating a Security-centric Culture: https://www.pluralsight.com/courses/security-culture-creating
- Search online for cybersecurity for small business or security essentials for business
- Free training for IT: https://www.cybrary.it
- Pinterest has lots of great ideas! Search for cybersecurity business or information assurance
- Great big list of cybersecurity resources: https://www.csoonline.com/article/3209670/it-careers/great-big-list-of-cybersecurity-resources.html
- State and Local Cybersecurity Policies: https://www.cisecurity.org/cybersecurity-policies/
- Expansive glossaries: https://www.sans.org/security-resources/glossary-of-terms/
- Watch cyberattacks in real time: http://map.norsecorp.com/#/