Legal & Regulatory Conference

IN PARTNERSHIP WITH

GRIDLIANCE

HUNTON
ANDREWS KURTH

Managing Cyber Risk from a Legal Perspective

APPA Legal & Regulatory Conference – October 8, 2018

Paul M. Tiao
Partner
(202) 955-1618
PTiao@HuntonAK.com

Kevin W. Jones
Partner
(804) 788-8731
Kjones@HuntonAK.com

The Cybersecurity and Privacy Team at Hunton Andrews Kurth

HUNTON ANDREWS KURTH

- Over **35 cybersecurity and privacy professionals** in the US, EU and Asia
- Energy Sector Security Team brings together **14 practice groups** to provide comprehensive cybersecurity and privacy assistance
- Our clients have included **6 of the Fortune 10**, and many major energy companies
- Represent clients across multiple industry sectors, including energy, utility, technology, financial services, transportation, retail, consumer products, health care, publishing and advertising
- Centre for Information Policy Leadership

Thought Leadership

Our team regularly provides insights on current privacy and cybersecurity issues and trends.

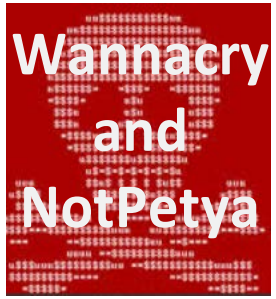
www.HuntonPrivacyBlog.com @hunton_privacy

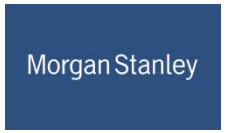
Roadmap

HUNTON ANDREWS KURTH

The Cyber Threat Landscape

HUNTON ANDREWS KURTH





Cyber Threats to the Energy Sector

HUNTON ANDREWS KURTH

2012
- Destructive malware attacks on Saudi Aramco and Qatar RasGas

2013
- Iranian cyber attacks on control systems of oil and gas companies
- PRC cyber espionage targets 23 natural gas pipeline companies

2014
- Black Energy, Havex and Sandworm malware attacks on energy ICS

2015
- Cyber attack on Ukraine power grid

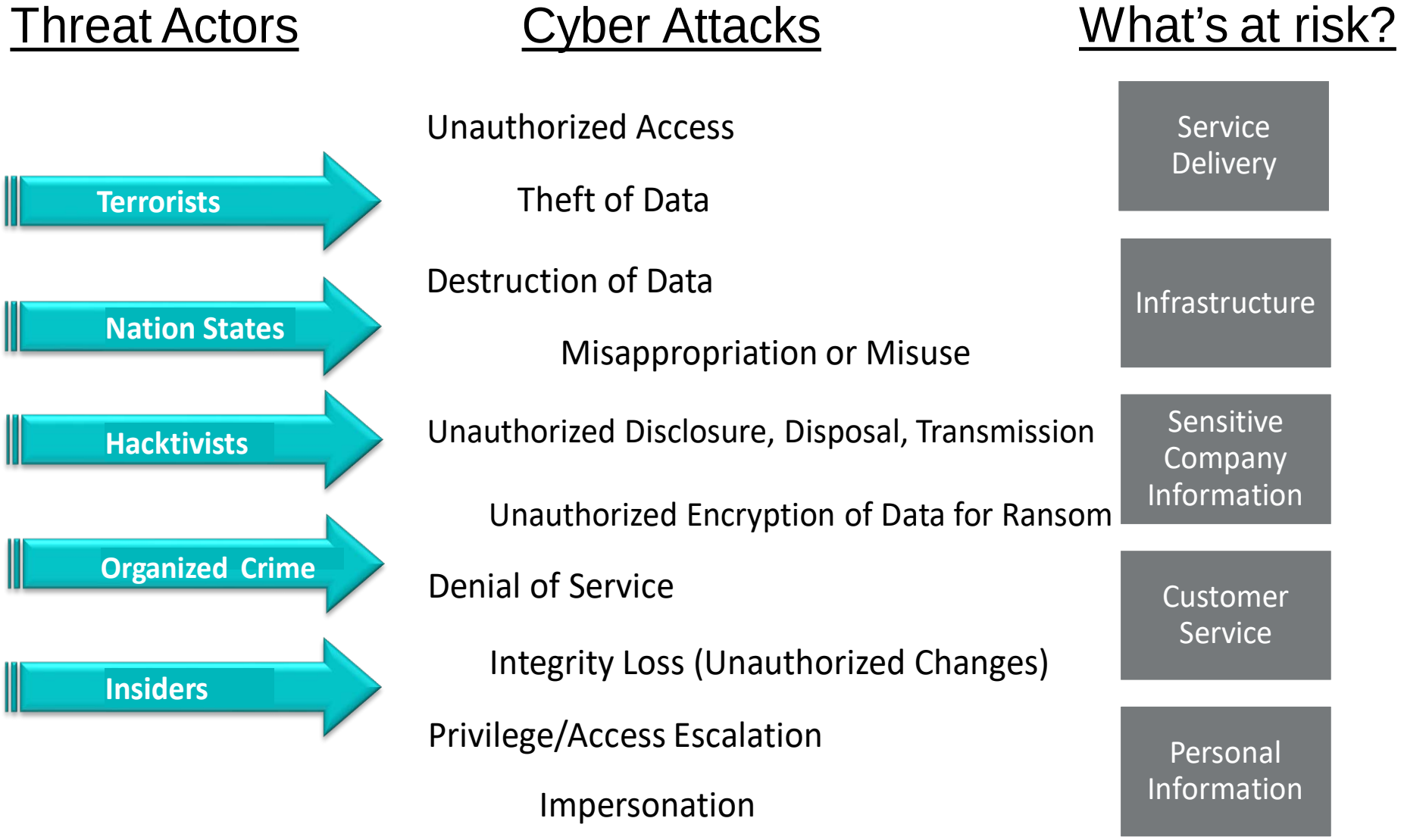
2016
- Ransomware attacks on midwest utility company

