The Cyber Threat Landscape

Intrusion Investigations and The InfoSec Playbook

M. K. Palmore, CISSP
Information Security Executive
ASAC - FBI San Francisco

Global Threat Landscape

$4 mil

Average Cost of Breach

81%

# of Breaches Using Stolen Credentials or Weak Passwords

Over 2K

# of Breaches 2016

51%

Breaches executed by Organized Crime Groups

“No locale, industry or organization is bulletproof when it comes to the compromise of data.” - Verizon 2016 Data Breach Report

Global Threat - Intrusion Investigations

Indictment of PLA Officers

Game Over Zeus

Yahoo Breach and Indictments

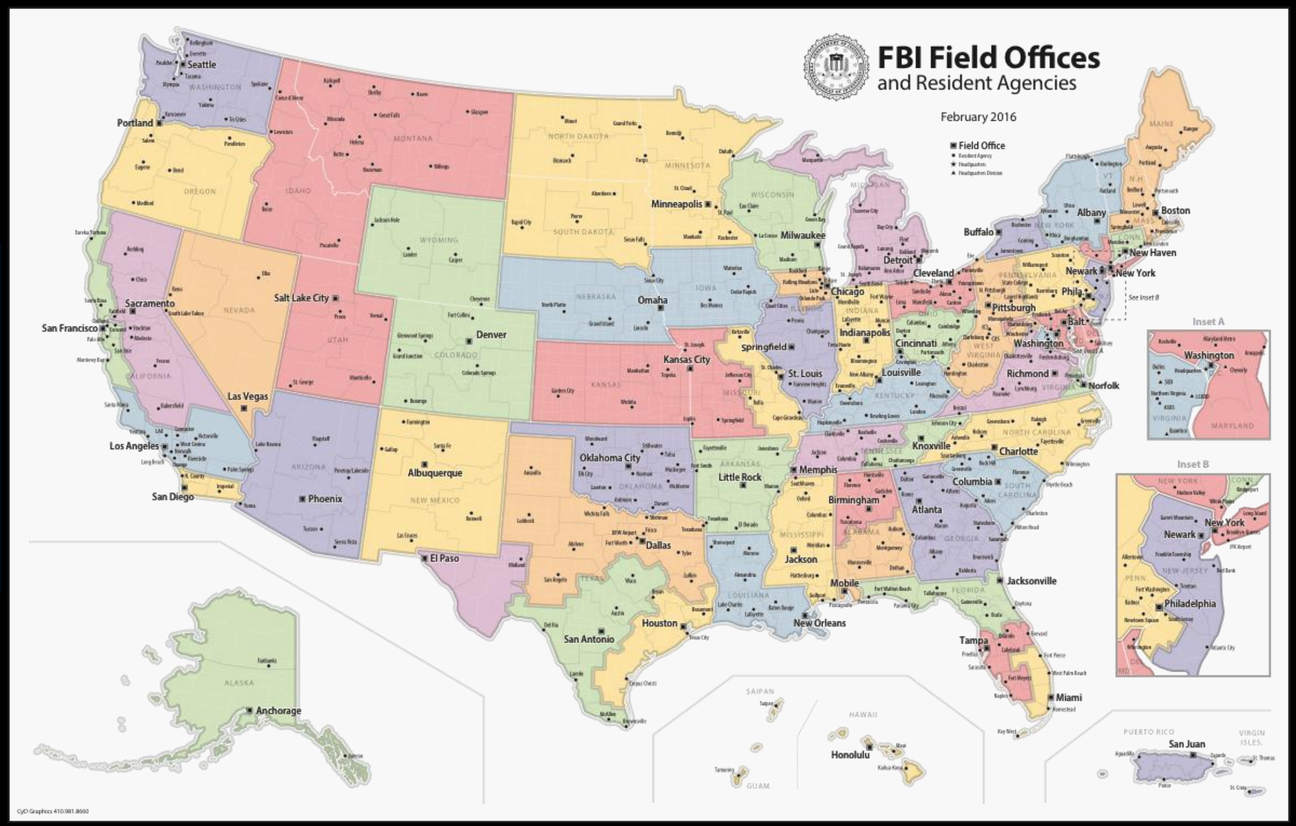
	National Security	Criminal (Financially Motivated)	Hacktivism	Insider Threat
Motivation	Strategic Advantage (Geo-Political)	Money	Social - Reputational Damage	Business Intelligence Money Revenge
Probability	Medium	High	Low	Medium
Impact	High	High	Medium	High

Global Threat - Advanced Persistent Threat

Closer Examination

- **Scope**
- **Complexity of Threat**
- **High-Impact v. Medium Likelihood**
- **Extended Time to Discovery (TTD) - 180 days**
- **Overlap with Criminal Enterprise to achieve repudiation**

