DATA & TECHNOLOGY

Mid-Atlantic CIO Forum

Cyber Incidents: When to Involve Law Enforcement

MARCH 2023

Agenda

Your Presenters

ankura

Introductions

TED THEISEN

Senior Managing Director

Ted.Theisen@ankura.com

571-328-1531

- 20+ years experience in information technology
- Former FBI Special Agent – Cyber Crime
- Former Branch Chief of Cyber Integrity at the White House

CHRISTOPHER “TODD” DOSS

Senior Managing Director,

Todd.Doss@ankura.com

540-935-9036

- 3,000 Clients Assisted Through Breach Investigations
- Over 35 years of Local, State and Federal Law Enforcement Experience
- Former FBI Special Agent – Assistant Director
- Served 8 years as the Director of the FBI Crime Laboratory
- Former Director of the FBI Special Technologies and Applications Office/Counterterrorism Division

About Ankura

About Us – By the Numbers

1,800+
Full-Time Employees

600+
Consultants with Advanced Degrees or Industry Certifications

~64%
of Projects Leverage Expertise from Multiple Business Groups

~34%
of Projects Include Data & Analytics

WHO WE ARE

- **Ankura is a global firm of experts and advisors** uniquely built to tackle each challenge or need, by effectively combining the right expertise into solutions, services, and results.
- **We are a trusted advisor** for companies, governments, law firms, and institutions around the world.
- Ankura leverages **highly specialized technical skills** and **industry expertise** to solve complex and mission critical challenges for clients without the siloes and boundaries normally found in consulting firms.
- Our **collaborative culture** brings together industry leading experts and technology-enabled solutions to **solve highly complex and high-stakes issues for blue-chip clients.**

OUR GLOBAL REACH

35+ locations with projects in 115+ countries. 44 languages spoken.

Ann Arbor • Atlanta • Baltimore • Beijing • Boston • Brussels • Chicago • Dallas • Delhi • Dubai • Fairfield
Frankfurt am Main • Gurugram • Hong Kong • Houston • Irvine • London • Los Angeles • Melbourne
Miami • Mumbai • Nashville • New York • Orlando • Perth • Philadelphia • Phoenix • Riyadh
San Francisco • San Juan • Seattle • Shanghai • Singapore • Sydney • Tampa • Toronto • Vancouver
Washington, DC

Ankura Data & Technology Solutions

PROACTIVE ADVISORY

Managed Data Protection Services

THREAT DETECTION AND RESPONSE

- Continuous threat-hunting
- Real-time incident response
- Malicious activity detection
- Ongoing testing of security controls
- Targeted attack simulations

THIRD PARTY RISK MANAGEMENT

- Design, deployment, management of risk assessment
- Remediation activities

SECURITY ANALYTICS AND DATA MINING

- On-demand data mining services
- Identification of sensitive data exposure/data breaches
- Advanced log analysis
- Complex data mapping
- Data loss prevention program management

Technology, Privacy, and Cyber Risk Advisory

CYBER RISK ADVISORY

- IT and cyber strategy & governance
- Cyber assessments and compliance
- Cyber resiliency and planning
- Operational cyber functions

DATA PRIVACY ADVISORY

- Data privacy assessment and readiness programs
- Data inventory and mapping
- Development of policies and procedures
- Fractional privacy manager services
- Technology implementation

TECHNICAL SOLUTIONS

- Vulnerability and penetration testing
- Solution specific security assessments
- Security Architecture
- Security Solution Implementation
- Cloud Security
- Social Engineering Campaigns

REACTIVE, EVENT DRIVEN SCENARIOS

Data Analytics, Advisory and eDiscovery

DATA ANALYTICS AND DATA STRATEGY

- Interpretation of structured information
- Identification of trends and patterns in data
- Application to fraud, money-laundering, and other investigations

DATA COLLECTION AND DIGITAL FORENSICS

- Data captures
- Analyses of devices, servers, information systems

eDiscovery PROJECT MANAGEMENT AND HOSTING

- Utilization of advanced technology
- Data hosting and management for litigation, regulatory requests
- Machine learning technology to prioritize data

