Introduction

01 Disclaimers
02 Key terms
03 Cybersecurity in the enterprise - a visualization
04 The solutions
05 What can I do and why should I care?
06 Q&A
Some Key Terms

- Endpoint
- Anti Virus (AV)
  - Malware (AM)
  - Fingerprint
  - Hash - password/other
- Firewall
  - Traffic gateway
  - Packet inspection
- IDS/IPS - Intrusion Detection & Prevention Systems
- DLP - Data Loss Prevention
- AI - Artificial Intelligence; BA - Behavior Analytics;
  ML - Machine Learning; DL - Deep Learning
- MCA - Mission Critical Assets
- Threat Intelligence
- Penetration Testing - PenTest
- Active Defense
  - Active vs passive activity on your network
  - Honeypots
  - NOT hackback
- Attack Surface Baseline
- Cyber Hygiene
- Phishing
- Social Engineering
The Solutions

1. Data/Mission
   Critical Assets
   - Encryption, Access Management, Tags, DLP - Policy

2. Application
   - Access Management, Monitoring, Multi Factor Authentication, VPNs

3. Endpoints
   - Local Firewall, IDS/IPS, Patch Management, ML, DL, BA, DLP, Asset Tracking, AV

4. Network
   - AI Suite (ML, DL, BA), IDS, Segmentation, Active Defense

5. Perimeter
   - AV, Firewall, IDS/IPS, Honeybots, DLP, Tags, Attack Surface

6. Outside Threat

What Can I Do? Why Should I Care?

What Can I Do?
• Understand and question policies - then follow them.
• Hyper vigilant - on the home front as well.
• Educate friends, family and colleagues.
• Social media - just know.
• Over 90% of breaches come from phishing and/or social engineering.

Why Should I Care?
• Company asset protection
• National security asset protection
• National security defense
• Personal and family defense
Dan Wachtler
Cybersecurity, Financial Crime Investigations, Risk Mitigation

Contact at
dan@jatiff.com
jatiff.com

Follow on
Twitter: @CyberDanW
LinkedIn: linkedin.com/in/dan-wachtler/