Sword & Shield
ENTERPRISE SECURITY

# Life in the Convenience Lane, Do We Dare Acknowledge the Security Implications

**By: Teddy Ansink**

# My Background

- Education
  - BS in Electrical Engineering from the University of Tennessee, Knoxville
  - MBA from King College

- Experience
  - US Navy
  - IBM
  - Pilot Flying J
  - Sword & Shield Enterprise Security

- Responsibilities
  - Virtual Chief Security Officer (Healthcare, Financial, and Federal)
  - Assessments and Audits
  - Remediation of Findings from Assessments and Audits
  - Social Engineering

# Security Concerns with New Technology

**New Technologies**

***How do new technologies impact cybersecurity moving forward***

With the addition of new technologies such as Amazon Alexa, iWatches, Electronic Prescription Systems, etc. life becomes easier while opening new avenues for malicious attacks.  Without proper security controls in place that may make these technologies inoperable, we may be accepting risks that we are unaware of.

# Scary Threats for 2018

**From KnowBe4**

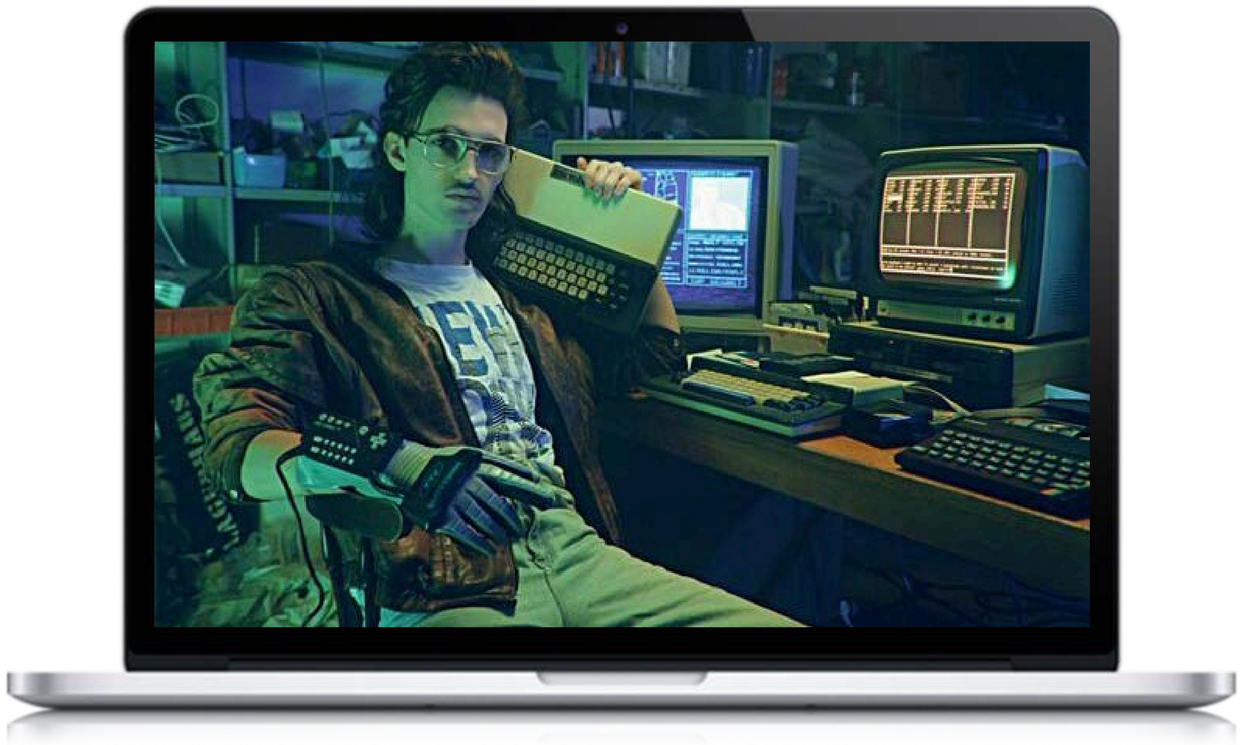
- Exponential growth of the ransomware plague. This attack isn't going anywhere. We have seen a rise in attacks that exfiltrate data, giving the bad guys a secondary way to get ransom payments with threats of data exposure. Also ransomware-as-a-service strains have grown, allowing newbies to easily get in on the game. Kits sell for anywhere from $10 to a few thousand dollars. Custom-made ransomware attacks focusing on high-value targets has been on the rise, and that trend will continue.
- Pseudo-ransomware will continue to be used to distract organizations. They seem like ransomware on the surface, but really in the background hackers are just trying to infiltrate the organization. Multi-vector attacks including smishing, phishing and vishing will increase.
- Phishing automation - bots and intelligent scraping of social media and dark web will make automated spear phishing a very hard to identify problem. The amount of data stolen in breaches over the last couple of years makes it very easy to automate mass spear phishing attacks.

# Scary Threats for 2018 Continued

**From KnowBe4**

- Extortion scams targeting businesses and individuals. Rather than immediate payment to get files back, a different tactic being used which is to demand sensitive content (such as ransomware that demands questionable material, or in the corporate world demanding customer info to get data back). Expect micro-ransomware; extortion one document at a time.
- Search result tampering that will drive users to compromised websites are nothing new, we have seen an increase in this technique over the past years.
- Mobile malware - new families are on the way that will target smartphones and mobile-first users.
- Blame-ware and False-Flag operations increased - The European Union recently declared cyberattacks as acts of war and will appropriately respond to countries carrying out such attacks. Expect to see cyber propaganda operations that are engineered to spark controversy between countries, undermine democracies and destabilize trust globally. Watch out for related clickbait!

