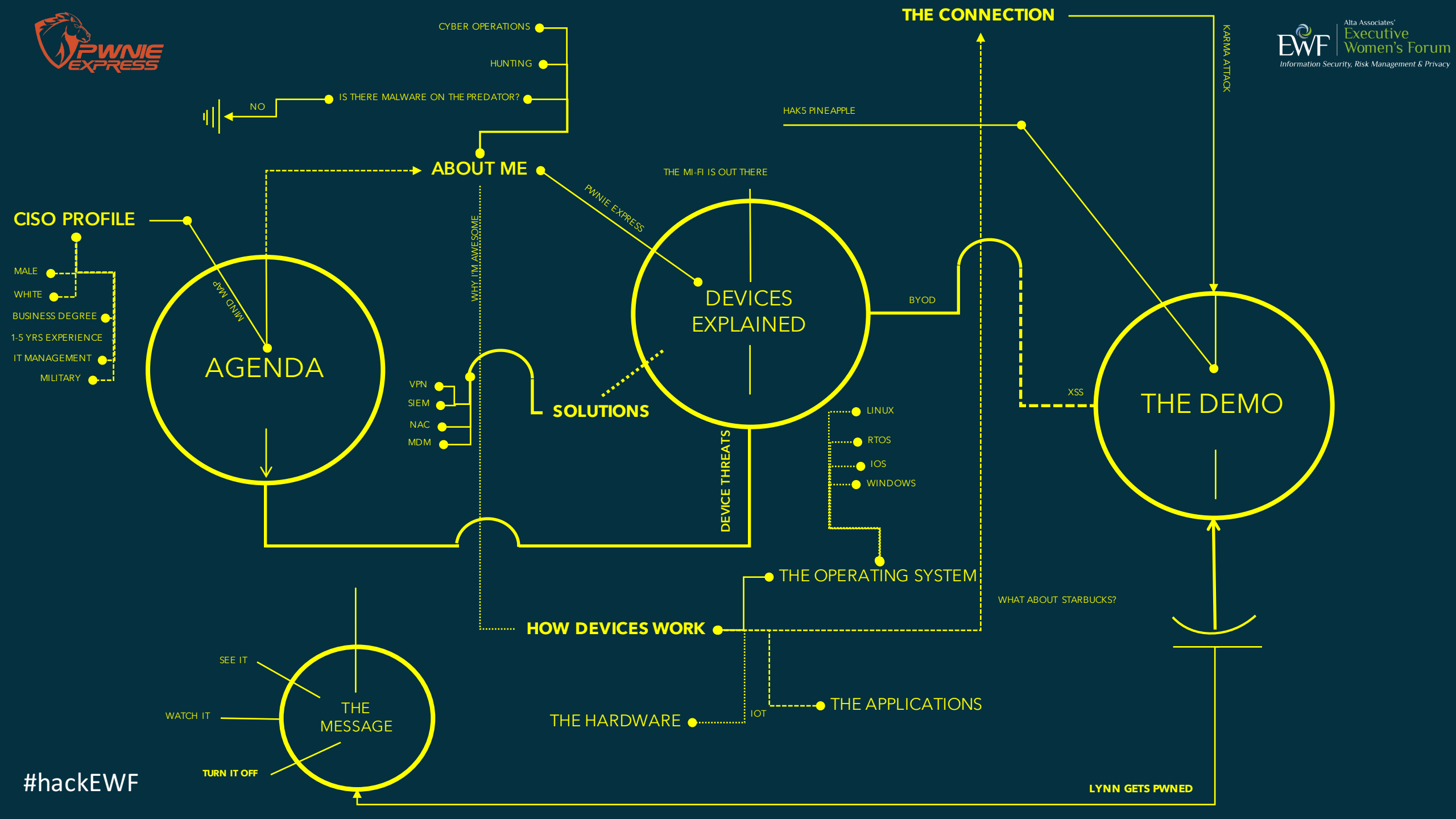

Alta Associates'
Executive
Women's Forum
*Information Security, Risk Management & Privacy*

# The New Device Threat Landscape

## Risks & Mitigations

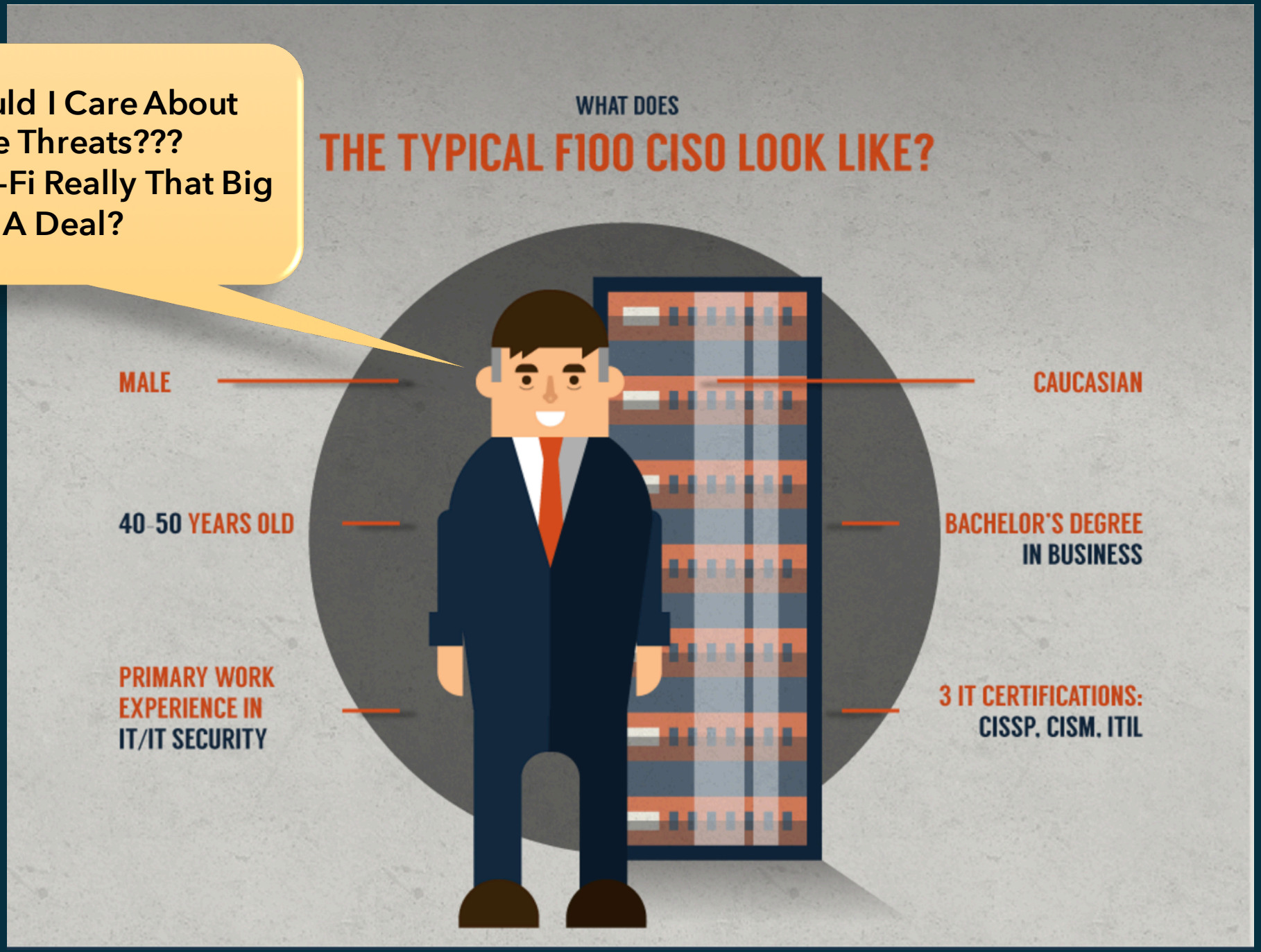
Yolonda N. Smith
Director of Product Management
Pwnie Express