Response Intelligence and Investigations

INCIDENT RESPONSE

- Evaluation and mitigation of security incidents
- Crisis handling and response
- Leverage of endpoint detection, user behavior, threat analytics

INVESTIGATIONS

- Support of criminal/civil litigation efforts
- Assistance with regulatory proceedings
- Confidential internal investigations
- Legally defensible outcomes

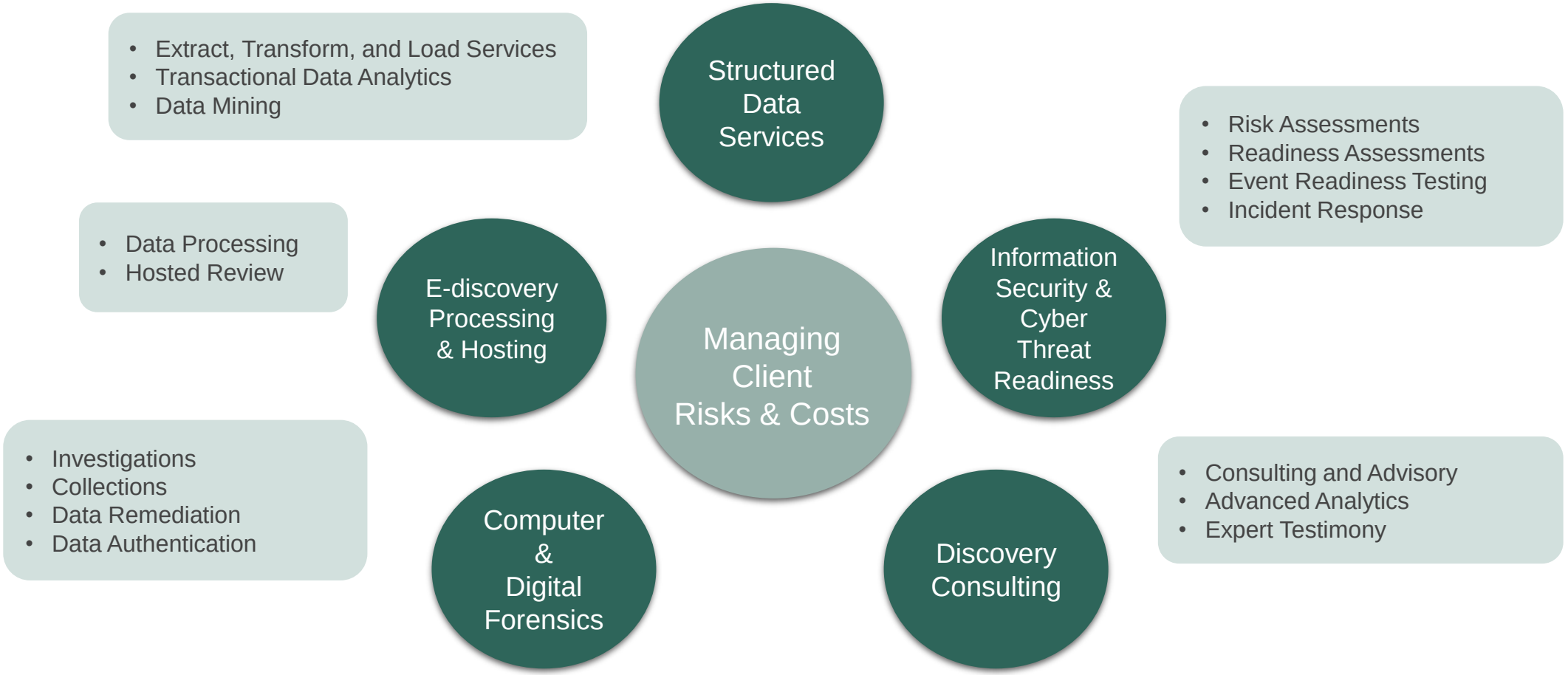
THREAT INTELLIGENCE

- Multi-sourced technical collections
- Dark web data
- Context and efficiency for investigations