# Perception of an Attacker



## Remote Hacking

The attacker is located at some remote location and trying to break through security controls

## Using a Computer

The attacker is located at a terminal and using a computer to hack an environment

## Who They Are

Someone with a grunge personality using exotic software who is a loner or introvert

# Examples of New Technologies

## Electronic Prescription Services

Electronic Prescription Services (EPS) make it possible for your prescriptions to be sent electronically to the pharmacy or dispenser of your choice

## Google Home

Google Home is a brand of smart speakers developed by Google

## Cryptocurrency

Cryptocurrency is a digital asset designed to work as a medium of exchange that uses strong cryptography

## Wearable Technology

Wearable technology includes smart electronic devices that are incorporated into clothing or worn on the body as implants or accessories

## Cloud Ransomware

Ransomware targeting cloud services is one of the six biggest cyber threats likely to face organizations in 2018

## Amazon Alexa

Amazon Alexa is a virtual assistant developed by Amazon

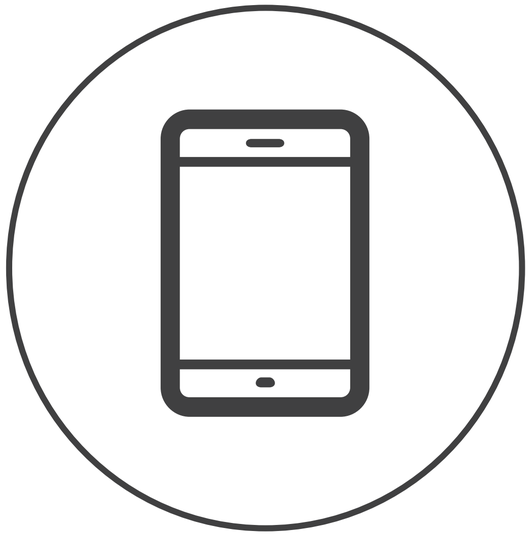
# Electronic Prescription Services (EPS)

**Medical Technology**

***Pros and Cons of E-Prescribing***

- More physicians are starting to transmit their prescriptions to pharmacies online
- Two-thirds of pharmacies-including most chain stores-are ready to accept online scripts
- Electronic renewals are the biggest win so far for physician offices.
- In the future, doctors will have access to pharmacy-supplied medication histories
- The availability of this information poses some liability issues
    - Application Development
    - Availability of Patient Data
    - Accuracy of Information
    - Security on Mobile Devices

# Google Home and Amazon Alexa



**Virtual Personal Assistants**

***Voice-Activated, Internet-Connected Personal Assistants***

- Speakers enable users to speak voice commands to interact with internet services through Google and Amazon intelligent personal assistants
- Your technology is listening – to what degree are the listening
- Internet of Things (IoT) - Mirai malware was used to hijack devices into massive botnets that were then used to launch a coordinated assault against Dyn, a company that hosts the Domain Name System (DNS). That attack crippled such major sites as Twitter, Paypal, Netflix and Reddit
- Defensive Measures
    - Mute the Device
    - Disconnect Sensitive Accounts
    - Erase Old Recordings
    - Online Configuration Settings

# Cryptocurrency

**Cryptocurrency**

## *Cryptocurrencies are Tradeable Cryptographic Tokens*

- Used to secure financial transactions, control the creation of additional units, and verify the transfer of assets
- Limited Legal Protection – there is no precedent to cryptocurrency lawsuits so predicting the outcome is impossible
- Cyberthieves can break into crypto exchanges, drain crypto wallets, and infect computers with malware
- Faced with a growing risk from these cryptocurrency purchases — including fraudulent transactions, disputed charges from cardholders burned by a crypto scam and the inability for some to pay off these large purchases — several of America’s largest banks have decided to ban crypto purchases

# Wearable Technology

**Fitness Accessories**

## *How Much Tracking is Too Much?*

- Fitness trackers can upload a nearly complete record of where you've been and what you've been doing during your every waking moment
    - Police Tracking
    - Employer Tracking – Activity Bonuses
    - Medical Assessment
- Axelle Apvrille (@cryptax) has found that FitBit wearables are open on their Bluetooth ports allowing devices to connect and deliver malware to the bracelet
    - The hack takes about 10 seconds to complete and requires a minute to verify
    - Once the malware has been delivered, any device that connects to the wearable can be infected with a backdoor, trojan, or other malicious software program

# Cloud Ransomware

**Cloud Attacks**

***Ransomware Breaches Defenses and Locks Down Computer Files***

- Ransomware Hits Everywhere
- Ransomware is a particular nuisance because of the files it targets
    - Photos, Music, Films
    - Presentations and Work Documents
    - PDF
- CryptoLocker – scans the local hard drive for a specific list of file extensions AND scans for connected drives/devices (USB's, network drives, etc.)
- CryptoFortress – Encrypts specific file extensions AND enumerates all open network Server Message Block (SMB) shares and encrypts them
- Petya – encrypts an entire Master Boot Record (MBR) causing the system to crash to a blue screen
    - Petya was spread to some systems through an infected file hosted on Dropbox, posing as resume (Social Engineering)


Sword & Shield Enterprise Security, Inc.

1431 Centerpoint Blvd, Suite 150

Knoxville, TN 37932-1984


Social Media

Facebook.com/SwordShieldSec

Twitter.com/SwordShieldSec

Youtube.com/SwordShieldSec


TLA@swordshield.com

www.swordshield.com