Top cyber security threats for 2019 (Notes for MVI Boot Camp)

(Distilled from a conversation with FBI)

1. Data Breach

   Cloud data storage and applications

2. Insecure Application User Interface (API)

   Encryption and authentication process must be stringent.

   Cloud-based / web-based practice software for professionals

   (dentists, lawyers, doctors) malicious attacks

3. Malware Attack
4. Loss of Data
5. Hacking
6. **Single-factor Passwords**
7. Insider Threat
8. IOT (Internet of Things) / Convenience Devices

SECURITY TRENDS for 2019

TREND MICRO

- Actual Mass Real-World Use of Breached Credentials Will Be Seen

- Sextortion Cases Will Rise

- Home Networks in Work-From-Home Scenarios Will Open Enterprises to BYOD-like Security Risks

- Innocent Victims Will Get Caught in the Crossfire as Countries Grow Their Cyber Presence

- 99% of Exploit-Based Attacks Will Still Not Be Based on 0-Day Vulnerabilities

- Cybercriminals Will Compete for Dominance in an Emerging IoT ‘Worm War’

- **My favorite from Trend Micro:** Cybercriminals Will Use More Techniques to Blend In - “In response to security vendor technologies, specifically the renewed interest in machine learning for cybersecurity, cybercriminals will use more malicious tactics to “blend in.” New ways of using normal computing objects for purposes other than their intended use or design — a practice known as “living off the land” — will continue to be discovered, documented, and shared. We have been observing a few of these.”

FIRE-EYE

- (More) Nations developing offensive capabilities

- Breaches continuing due to lack of attribution and accountability

- The widening skills gap, and fewer trained experts to fill security roles

- Lack of resources, especially for small and medium-sized enterprises

- Supply chain as a weakness

- Attackers eyeing the cloud, since that’s where the data is headed

- Social engineering, considered by many to be the most dangerous threat

- Cyberespionage, cybercrime and other threats to the aviation industry

MCAFEE

- Cybercriminal Underground to Consolidate, Create More Partnerships to Boost Threats

- Artificial Intelligence the Future of Evasion Techniques

- Synergistic Threats Will Multiply, Requiring Combined Responses

- Misinformation, Extortion Attempts to Challenge Organizations' Brands

- Data Exfiltration Attacks to Target the Cloud

- Voice-Controlled Digital Assistants the Next Vector in Attacking IoT Devices

- Cybercriminals to Increase Attacks on Identity Platforms and Edge Devices Under Siege

WATCHGUARD

- **AI-Driven Chatbots Go Rogue**

- Utilities and Industrial Control Systems Targeted with Ransomware (heard this from others)

- A Nation-State Launches a “Fire Sale” Attack

  A Fire Sale is an all-out cyberwarfare attack that performs a three- stage systematic attack on a nation's computer infrastructure. Hackers called it Fire Sale because "Everything must go". ... It was a major part of the fourth Die Hard film, Live Free or Die Hard.

- **Fileless, Self-Propagating “Vaporworms” Attack**

  29 percent of attacks used fileless malware in 2017

- **Attackers Hold the Internet Hostage**