PWNIE EXPRESS
THE CONNECTION
CYBER OPERATIONS
HUNTING
IS THERE MALWARE ON THE PREDATOR?
NO
KARMA ATTACK
Alta Associates' Executive Women's Forum
Information Security, Risk Management & Privacy
HAK5 PINEAPPLE
ABOUT ME
THE MI-FI IS OUT THERE
PWNIE EXPRESS
CISO PROFILE
MALE
WHITE
BUSINESS DEGREE
1-5 YRS EXPERIENCE
IT MANAGEMENT
MILITARY
MIND MAP
WHY I'M AWESOME
DEVICES EXPLAINED
BYOD
AGENDA
VPN
SIEM
NAC
MDM
SOLUTIONS
DEVICE THREATS
LINUX
RTOS
IOS
WINDOWS
XSS
THE DEMO
THE OPERATING SYSTEM
WHAT ABOUT STARBUCKS?
HOW DEVICES WORK
SEE IT
WATCH IT
TURN IT OFF
THE MESSAGE
THE HARDWARE
IOT
THE APPLICATIONS
LYNN GETS PWNED
#hackEWF

# Yolonda in 1 Slide

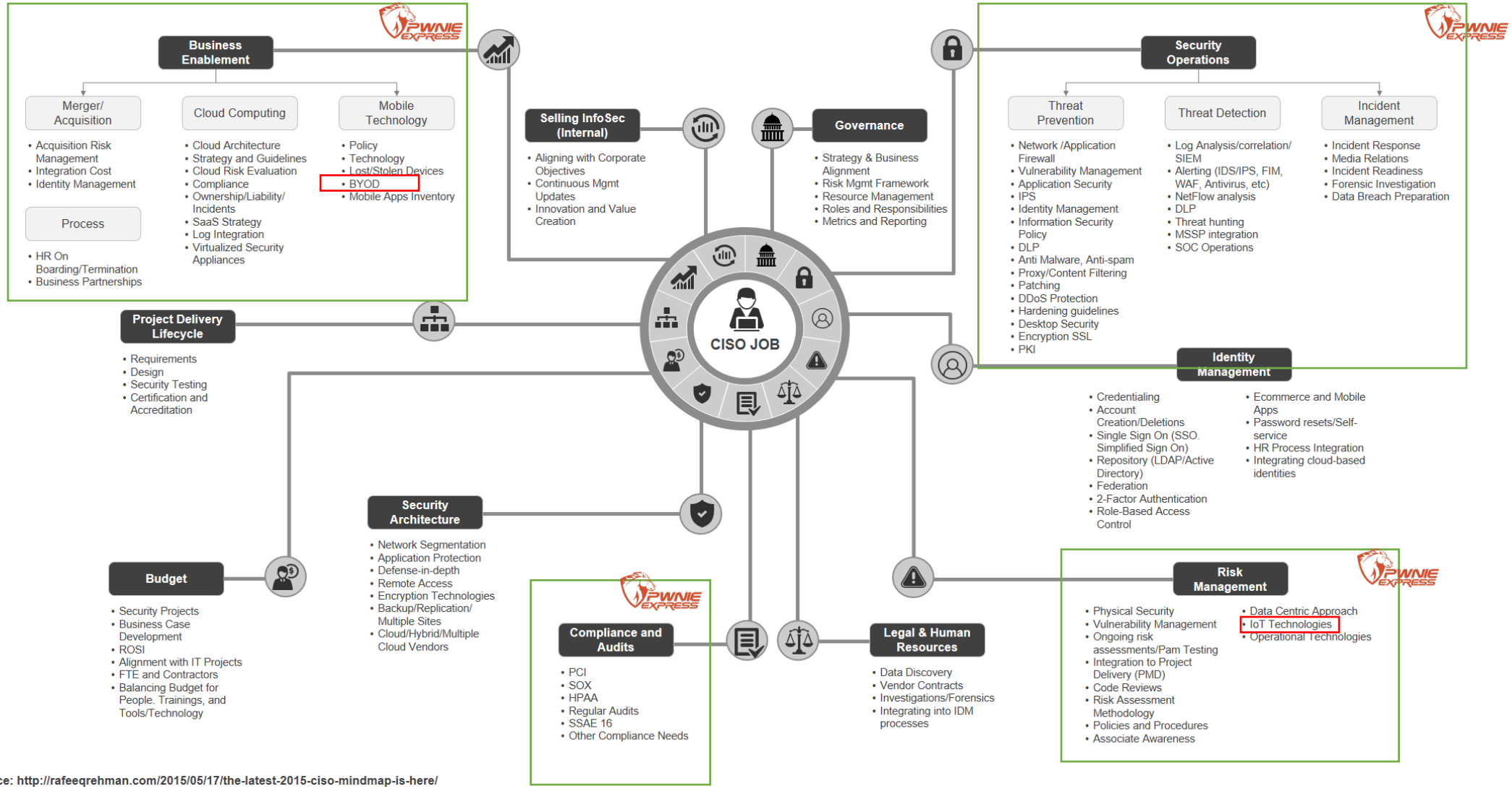
#hackEWF

Why Should I Care About Device Threats???
Is Rogue Wi-Fi Really That Big of A Deal?



# CISO Mind Map

Momentum PARTNERS



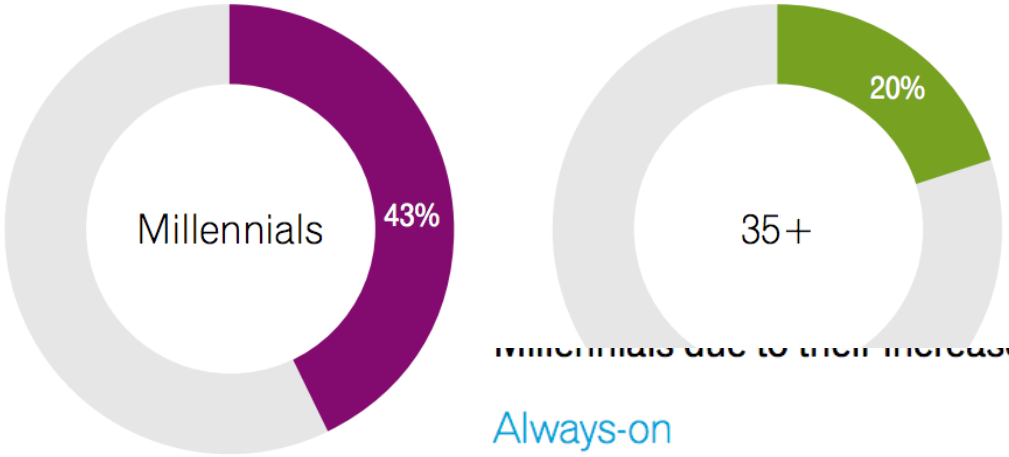

Source: http://rafeeqrehman.com/2015/05/17/the-latest-2015-ciso-mindmap-is-here/

An Overview of The Responsibilities and Ever Expanding Role of The CISO

