

# Cyber Security Trends

Eddie Galang  
Chief Information Security Officer  
Port of Long Beach

October 29, 2019

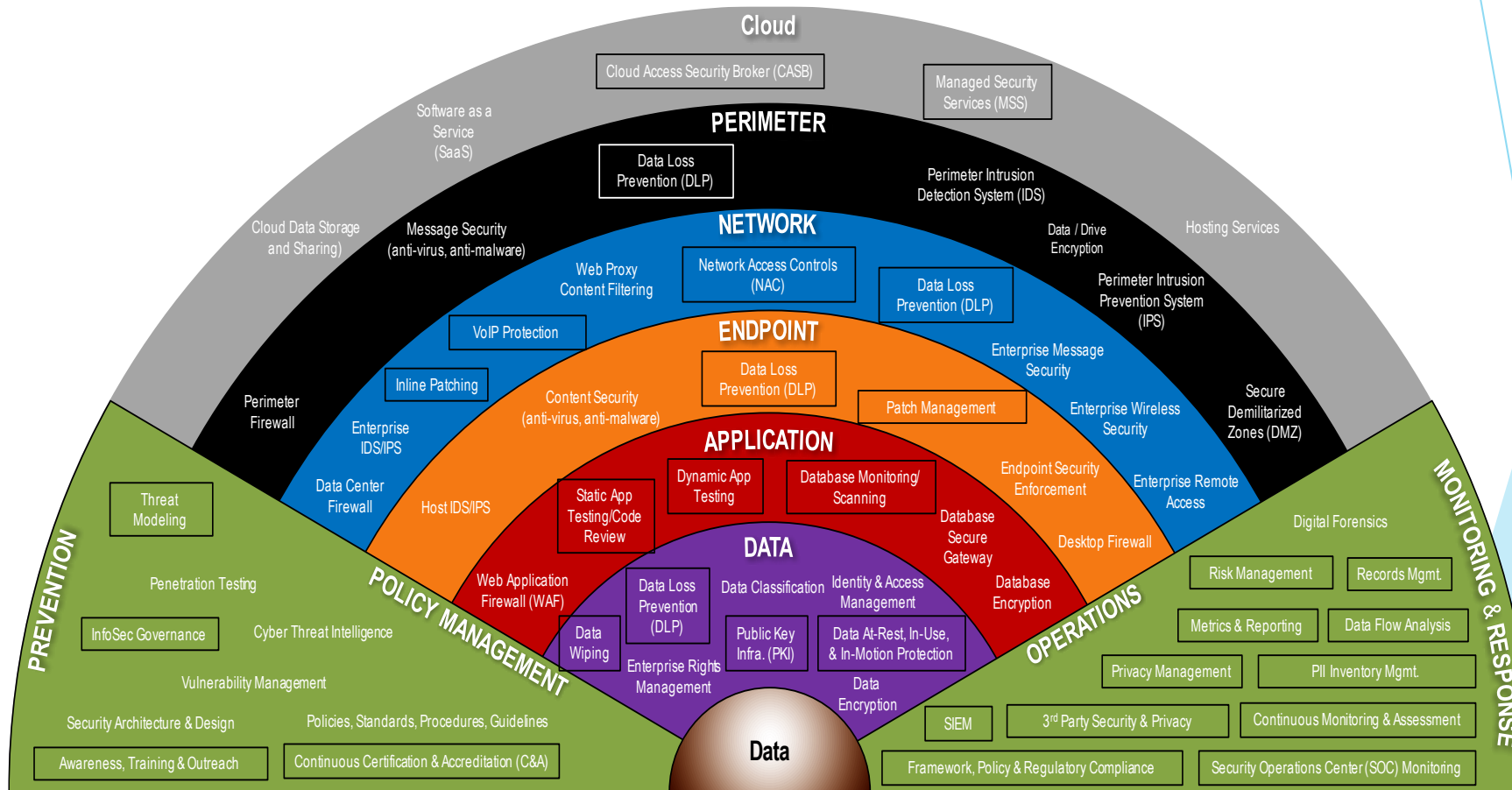


# Agenda

- Layered Defense
- Threat Landscape
- Threat Actors and Motives
- Anatomy of an Attack
- What You Are Trying to Protect
- Partnering with Law Enforcement
- Future Trends
- Micro Segmentation and Zero Trust

# Layered Defense

Layered defense refers to security systems/capabilities that use multiple components to protect operations on multiple levels, or layers against multiple threats including malware, theft, unauthorized access, insider attacks and other security considerations.



# Threat Landscape

*Far-reaching vulnerabilities, faster attacks, files held for ransom and more malicious code than ever*



## MOBILE DEVICES

- **1 in 36** mobile devices are classed as **high risk**.
- The U.S. is most affected by Mobile Ransomware at **33%**.