2017
- Cyber attacks on Wolf Creek Nuclear and other energy companies

2018
- DHS/FBI report on Russian cyber attacks on energy and other companies
- Cyber attack on Energy Transfer Partners electronic data interchange

Cyber Threats

HUNTON ANDREWS KURTH



US Cybersecurity Regulatory Landscape

HUNTON ANDREWS KURTH

Federal Law

- ☐ PHMSA & MTSA
- ☐ CFATS
- ☐ NERC CIP
- ☐ HIPAA/HITECH
- ☐ FTC & GLB Acts
- ☐ SEC Reporting
- ☐ ECPA/CFAA
- ☐ SOX
- ☐ CISA

State Requirements

- ☐ NYDFS Regulations
- ☐ MA, NV, CA and progeny
- ☐ Breach notification laws
- ☐ Mini-FTC Acts
- ☐ Disposal Laws
- ☐ Surveillance Laws

Industry Standards

- ☐ PCI DSS
- ☐ ISO
- ☐ NIST
- ☐ COBIT
- ☐ ISA/IEC

NERC CIP Requirements

HUNTON ANDREWS KURTH

- Mandatory and Enforceable Cyber Security Standards
  - (CIP-002 through CIP-011)
- Compliance is subject to intensive review by NERC, NPCC, and FERC
- Have been in place for a decade and evolved substantially in recent years
  - Recent developments
- Enforcement was traditionally aggressive. Has moderated but risks are still considerable.
- Supply Chain Risk Management
  - (CIP-013)