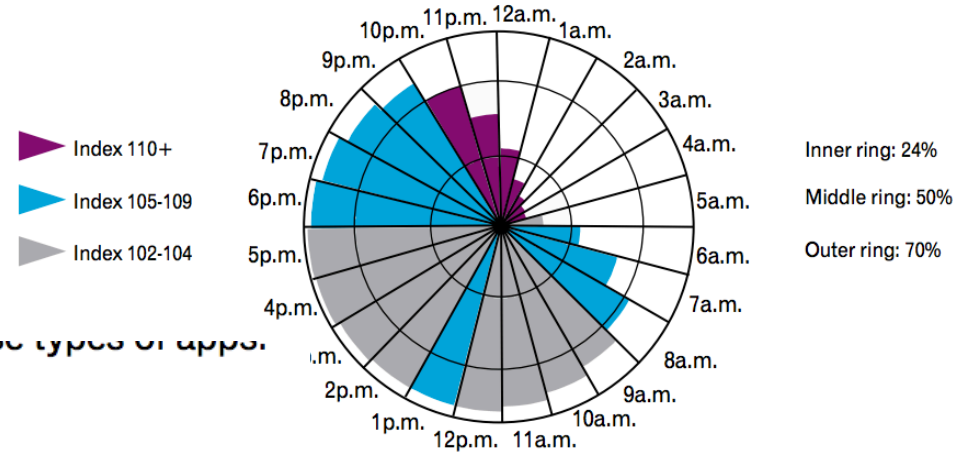
# MILLENNIAL MENACE

# The Connected Workforce

Percent of adults who are mobile dominant when going online




Share of Millennial smartphone owners actively using the device throughout a typical day




## Always-on

Millennials are so connected that half (50 percent) say that they need constant Internet access even on-the-go (compared with 38 percent of all adults). Smartphones are a natural solution to this need and 43 percent of Millennials say that they now access the Internet more through their phone than through a computer compared with just 20 percent of adults ages 35 and older. Hispanic Millennials are even more likely to be mobile dominant with 46 percent accessing the Internet more through their phone than a computer.

The fundamental premise of *every* modern computing device is the consistent, persistent ability to connect to the outside world

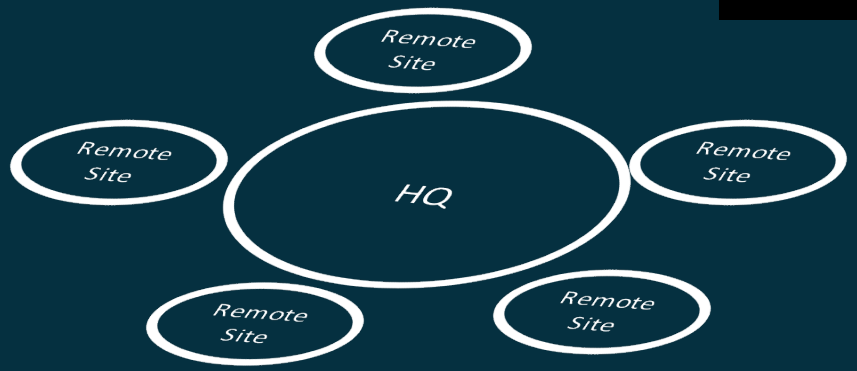
# Connected Devices – The New Threat Gateway