## WEB ATTACKS

- **1 in 10 URL's** analyzed were identified as **malicious**
- **4,800 Formjacking** compromises via websites per month



## SCAMS & SOCIAL MEDIA

- Landscape continues to **evolve**.
- **1 in 302**– Rate of Malicious email delivered.
- **48%** of Malicious email attachments are office files...up from 5% in 2017
- Small/Med sized orgs more likely to be targeted



## RANSOMWARE

- Overall activity drops 20%, but remains a challenge for organizations
- Mobile ransomware climbs to 33%









## TARGETED ATTACKS

- Overall attacks have dropped.
- **65%** used spear phishing as the primary infection vector.
  - **96%** primary motivation is intelligence gathering

# Threat Actors and Motives

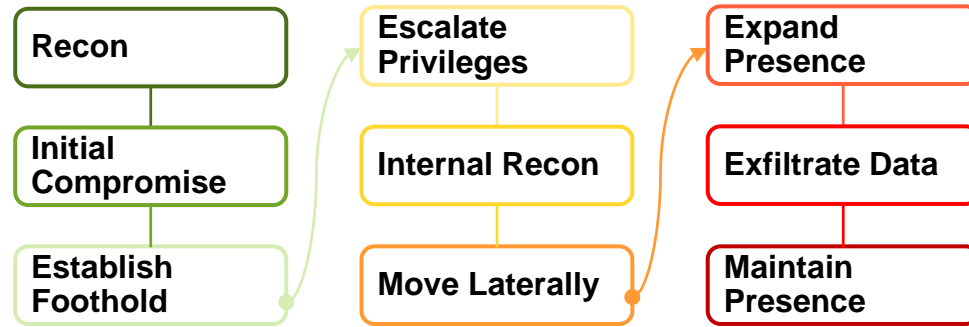
*Who would target you and why?*

THREATS

	<b>HACKTIVISM</b> <ul style="list-style-type: none"><li>• Hacktivists use computer network exploitation to advance their political or social causes.</li></ul>
	<b>CRIME</b> <ul style="list-style-type: none"><li>• Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.</li></ul>
	<b>INSIDER</b> <ul style="list-style-type: none"><li>• Trusted insiders steal proprietary information for personal, financial, and ideological reasons.</li></ul>
	<b>ESPIONAGE</b> <ul style="list-style-type: none"><li>• Nation-state actors conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.</li></ul>
	<b>TERRORISM</b> <ul style="list-style-type: none"><li>• Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.</li></ul>
	<b>WARFARE</b> <ul style="list-style-type: none"><li>• Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the even of conflict.</li></ul>



# Anatomy of an Attack



## Common Attack Vectors

- Known Vulnerabilities
- SQL Injection
- Phishing, Spear-phishing, Whaling
- Weak Authentication
- Viruses/Malware attacks
- Social engineering

## Targeted Information Types

- Corporate finances
- Internal corporate information
- Customer/Employee PII
- Proprietary technology
- IT infrastructure
- Bandwidth (DDoS)

# What You Are Trying to Protect

Intellectual Property (IP) · Proprietary Information (PI) · Personally Identifiable Information (PII)

## Identity Theft

- 7% report harm post breach<sup>1</sup>
- 0.3% suffer actual harm<sup>2</sup>
- 2<sup>nd</sup> highest complaint at the FTC<sup>3</sup>



## Driver's License<sup>4</sup>

- First / last name
- ID #
- Address, DOB

**\$100 - \$150**



## Bank Info<sup>4</sup>

- First / last name, bank, acct #
- Login credentials

*\*Based on account balance*

**\$300 - \$4200**



## Credit Card (CC)<sup>4</sup>

- First and last name
- Card #
  - Active Users: 601
  - Credit Range \$1K - \$25K

**\$1 - \$8**



## Credit Card with PIN<sup>4</sup>

- First / last name
- Card #
- PIN
- Expiration date

**\$17 - \$35**



## Social Security Card<sup>4</sup>

- First / last name
- SSN
- DOB

**\$250 - \$400**



## Health Insurance Info<sup>1</sup>

- First / last name
- Login credentials
- Plan provider
- ID #

**\$250**



## Identity Profile<sup>5</sup>

- Name, SSN, DOB
- Address, phone #
- Email credentials
- Credit card # or bank info

**\$1200 - \$1300**

## Other Online Accts:

- Gift Cards: 15 - 50% value
- Cloud service: \$5 - \$10
- Retail Shopping: \$.50 - \$99
- Online Payment: \$1 - \$100

Sources: 1. AllClear ID  
2. ID Experts, LifeLock  
3. FTC, Consumer Sentinel Network Data Book  
4. Underground Hacker Markets by Dell SecureWorks  
5. "What your information is worth on the black market" by Bankrate



# Partnering with Law Enforcement

*Domestically, the FBI has Field Offices throughout the U.S., with Special Agents dedicated to work Cyber investigations*

*Internationally, the FBI has Special Agents, called Legal Attachés, who work in U.S. Embassies, around the globe. They work with the local countries law enforcement agencies*



## *Engaging Law Enforcement*

### **Call the FBI as soon as possible**

- Delays can result in loss of digital evidence
- Determine how your internal investigation and the criminal investigation will work together

### **What does the FBI do?**

- Focuses on criminal prosecution
- Forensically collects and analyzes evidence
- Can, with consent, monitor victim's network for activity related to the attack
- Testifies in court