Global Cybersecurity Legal Developments

HUNTON ANDREWS KURTH

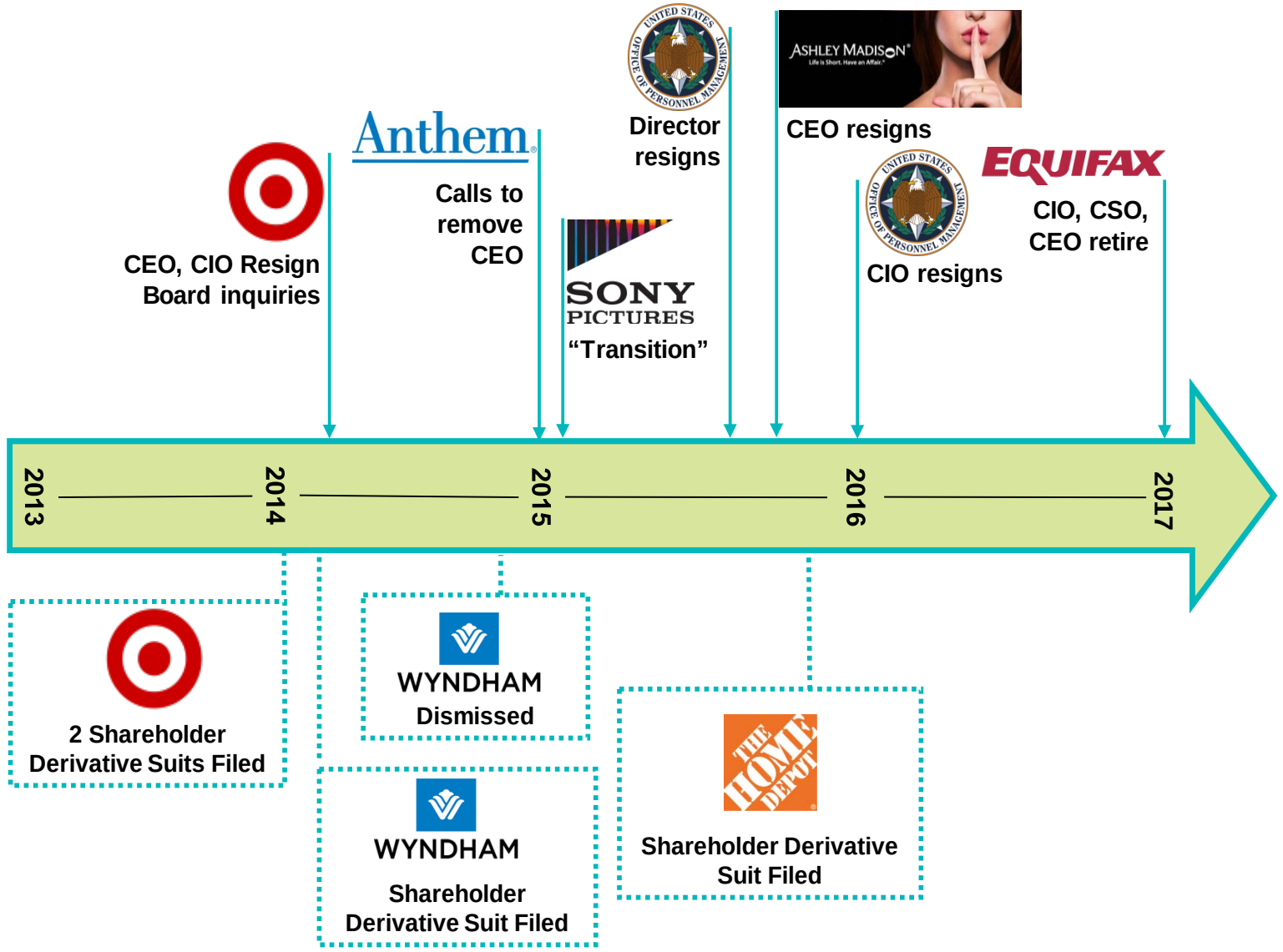
US breach notification regime	• Mature framework
EU General Data Protection Regulation (GDPR)	• Harmonization of legislation • Widened scope • Increased enforcement, fines and liability
EU Directive on Security of Network and Information Systems	• First set of pan-EU rules governing cybersecurity • Applies to "operators of essential services" and "digital service providers" • Requires managing cyber risks and reporting major security incidents
China Cybersecurity Law	• Establishes robust data security requirements for "network operators" and "operators of critical information infrastructure" in China • Law went into effect in June 2017 but several requirements have yet to be finalized
Breach notification requirements and guidance emerging across the world	• EU breach notification requirements (GDPR and NIS Directive) • Australia, Canada (Alberta), China, Mexico, Philippines, Russia, South Korea, Taiwan

Harsh Realities at the Top

HUNTON ANDREWS KURTH

"There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again."

