PRIMA'S 2018 RISK MANAGEMENT
WEBINAR SERIES

The Ever-Changing Cyber Landscape

Presented By:
Bryan Thornton, Director, Net Reaction
Hunter Maskill, Vice President, AIG

Common Scenarios

- There's rarely anything new under the sun
- 99% of cybercrime follows common, repeatable patterns
- 85% of vulnerabilities exploited in technical hacks had patches available for 18+ months

Four Common Events

- Phishing
- Ransomware / Cryptolocker
- Lost or Stolen Laptop
- Hacking

Phishing

- You cannot educate your way to zero

- We need to make the consequences associated with clicking not matter as much
  - Unique passwords for critical services
  - Multifactor authentication
  - Consider less access to information

Ransomware / Cryptolocker

- Typically initiated with an email or web-based click-event

- Can be a non-event or life changing event based on your preparation

Ransomware / Cryptolocker

- **Avoidance:**
  - Remove local administrative access
  - Consider multifactor authentication for network access
  - Regularly check backup schema
- **When it Happens:**
  - Best Scenario: wipe the device, restore data from backups
  - Common Scenario: pay the ransom, backup the data, wipe the device
  - Worst Case Scenario: data loss, start from scratch

Lost or Stolen Laptop

- Use whole disk encryption – it's free!
- Good backups are critical, consider the cloud
- Consider multifactor authentication for remote access



Hacking

- Technical Debt Happens
- Being aware of an managing vulnerabilities is critical
- You’re either automating patching or you’re likely woefully behind

Hacking Mitigation Steps

- Perform regular vulnerability analysis
- Automate / schedule patch installation
- Multifactor authentication for administrative access
- Consider cloud services

New & Evolving Coverages

- Dependent Business Interruption
- Unintentional Outages
- Bricking Coverage
- Cybercrime
- Proof of Loss Coverage
- Bodily Injury & Property Damage
- Coverage / Price Concerns

Questions to Take Home

- Have we mitigated the risks associated with phishing attacks?
- Are we using multifactor authentication?
- Are we using whole disk encryption?
- Does our backup schema cover everything?
- Where is our technical debt?
- Does our coverage address our exposure?

Questions?

Bryan F. Thornton, Director

Net Reaction, LLC

bthornton@netreaction.com

615.346.9209

Hunter Maskill

Vice President, AIG Financial Lines

hunter.maskill@aig.com

770.671.2366