EXPERT WITNESS

- Digital media forensic experts
- Cybersecurity practitioners

Ankura Data & Technology Group

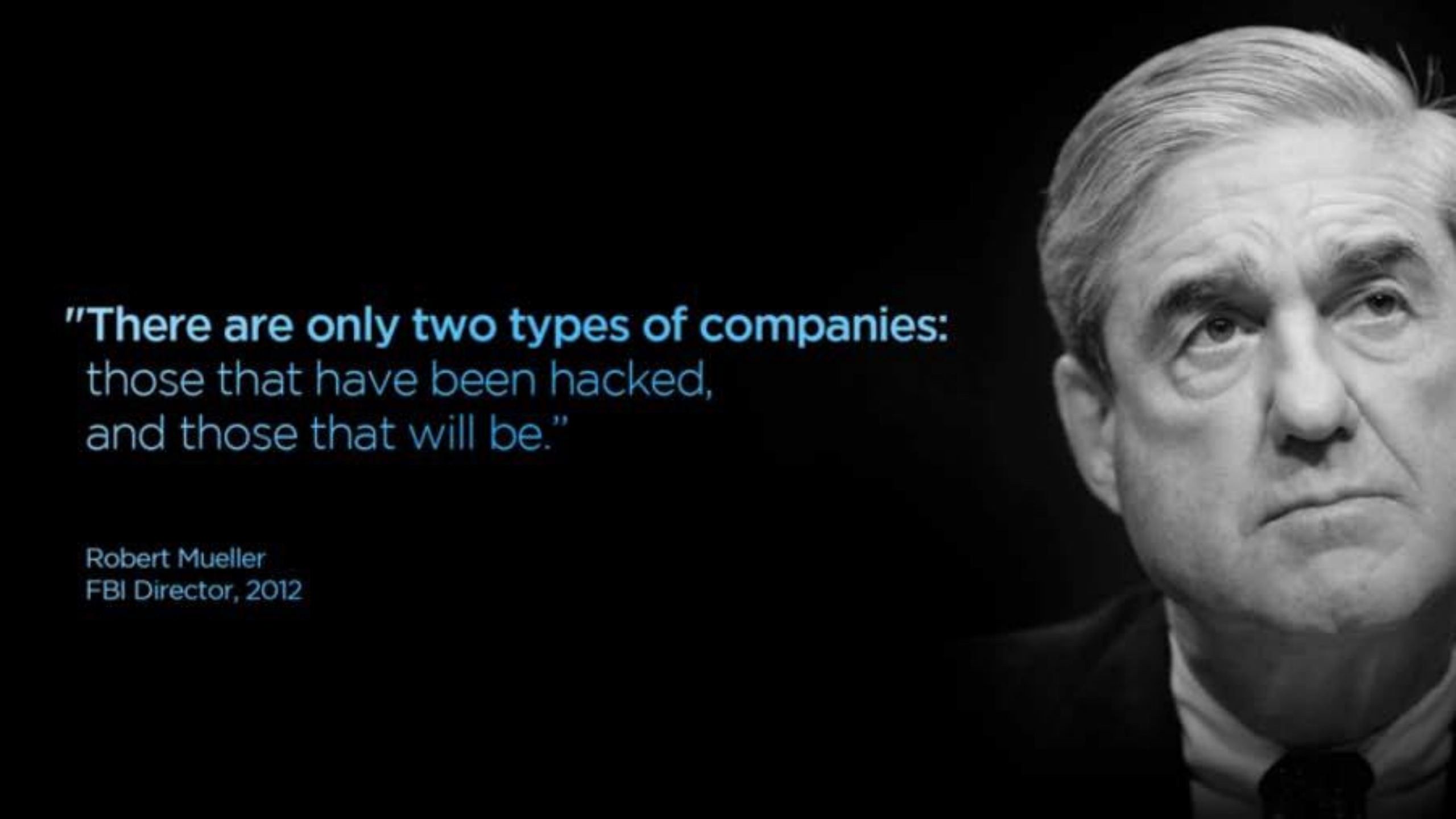


General Overview: Incident Response

ankura

"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012



Incident Response Support

Based on experience from **1000's of investigations** over the last four years, Ankura is efficient and effective in supporting clients during their incident response lifecycle using a combination of technology and well-versed playbooks to help clients rapidly contain and investigate security incidents.