– FBI Director Robert Mueller, March 2012

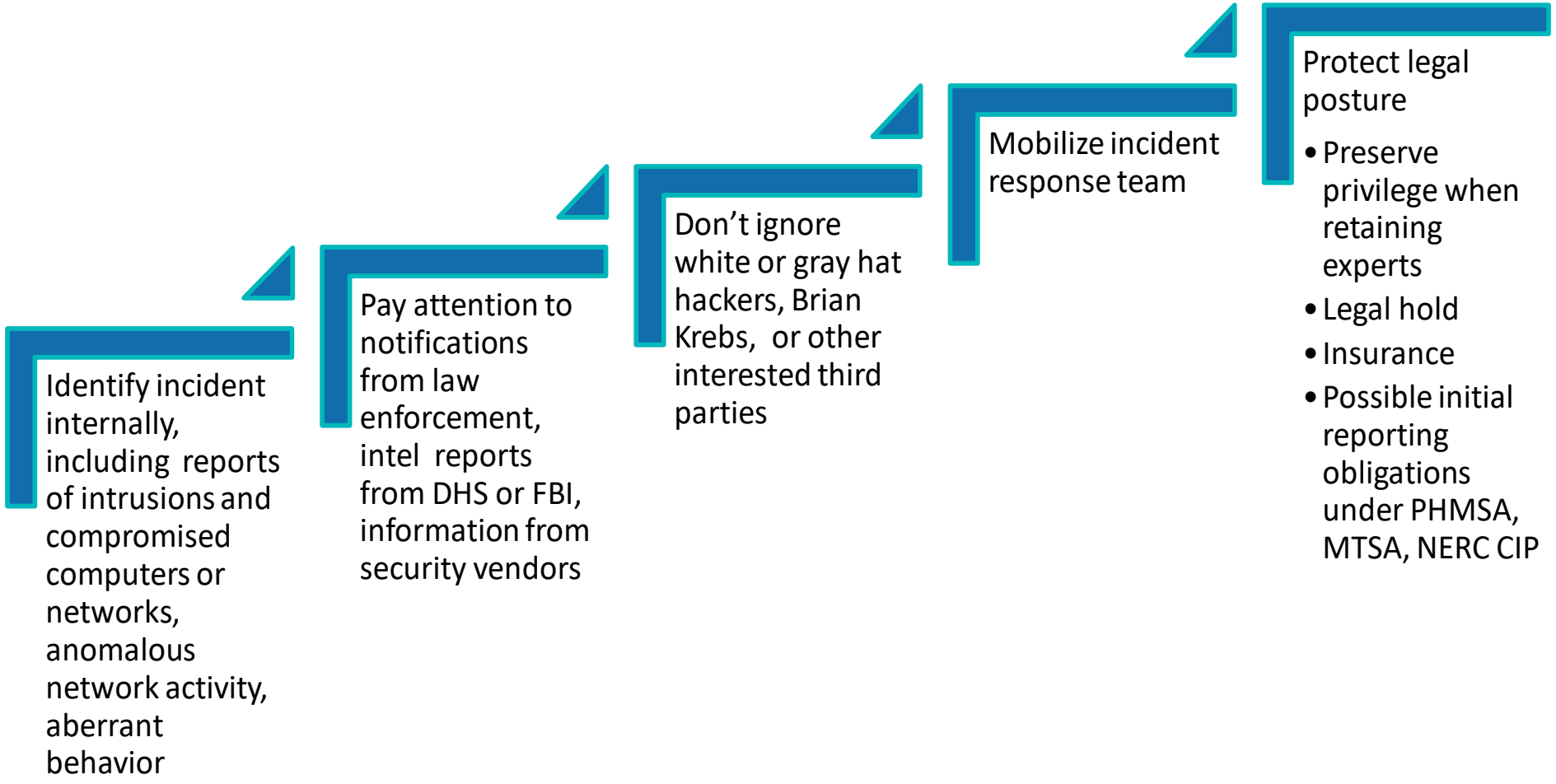


Data Breach Response Timeline

HUNTON
ANDREWS KURTH

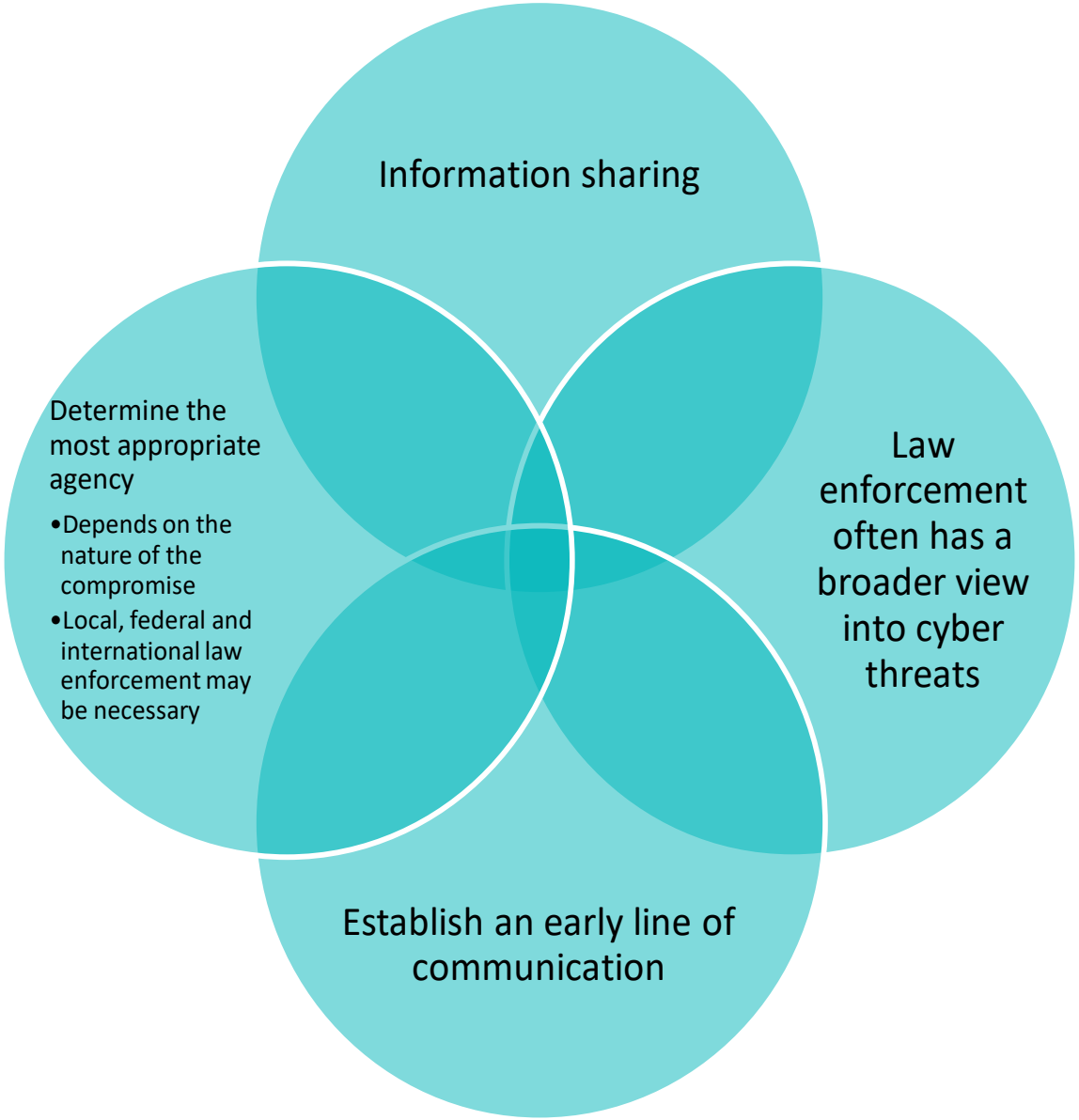
Cyber Attack: First Steps

HUNTON ANDREWS KURTH



Coordinate with FBI, DHS, Intel Community

HUNTON ANDREWS KURTH



Conduct an Investigation

HUNTON ANDREWS KURTH

- Stabilize affected systems and investigate scope
- Contain the attack
- Forensic imaging
- Restore the integrity of the system
- Retain third-party forensic experts?
- Understand:
  - Nature of the compromise
  - Data and systems at issue
  - Whether communications systems are secure
  - Whether insiders are involved

Legal Considerations

HUNTON ANDREWS KURTH

Analyze legal requirements

- State, federal, international law
- Industry standards
- Contractual obligations
- SEC reporting

Satisfy your legal obligations arising from the cyber event

- Individual and business notifices
- Reports to regulators
- Public disclosure

Notification Process

HUNTON ANDREWS KURTH

- Retain identity protection service
- Consider PR experts
- Assemble call center