More than 62 Cities around globe

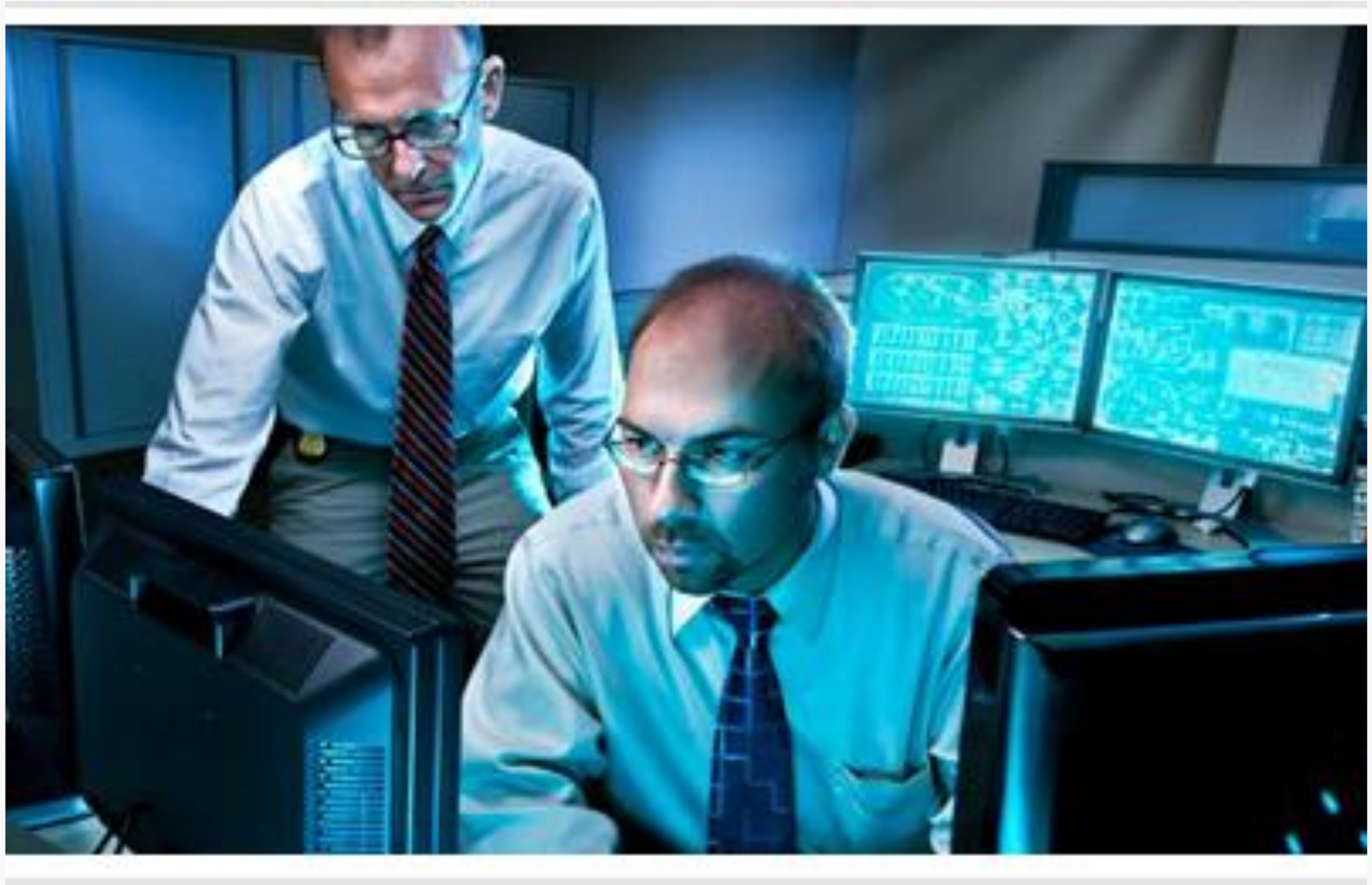


56 Field Offices/CTFs

Cyber Threats and Investigations

Investigations Playbook

- Prefer to develop relationships pre-breach
- Contact LE early during an incident
- Onsite evaluation of incident
- Confidentiality and dealing w/victims
- Global Reach
- Post Mortem Accuracy (complete picture)



Cyber Security - Common Mitigations

Mitigation Strategies

STRONG PASSWORD POLICY

TWO-FACTOR AUTH

PATCHING

AUDIT/LOG MANAGEMENT

VULNERABILITY ASSESSMENTS

INCIDENT/RESPONSE PLANNING

ACCESS MANAGEMENT

BCP/DRP

INFOSEC PROGRAM MANAGEMENT

Contact

M. K. PALMORE

INFORMATION SECURITY EXECUTIVE

ASAC - FBI

CALL

408 209 9339

E-MAIL

mkpalmore@fbi.gov

M. K. Palmore

@mk_palmore