### **Federal Prosecutor**

- Federal prosecutors can also speak to victim's legal team

# Future Trends

*Expected in 2020 and Beyond*

## 1. Current and Future Challenges

- Begin shifting from a compliance-based approach to a security-based approach for managing information security risk
- Lack of preparedness will continue allowing attackers to hide undetected

## 2. Endpoint Protection

- Resurgence of email as favored attack channel
- Increase in Spam, Malware, & Phishing tempting users to take action
- Customer & Financial data are highest priority

## 3. Web Attacks, Toolkits & Exploiting Vulnerabilities

- Increase in web attacks (e.g., Tech, Business)
- Browser vulnerabilities to increase (e.g., Chrome, Firefox)
- New cryptojacking exploit toolkits to surface

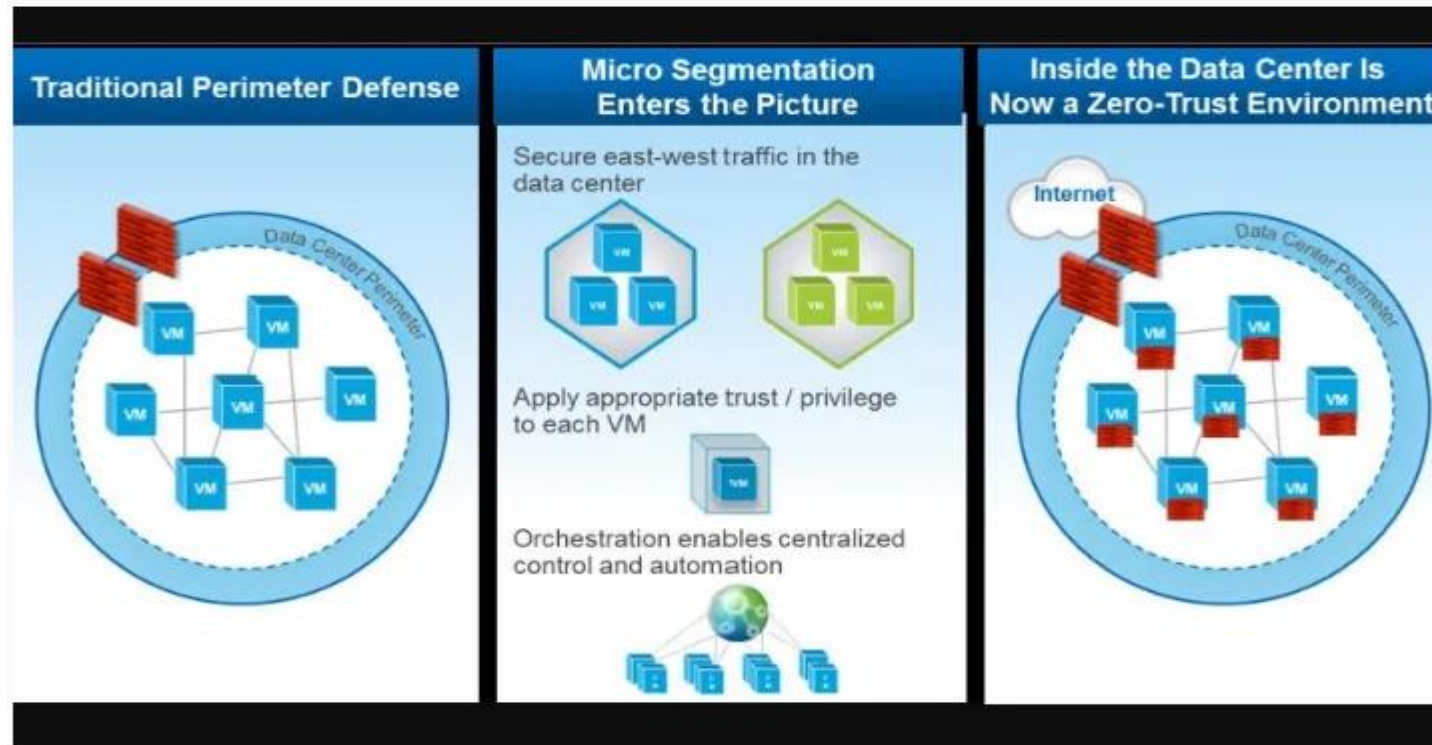
## 4. Internet of Things (IoT)

- IoT devices (Routers, Cameras) will continue to be favored (\$26B devices in 2020)
- 2x increase in attacks against IoT devices (5,200+ per month)
- Cloud attacks will increase until companies protect these assets
- Growing reliance on cloud services present security blind spots



# Micro Segmentation and Zero Trust

*Security technique that enables fine-grained security policies to be assigned to data center applications, down to the workload level and enables security models to be deployed deep inside a data center, using a virtualized, software-only approach.*



Why consider the Zero Trust model?

- Perimeter security approach is not effective (many data breaches happened because hackers, once they got past the corporate firewalls, were able to move through internal systems without much resistance).
- Perimeter itself is no longer clearly defined, because applications and data stores are on-premises and in the cloud, with users accessing them from multiple devices and locations.