- Do this carefully and quickly
- Develop FAQs and train call center agents

- Address questions from individuals
- Manage media response

Risk and Dispute Management

HUNTON ANDREWS KURTH

- Manage regulatory onslaught and defend against lawsuits
- Regulatory enforcement: State, federal and international
- Class action litigation
- Disputes with business partners and other third parties
- Insurance claims

Review and Improve

HUNTON ANDREWS KURTH

Conduct root cause analysis

- Document as appropriate

Ensure remedial actions have been taken, including disciplinary actions/invoking contractual remedies

Communicate status and outcome to senior leadership

Review and improve data security processes, policies and training

Lessons Learned

HUNTON ANDREWS KURTH

Focus on cybersecurity must come from the top

- Cybersecurity is a fundamental governance issue

Cybersecurity program maturity should be continually assessed

Preparation will mitigate harm

Cybersecurity Preparedness Measures

HUNTON ANDREWS KURTH

- Establish the appropriate governance structure
- Ensure written information security policies are state-of-the-art
- Identify and classify sensitive data
- Maintain incident response plan
- Prepare Incident Response Team though tabletop exercises
- Prepare data breach toolkit
- Improve access to cyber threat information
- Continually assess status of technical and physical protections
- Manage vendor risks
- Manage employee risks
- Train employees and increase awareness
- Assess cyber insurance, SAFETY Act

Cyber Governance: The Role of the Board

HUNTON ANDREWS KURTH

The board sets cybersecurity tone and direction

- Target was a wake-up call
- SEC warning

Cybersecurity is a fundamental risk issue for the company

- Case law provides scant direction regarding cybersecurity management

Boards typically delegate oversight responsibilities to committees but full board retains overall responsibility

Communication with management is critical for effective cybersecurity governance

Key recent actions

- Yahoo, Home Depot, Wyndham

Manage Vendor Risk

HUNTON ANDREWS KURTH

- Information security program
- Information security standards
- Data breach obligations
- Third party audits and certifications
- Inspection rights
- Indemnification
- Liability caps, liability carve-outs, warranties, force majeure clauses, insurance, termination and other remedies

Improve Access to Cyber Threat Data

HUNTON ANDREWS KURTH

DHS

- Automated Indicator Sharing
- Cybersecurity Information Sharing and Collaboration Program (CISCP)
- National Cybersecurity and Communications Integration Center (NCCIC)
- Hunt and Incident Response Team (HIRT)
  - US-CERT
  - ICS-CERT

FBI

- Cyber Division & FBI Field Offices
- National Cyber Investigative Joint Task Force
- National Cyber and Forensics Training Alliance
- Domestic Security Alliance Council
- InfraGard

Strengthen Insider Threat Program

HUNTON ANDREWS KURTH

Human Resources

- Background checks, training, rules and requirements
- Accurate and timely reporting of potential problems, incidents, red flags

Management

- Identify critical assets and implement a plan for protecting them
- Build a culture of awareness about insider threats
- Establish a central hub for data fusion, analysis and response

Information Security

- Login banners
- Segregation of duties and least access privileges
- Network logging and monitoring
- Security alerts

Risk Indicators

Personal, loyalty, technology, performance, foreign influence

Reduce Financial Risk

HUNTON ANDREWS KURTH

Cybersecurity Insurance

- In general
- Operational technology

SAFETY Act

- Background
- Homeland Security Act of 2002
  - Qualified anti-terrorism technology
  - Definition of “Act of Terrorism”
  - DHS determination that Act of Terrorism has occurred
- Liability protections
- Insurance protection

Update Incident Response Plan and Conduct Table Top Exercises

HUNTON ANDREWS KURTH

Incident Response Plan

- Work with cybersecurity team to update incident response plan
- Define triggers for mobilizing the response team
- Set out key roles and responsibilities
- Provide a clear roadmap for company to follow when an incident occurs

Tabletop Exercises

- Prepare a detailed scenario that includes multiple incidents
- Identify participants
- Conduct a tabletop exercise on-site, with discussion to follow
- Prepare a summary of issues identified during the exercise

Contact Us

Telephone

202 955 1500

Address

2200 Pennsylvania Ave., NW
Washington, DC 20037

Website

PTiao@HuntonAK.com
www.HuntonAK.com