

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

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

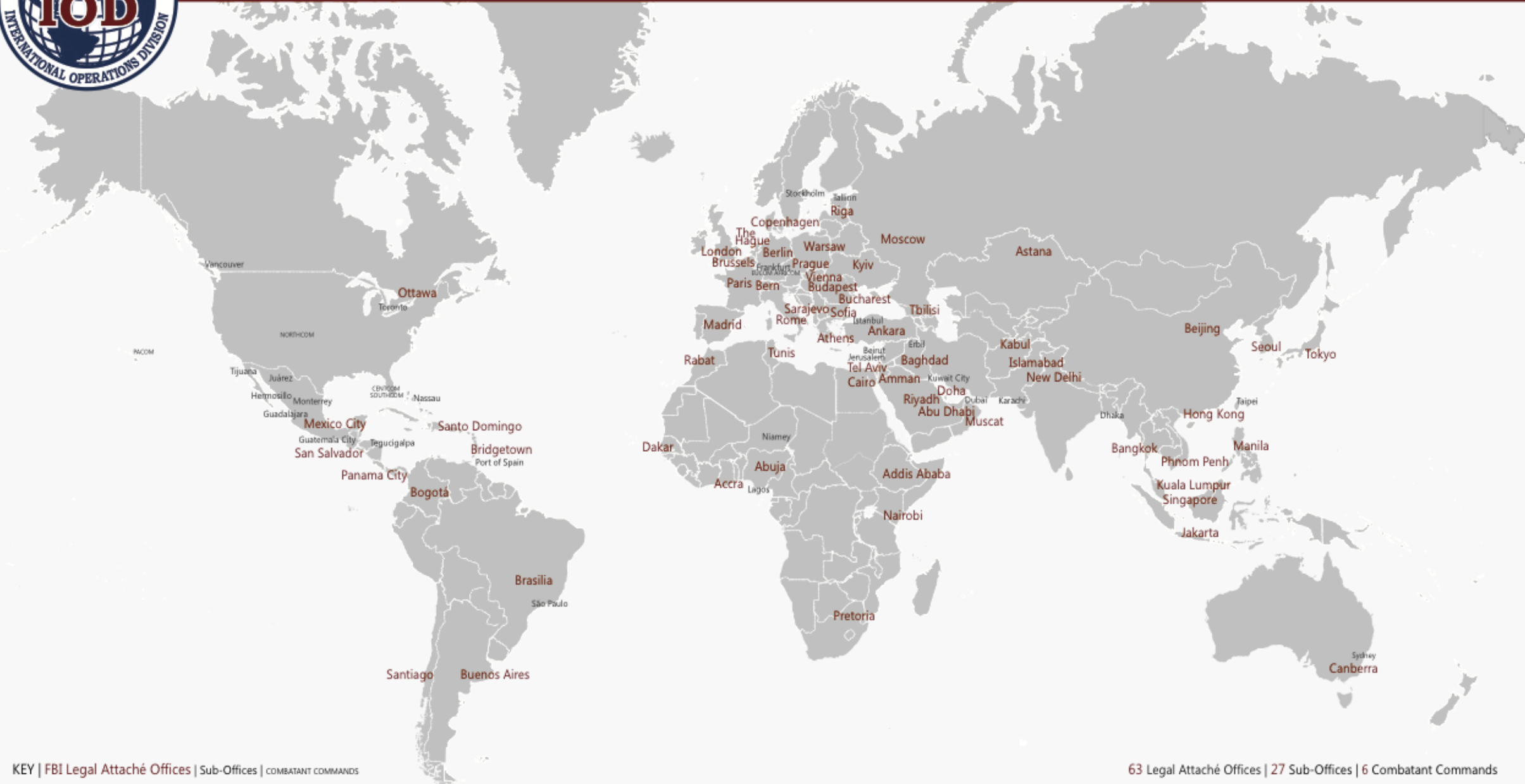
- **Scope**
- **Complexity of Threat**
- **High-Impact v. Medium Likelihood**
- **Extended Time to Discovery (TTD) - 180 days**
- **Overlap with Criminal Enterprise to achieve repudiation**