IoT Devices

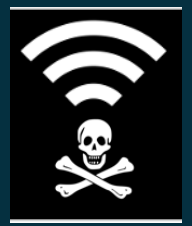
Accessories

Rogue Devices

Employee & Corp. Devices




Corporate Network

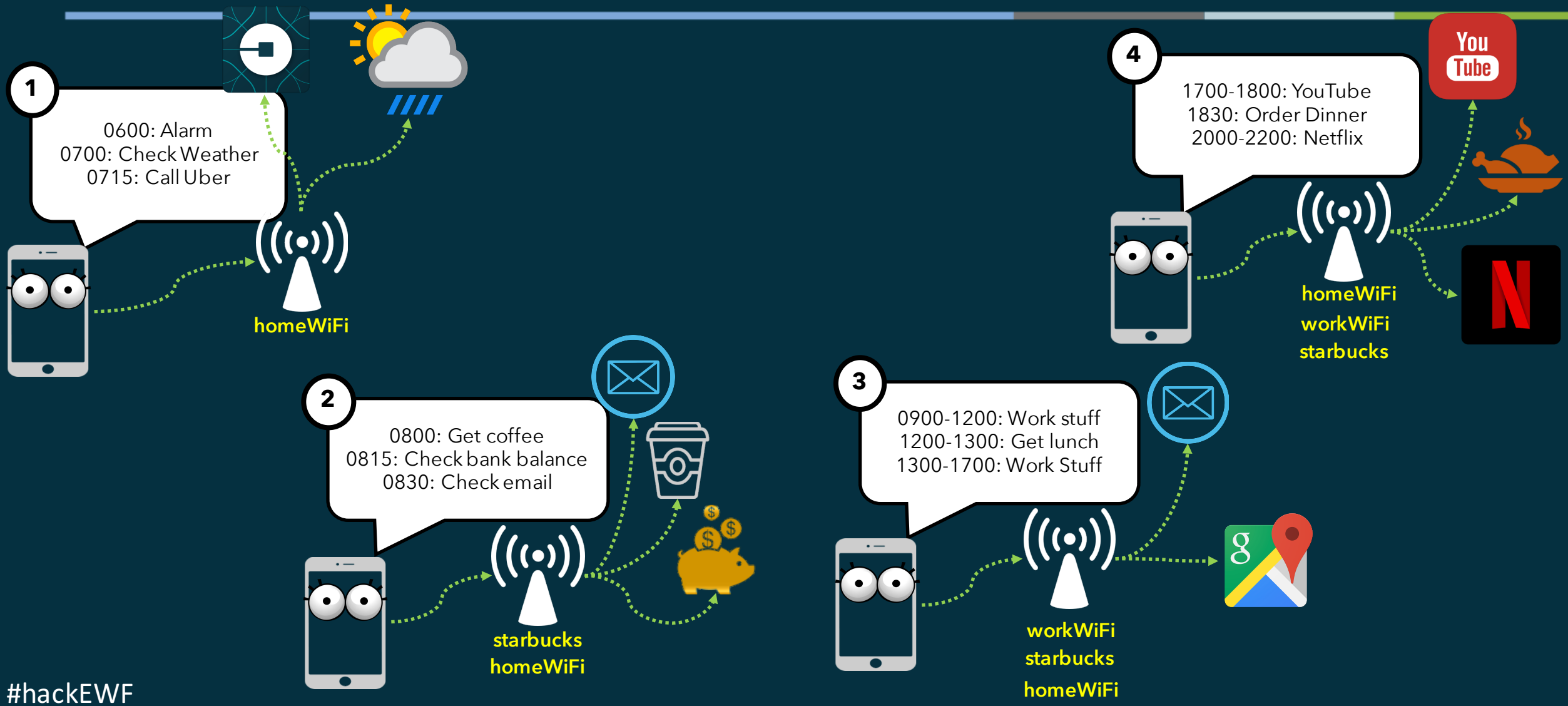


Evil AP


Open Networks

#hackEWF

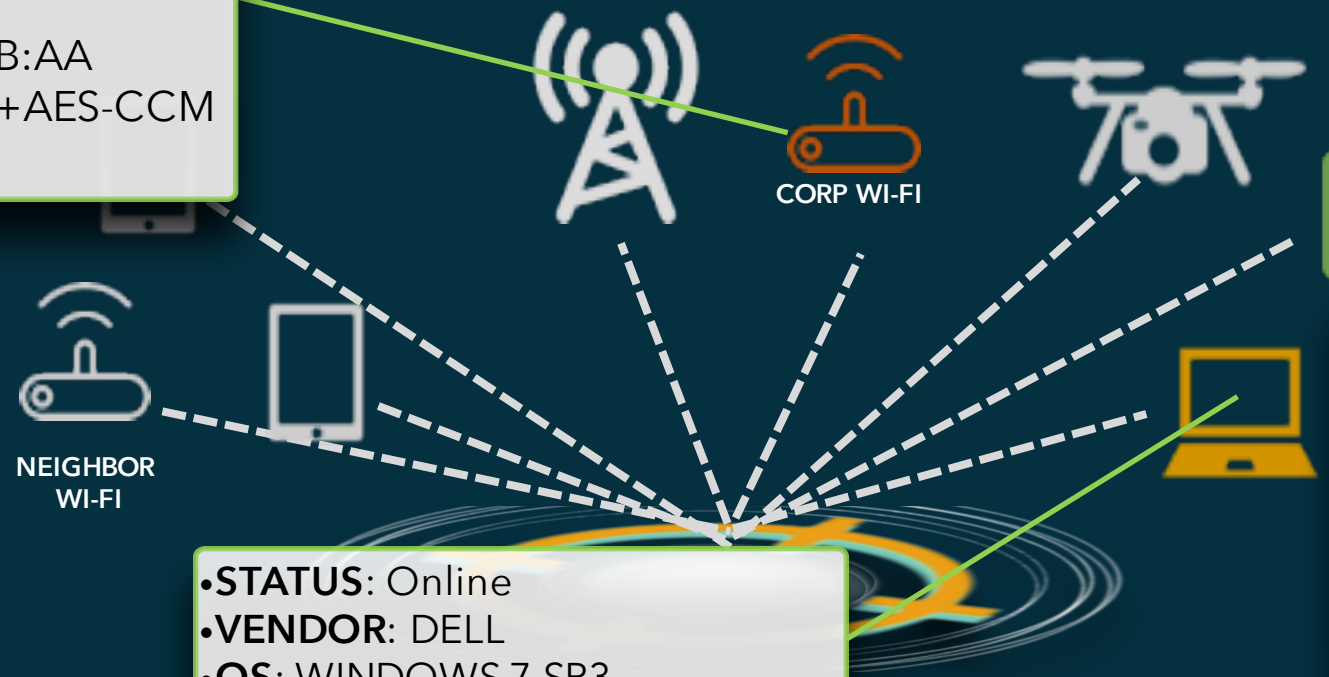
# A Day in the Life of Your Device




#hackEWF

# Our Devices Are Talking…What Are They Saying?

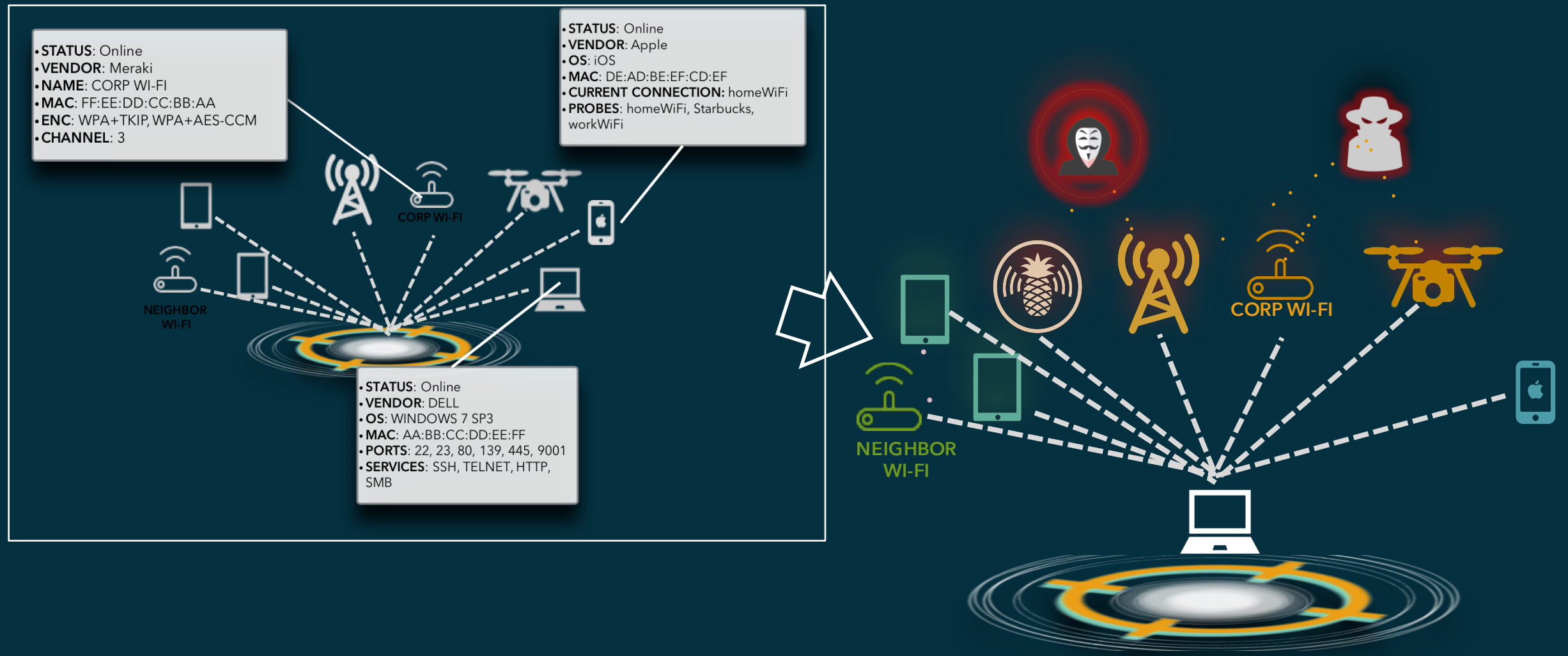
- **STATUS**: Online
- **VENDOR**: Meraki
- **NAME**: CORP WI-FI
- **MAC**: FF:EE:DD:CC:BB:AA
- **ENC**: WPA+TKIP, WPA+AES-CCM
- **CHANNEL**: 3




- **STATUS**: Online
- **VENDOR**: DELL
- **OS**: WINDOWS 7 SP3
- **MAC**: AA:BB:CC:DD:EE:FF
- **PORTS**: 22, 23, 80, 139, 445, 9001
- **SERVICES**: SSH, TELNET, HTTP, SMB

- **STATUS**: Online
- **VENDOR**: Apple
- **OS**: iOS
- **MAC**: DE:AD:BE:EF:CD:EF