Detection and Analysis

- Effective detection is key to ensuring all aspects of a breach have been identified, avoiding the risk of any compromise remaining, which might allow an attacker to regain access.
- Forensic analysis of compromised systems informs detection and allows you to make informed decisions about what actions a malicious actor has taken, and what steps need to be taken to recover affected systems.

Containment, Eradication and Recovery

- As compromised systems are detected, it's important to contain them, either by shutting them down completely, or making sure they cannot access the internet or the rest of the network.
- Once you know which systems are affected, and how, you can start to clean or replace affected systems.

Post-Incident Activities

- As you restore systems to operation it is vital that this is monitored and controlled, and that any data or systems restored from backups are subject to extra scrutiny.
- Once you have recovered from the incident, it's time to review the root causes, and use the lessons learned to come up with a plan for how to avoid the same thing happening again.

Preparation

Possibly the most important!

- IR Plans & Procedures
- Tabletop Exercises
- Preparation of System Diagrams and Data Mapping
- Identification of the Location and Pertinent Data
- Understand Existing Corporate Standards
- 3rd Party Relationships

"In preparing for battle I have always found that plans are useless, but planning is indispensable"

--General Dwight D. Eisenhower

Contacting Law Enforcement During a Cyber Incident

ankura

First, Understand Law Enforcement Motives

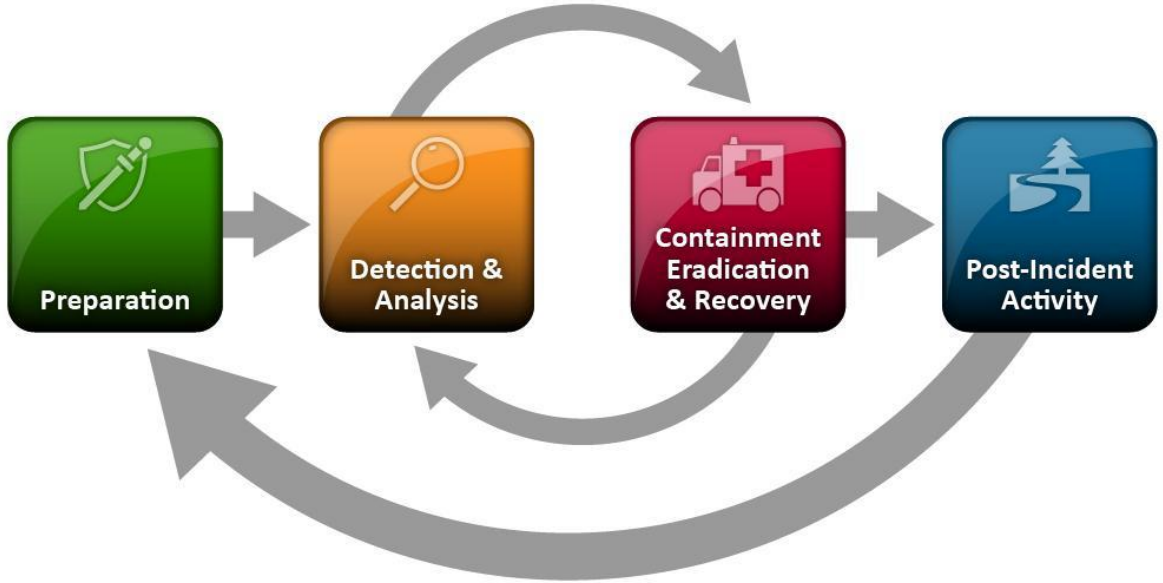
- LE Priorities probably do not match your corporate priorities
- LE is interested in:
  - Indicators of compromise (IOCs)
  - Attribution of thereat actors
  - Tactics, techniques, procedures
  - Catching the bad guys!
- LE is **NOT** interested in:
  - Securing your infrastructure
  - Remediation
  - Software/hardware recommendations

What Phase of the Incident Response Should I Call Law Enforcement?

It depends…

First, consult with inside/outside counsel

- Factors Associated with when to notify:
  - Do regulatory requirements require you to contact LE?
  - Is your business considered critical infrastructure?
  - Ongoing disruption to operations
  - Exfiltration of data (IP, PII, PHI, etc.)
  - Threats/concerns to life/health



Who is the Appropriate LE Entity to Contact?

