LEWIS BRISBOIS

Community Bankers of Washington

COVID19 Cyber Update

May 27, 2020

Exploitation of COVID19 by Malicious Attackers

- **Impact of remote workforce**
  - Attacks on remote users
    - Less protected endpoints
    - Lack of endpoint detection and response
    - Lack of multi-factor authentication
  - Attacks on Remote Desktop Protocol
    - Lack of multi-factor authentication
  - Attacks on networks
    - Fewer personnel watching the network

Primary COVID19 cyber attack vectors and exploits

- **Primary attack vectors**
  - **Phishing email messages**
  - **Brute force on remote desktop protocol**
- **Primary exploits**
  - **Ransomware attacks**
    - Encryption extortion
    - Exfiltration extortion
  - **Email Account Compromises**
    - Credential harvesting
    - Wire transfer redirects
    - Direct deposit redirects
    - W-2 image theft

Create a human firewall

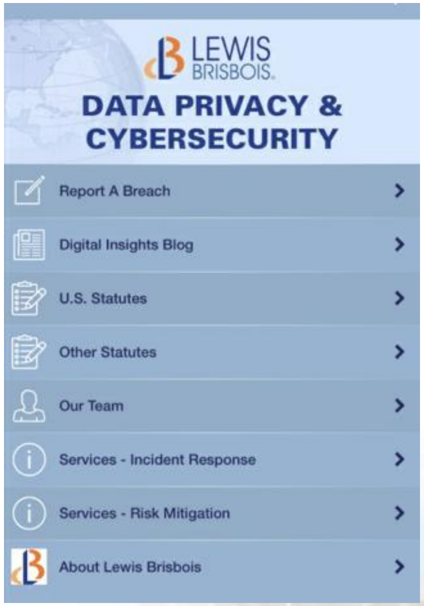
- Since all technological risk cannot be mitigated with technology … **the human user of technology – the employee - is essential to network security**
- It is critical to **establish a culture of security**
  - **Safe environment** in which to communicate
  - **Effective training** programs
  - **Efficient reporting** protocols
  - Create a **human firewall**

Lewis Brisbois – Free resources

- **24/7 telephonic & email hotline**:
  - **844.312.3961**
  - breachresponse@lewisbrisbois.com
- **Digital Insights blog**;
- **Interactive maps**:
  - data breach notification statute maps;
  - information security standards;
- **Data Privacy & Cybersecurity Handbook**; and
- **“Lewis Brisbois Cyber Practice” App**:
  - Available in App Store.

PLEASE VISIT OUR
DIGITAL INSIGHTS BLOG

VIEW OUR
DATA PRIVACY
STATUTE MAP


LEWIS BRISBOIS

DATA PRIVACY & CYBERSECURITY

Report A Breach
Digital Insights Blog
U.S. Statutes
Other Statutes
Our Team
Services - Incident Response
Services - Risk Mitigation
About Lewis Brisbois