More than 62 Cities around globe



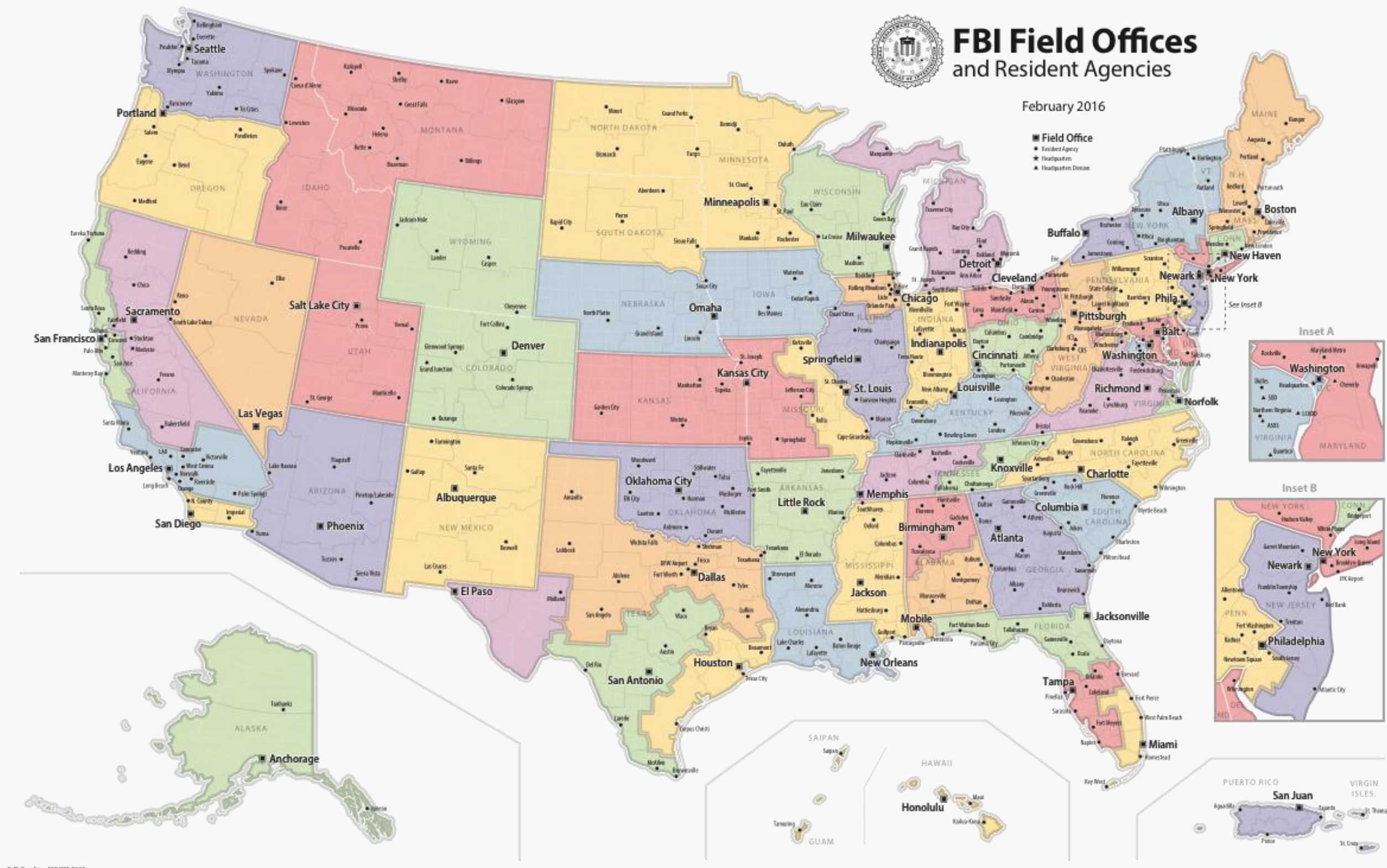
FBI INTERNATIONAL PRESENCE International Operations Division



KEY | FBI Legal Attaché Offices | Sub-Offices | COMBATANT COMMANDS

63 Legal Attaché Offices | 27 Sub-Offices | 6 Combatant Commands

AFRICA | Abuja, Nigeria; in-country suboffice Lagos | Accra, Ghana | Addis Ababa, Ethiopia | AFRICOM | Dakar, Senegal | Nairobi, Kenya | Pretoria, South Africa | Rabat, Morocco | Tunis, Tunisia; suboffice Niamey, Niger | Bogotá, Colombia | Brasilia, Brazil; in-country suboffice São Paulo | Bridgetown, Barbados; suboffices Nassau, Bahamas; Port of Spain, Trinidad and Tobago | Buenos Aires, Argentina | Mexico City, Mexico; in-country suboffices Guadalajara, Hermosillo, Juárez, Monterrey, Tijuana | NORTHCOM | Ottawa, Canada; in-country suboffices Toronto, Vancouver | Panama City, Panama | San Salvador, El Salvador; suboffices Guatemala City, Guatemala; Tegucigalpa, Honduras | Santiago, Chile | Santo Domingo, Dominican Republic | SOUTHCOM | ASIA | Bangkok, Thailand | Beijing, China | Canberra, Australia; in-country suboffice Sydney | Hong Kong SAR, China; suboffice Taipei, Taiwan | Jakarta, Indonesia | Kuala Lumpur, Malaysia | Manila, Philippines | New Delhi, India; suboffice Dhaka, Bangladesh | PACOM | Phnom Penh, Cambodia | Seoul, South Korea | Singapore, Singapore | Tokyo, Japan | EURASIA | Ankara, Turkey; in-country suboffice Istanbul | Astana, Kazakhstan | Athens, Greece | Bucharest, Romania | Budapest, Hungary | Kyiv, Ukraine | Moscow, Russia | Prague, Czech Republic | Riga, Latvia; suboffice Tallinn, Estonia | Sarajevo, Bosnia-Herzegovina | Sofia, Bulgaria | Tbilisi, Georgia | Warsaw, Poland | EUROPE | Berlin, Germany; in-country suboffice Frankfurt | Bern, Switzerland | Brussels, Belgium | Copenhagen, Denmark; suboffice Stockholm, Sweden | EUCOM | London, England | Madrid, Spain | Paris, France | Rome, Italy | The Hague, Netherlands | Vienna, Austria | ICMC | Abu Dhabi, UAE; in-country suboffice Dubai | Amman, Jordan; suboffice Beirut, Lebanon | Baghdad, Iraq; in-country suboffice Erbil | Cairo, Egypt | CENTCOM | Doha, Qatar | Islamabad, Pakistan; in-country suboffice Karachi | Kabul, Afghanistan | Muscat, Oman | Riyadh, Saudi Arabia; suboffice Kuwait City, Kuwait | Tel Aviv, Israel; in-country suboffice Jerusalem



56 Field Offices/CTAs

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**



**AUDIT/LOG
MANAGEMENT**



**ACCESS
MANAGEMENT**



**TWO-FACTOR
AUTH**



**VULNERABILITY
ASSESSMENTS**



BCP/DRP



PATCHING



**INCIDENT/RESPON
SE PLANNING**



**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