The best LE entity is the one you have a relationship with!

- Proactively join groups like InfraGard and NCFTA
- Federal/State/Local are all options
- Local Cyber Crime Task Force
- Most important take away is to introduce yourself and your company to LE beforehand
- Internet Crime Complain Center, or IC3, is the FBI’s virtual complaint desk

Impact of Contacting Law Enforcement

ankura

What will Law Enforcement Request?

- They will likely conduct **on-site interviews**
- May request:
  - Full image copies of systems
  - Pertinent system logs
  - All IOCs
  - Copies of malware
  - Source IP addresses of threats
  - Email with extended headers
  - Packet captures
- Consent vs. Subpoena/Search Warrants

What is the Potential Impact of Notifying Law Enforcement?

It is important to weigh the risks vs. benefits before contacting LE

Benefits:

- They may share TTPs and IOCs used by the TA
- They may have ransomware decryptors
- The public/shareholders may have expectations that your company calls LE

Risks:

- Loss of control of the investigation
- Communications will probably be one-way
- Provision of evidence may provide indication of other unknown illegal activity

Case Study: Intrusion of a Medical Device Corporation

ankura

Case Study Overview: Criminal Intrusion

Preparation

- **No IR Plan- no LE contacts**

Detection and Analysis

- **Hacker communicated directly with system administrator**
- **Identified vector of compromise: remote access tool**
- **Identified originating IP address**

Containment, Eradication, and Recovery

- **Blocked remote access**
- **Obtained search warrant**
- **Arrested main subject**

Post Incident

- **Scanned infrastructure for similar vulnerabilities**
- **Reviewed needs for remote access tools**

Outcomes and Findings

- Preservation of Evidence requested filed in the US
- Emergency subpoena and search warrant served in the US
- Search Warrant executed at residence of main subject

Lessons Learned

- Have an incident Response plan in place before an incident occurs
- Engage outside counsel prior to an incident
- Proactively reach out to your local law enforcement

Applying This to Your Business

NEXT WEEK

- Draft or review your cyber incident response plan
- Begin to prepare for the cyber incident that will occur
- Identify and reach out to Law Enforcement and or groups and like Infragard and NCFTA

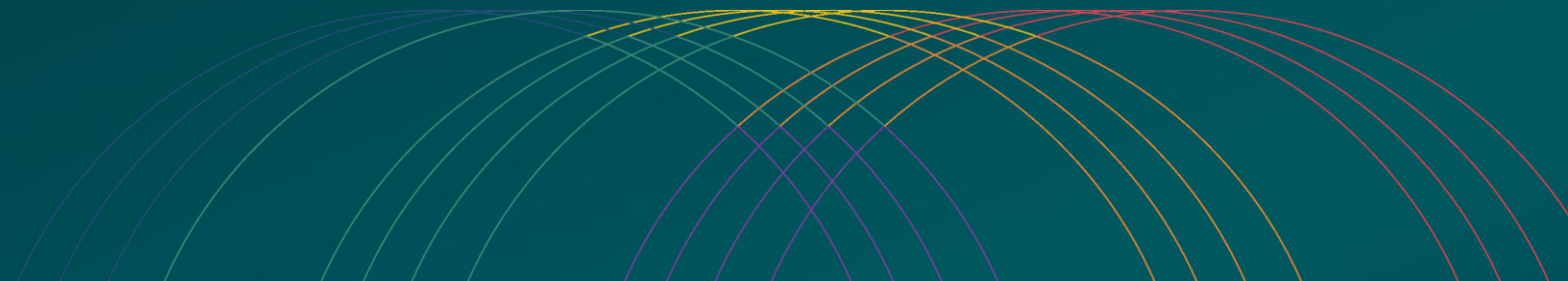
NEXT 3 MONTHS

- Ensure that your cyber incident response plan adequately reflects escalation to Law Enforcement entities

WITHIN 6 MONTHS

- Conduct a tabletop exercise to practice your cyber incident response plan, preferably while including Law Enforcement and other outsiders to provide unbiased feedback

Questions?



ankura

DATA & TECHNOLOGY

Mid-Atlantic CIO Forum

ankura.com