- **CURRENT CONNECTION:** homeWiFi
- **PROBES**: homeWiFi, Starbucks, workWiFi

# Good Things Talk to Bad Things




#hackEWF

# Doesn't HTTPS/VPN/TLS Save Me?

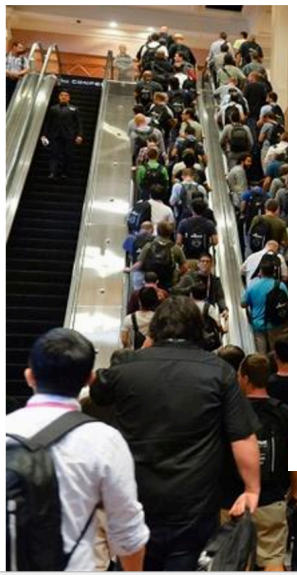
Home / Security Watch / First Look at a Wi-Fi Attack Happening at Black Hat Right Now

## First Look at a Wi-Fi Attack Happening at Black Hat Right Now

BY MAX EDDY AUGUST 4, 2016 10:49AM EST 10 COMMENTS

*How bad could it be?*

0 SHARES





//MOST POPULAR ARTICLES


Crypto Wars: Why the Fight to Encrypt Rages

18 Slick Xbox

of All Time

The Eerie World of Abandoned Arcade Games

**ReadandShare** · 2 months ago

@Max Eddy, who wrote, "if someone [illegible] of the access point, they can decrypt your traffic, monitor it, and then pass it along its intended destination with you being none the wiser."

As an individual user, I don't care that much if people snooped my browsing CNN and PCMag. But when emailing (via Android Chrome browser using HTTPS) or banking (bank app also encrypted) -- my understanding is snoopers will just get a bunch of gibberish. You say they can decrypt. But if indeed they can decrypt HTTPS traffic - don't we have a far, far bigger problem worldwide than just an insecure Wifi?

NOPE

# Yeah, but NAC Tho….

1. Client-side attacks start off-network at the endpoint (i.e. *the device*) against known-good devices can circumvent basic controls
   - Anti-virus won't catch it
   - Policy Orchestration won't [illegible]
   - SIEM may think it's weird if you've tuned it correctly
   - Firewalls will look at it as normal, outbound traffic
2. NAC deployment best practice: install in "monitor mode" first– most people *never* move from monitor to enforcement

NOPE

Alta Associates'
Executive
Women's Forum
*Information Security, Risk Management & Privacy*

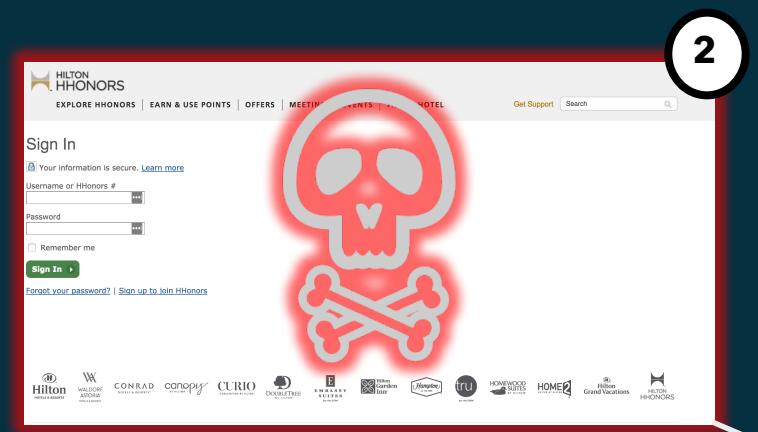
# Prove It!

This is a targeted attack, done with the permission and discretion of EWF. The specific exploits and tools presented here were acquired, purchased & configured for demonstration purposes only against *a specific, designated device*. No other devices were targeted as part of this exercise, so if your laptop stops working it wasn't me, okay? Just turn off your Wi-Fi to be on the safe side.

You ***should not*** attempt to do this without expressed, written permission of the granting authority .

# DISCLAIMER

# Constructing the Attack




2


4

1

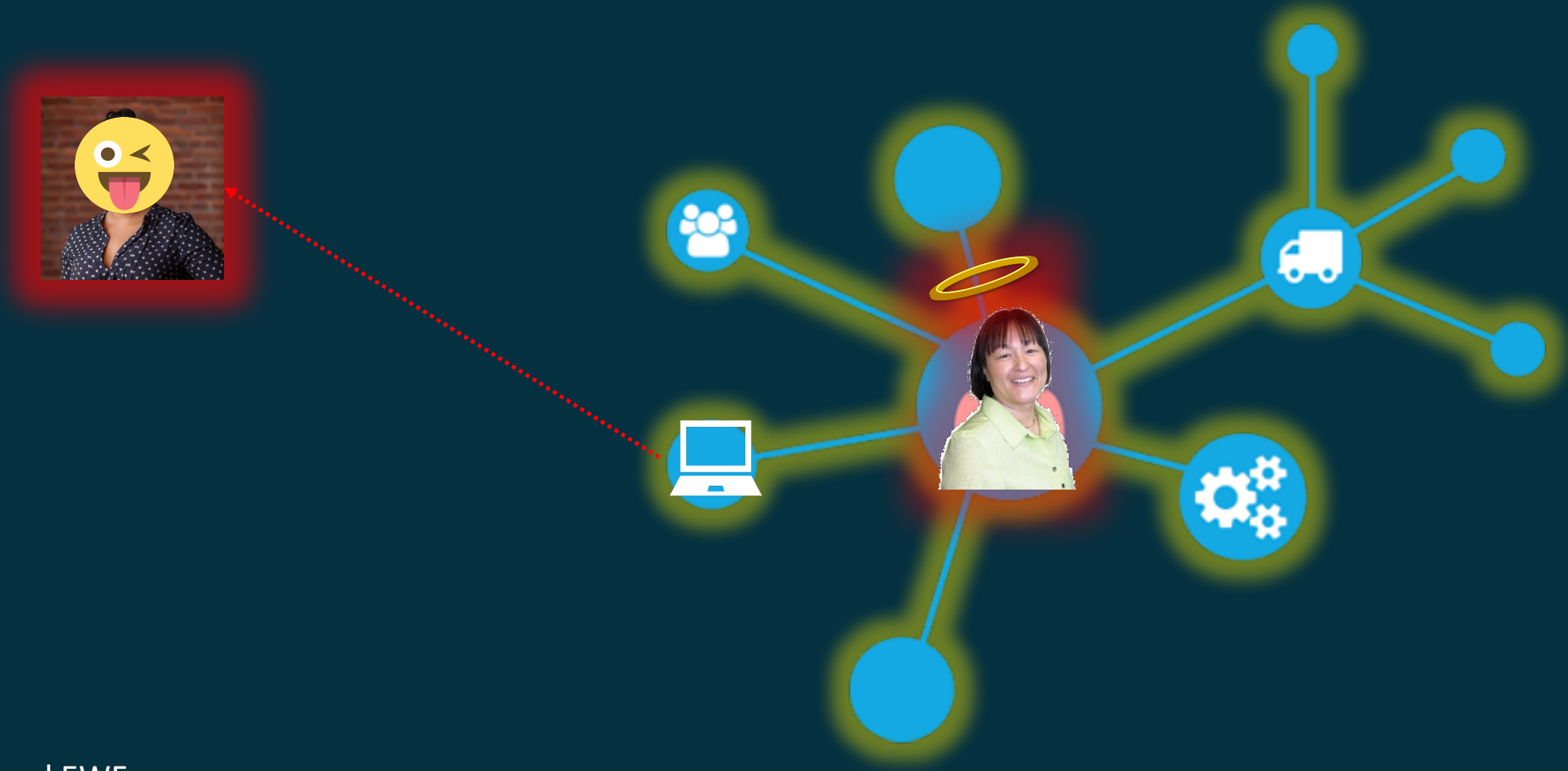
3 Credential Sniffing


Objectives

1. Snag Credentials
2. Drop backdoor on laptop
3. Gain access to privileged networks & data

#hackEWF

# Impact to the Corporation



# Tools of the Demo

- Hak5 Pineapple Nano - ~$100 USD
- Kali Linux (Rolling) & Associated Tools
- Social Engineering Toolkit
- Metasploit
- Windows 10 Virtual Machine (for testing)
- Various cables, chords
- Lots of candy to keep me motivated

- For the purposes of this demonstration, we were intentionally heavy handed and obvious with the tools, payloads and delivery mechanism to show each part of the attack.

- In reality there are ***many*** sophisticated & stealthy ways to evade detection & quarantine.
  - Check out Mass Mailer, Spearphishing attacks from SET (Dave Kennedy, Trusted Sec)
  - VEIL Framework (by @harmj0y)

# DISCLAIMER

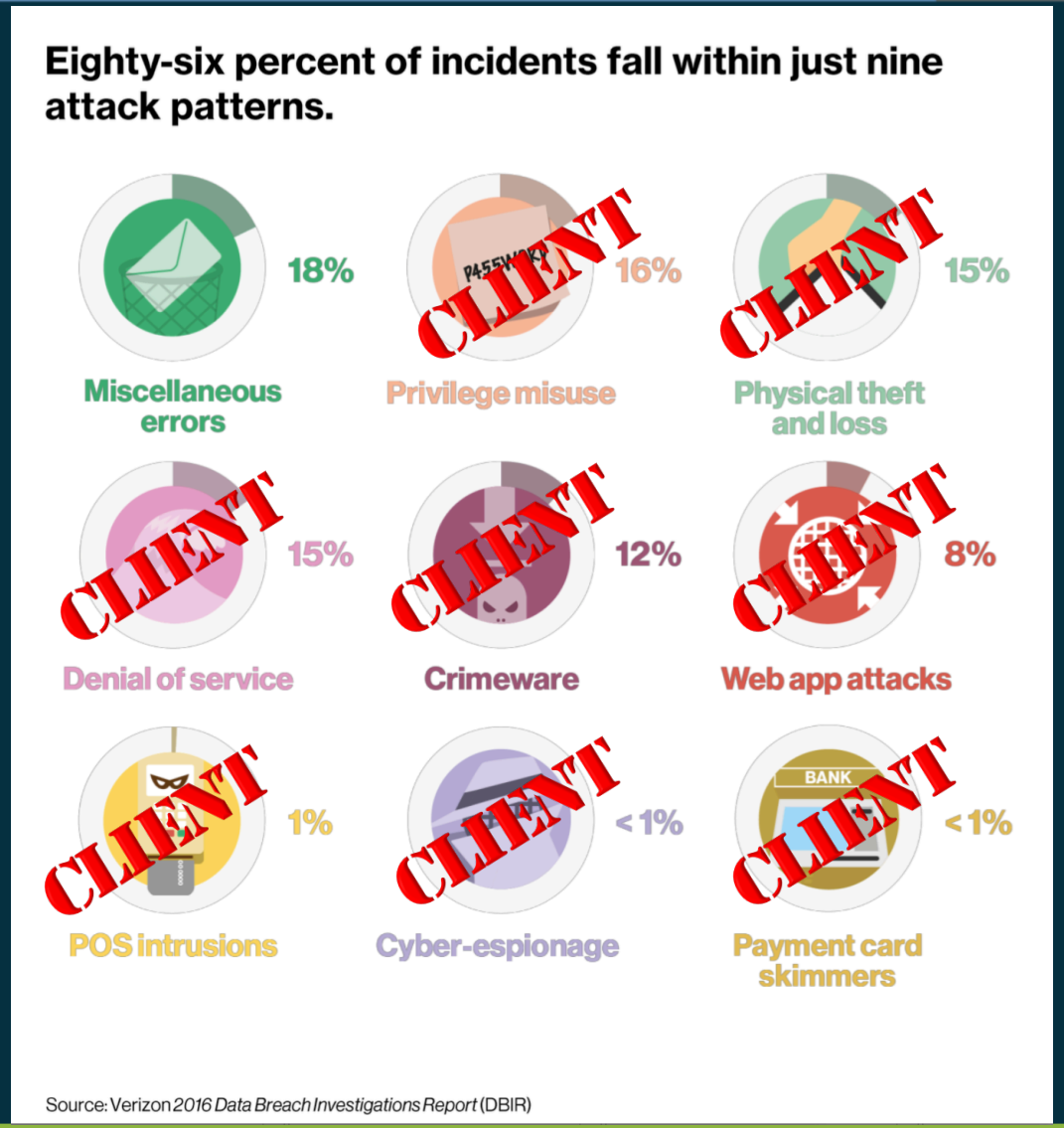
# Was the Attack Successful?

Pulse

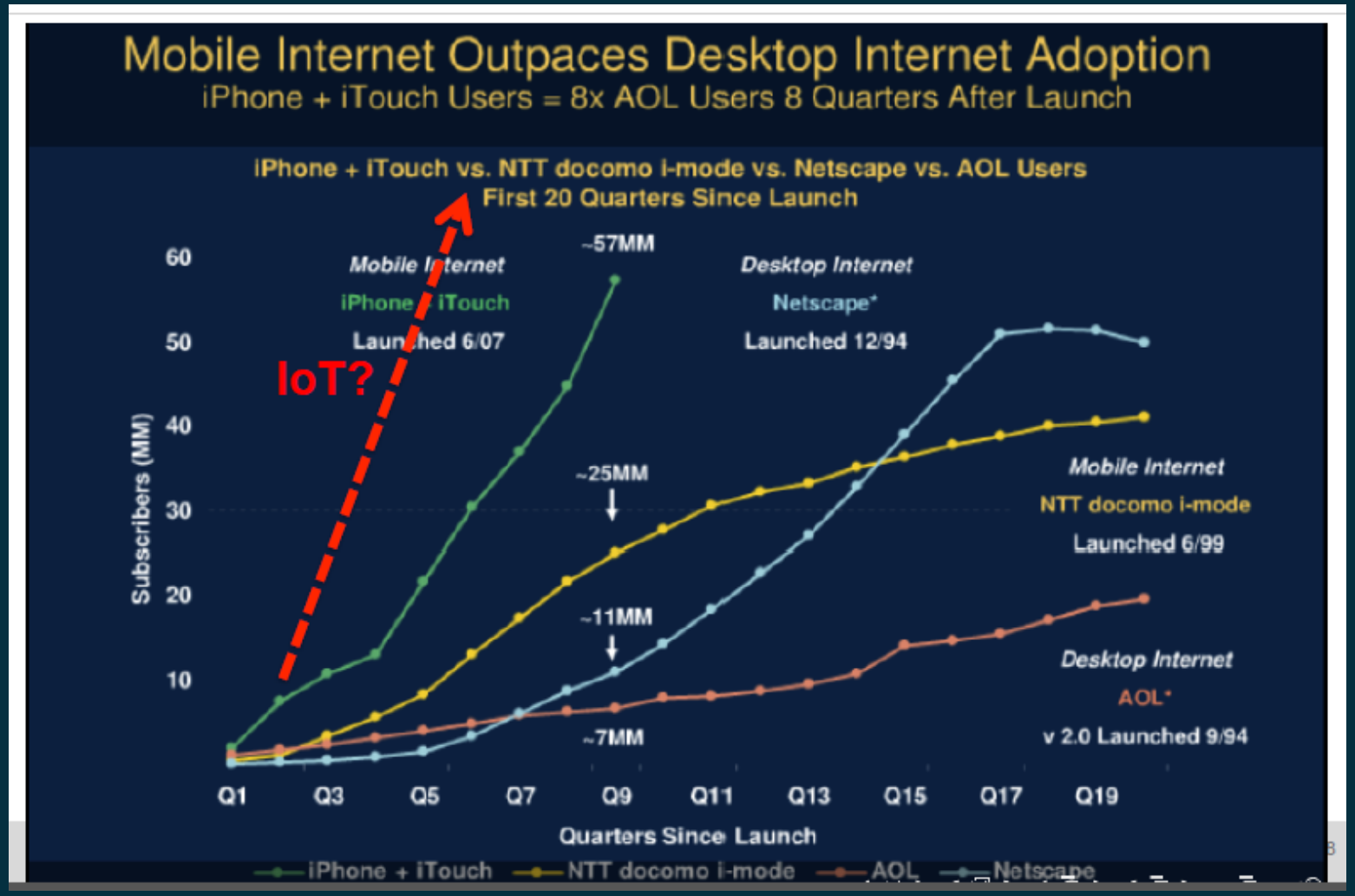
Alta Associates'
Executive
Women's Forum
*Information Security, Risk Management & Privacy*

# *The Message*

# Devices at the *Center* of Modern Attacks



# What Does History Tell Us?




Source: Grey Lock Partners

# Things *You* Can Do

- Don’t connect to (or trust) Free/Open Wi-Fi
  - If you must, refrain from sensitive/privileged transactions
- Use a password manager
- Yes, VPN, MDM, Sandboxing, Anti-Virus
  - They should talk to *each other* to offer the best protection
- Remove probes from your devices

# Takeaways

1. A proactive risk mitigation strategy starts with *understanding* what's out there first
   a. Build threat models from *real* data
   b. Adjust fire once you know what's out there

2. From Threat Models → **P**olicy
   a. Flexible
   b. Tied to organizational goals & objectives

3. Effective strategy will include a *combination* of technologies
   a. Application
   b. Device
   c. Network

#hackEWF

@ysmithND | @pwnieexpress

linkedin.com/in/yolonda-smith

yolonda@pwnieexpress.com

# Questions?

#hackEWF


Alta Associates'
Executive
Women's Forum
*Information Security, Risk Management & Privacy*

# Thank You!

Yolonda N. Smith
Director of Product Management
Pwnie Express

Alta Associates'
Executive
Women's Forum
*Information Security, Risk Management & Privacy*

# Backup

# Deny by Default

## Where it Works

- Allows IT Ops to focus on protecting the known-good devices on the network

## Where it Fails

- Unrealistic in the world of BYOD
  - Stunts the growth & effectiveness of your organization
  - Keeps IT Ops mired in constant policy development, monitoring & modification
  - Forgets the common tenant: *the ants will always find a way*
- Doesn't cover what happens off-network
- Built on assumption that you always have a clear idea & control of what's on your network

# Secure Containers

## Where it Works

- Contains critical apps and services to a "pristine" environment
  - Allows employee/company data to co-exist on the same device
  - Gives company more granular control over proprietary data without having to maintain or sanitize the device itself

## Where it Fails

- Covers some apps, but not the device itself
- Covers some apps, but not the network
- Often relies well-known OS types, apps to be effective
  - IoT?
  - PS4?
  - Wearables?

# MDM/EMM

## Where it Works

- Devices which meet the standard are allowed to connect to the network
- Maximizes productivity while decreasing support costs (company doesn't have to pay for or manage new OS roll out)

## Where it Fails

- Potentially administrative nightmare: every OS, Device type and associated applications have to be vetted by policy
  - Just because a capability is available, doesn't mean it will be turned on or used
- Not everyone wants to have "the company" agent following them everywhere (Privacy concerns), increasing likelihood of data leakage
- Inside-out approach means that administrators don't have visibility into device behavior *once it leaves the network*