HUNTON
ANDREWS KURTH

Cybersecurity Crisis Management – Are You Ready?

Society of Corporate Compliance and Ethics
Utilities & Energy Compliance & Ethics Conference

Paul M. Tiao
Hunton Andrews Kurth LLP
(202) 955-1618
PTiao@HuntonAK.com

Lori Spence
MISO
(317) 249-5442
lspence@misoenergy.org

David Douglass
Evergy, Inc.
(816) 556-2016
david.douglass@kcpl.com

What is your role?

HUNTON
ANDREWS KURTH

A) Compliance & Ethics Professional
B) Legal
C) Executive
D) Consultant
E) Finance
F) Jack of All Trades, Master of None

2

Results of Poll

HUNTON ANDREWS KURTH

3

Roadmap

HUNTON ANDREWS KURTH

- Cyber Threat Landscape
- US Regulatory Cyber Landscape
- Global Legal Developments
- Responding to a Cyber Incident
- Cybersecurity Preparedness Measures

4

The Cyber Threat Landscape

HUNTON ANDREWS KURTH

5

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

6

Who do you think is your company's biggest Threat Actor?

HUNTON ANDREWS KURTH

A) Terrorists
B) Nation States
C) Hacktivists
D) Organized Crime
E) Insiders
F) Other

7

Results of Poll

HUNTON ANDREWS KURTH

8

What do you think is most at risk for your company due to cyber threats?

HUNTON ANDREWS KURTH

A) Service Delivery/Reliability
B) Infrastructure
C) Sensitive Company Information
D) Customer Service
E) Personal Information
F) Other

9

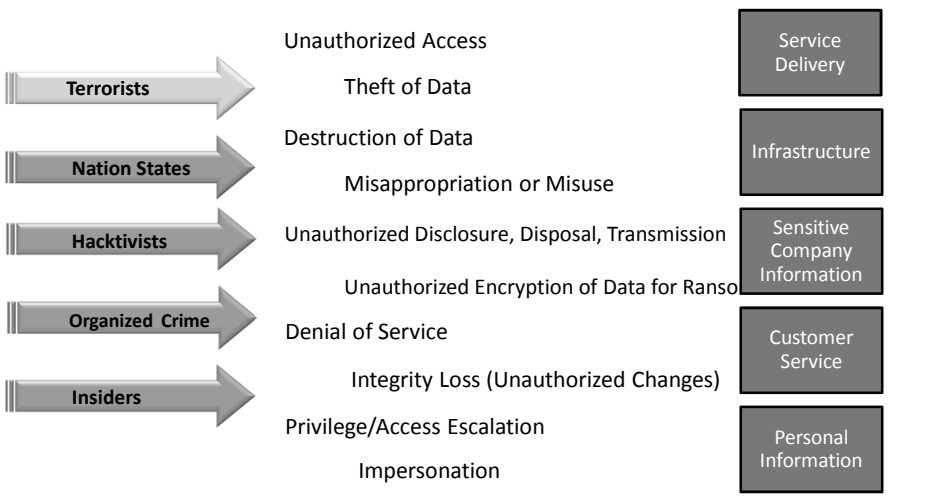
Results of Poll

HUNTON ANDREWS KURTH

10

Cyber Risks

HUNTON ANDREWS KURTH



11

US Cybersecurity Regulatory Landscape

HUNTON ANDREWS KURTH

Federal Law	State Requirements	Industry Standards
☐ PHMSA & MTSA	☐ NYDFS Regulations	☐ PCI DSS
☐ CFATS	☐ MA, NV, CA and progeny	☐ ISO
☐ NERC CIP	☐ Breach notification laws	☐ NIST
☐ HIPAA/HITECH	☐ Mini-FTC Acts	☐ COBIT
☐ FTC & GLB Acts	☐ Disposal Laws	☐ ISA/IEC
☐ SEC Reporting	☐ Surveillance Laws	
☐ ECPA/CFAA		
☐ SOX		
☐ CISA		

12

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 -- which are themselves subject to close political scrutiny
- Have been in place for a decade and evolved substantially in recent years
  - Incremental recent developments
- Enforcement was traditionally aggressive. Has moderated but risks are still considerable.
- Supply Chain Risk Management
- Block Chain Technology

13

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

14

How prepared are your company's Executives and Board to respond to a cyber security incident?

HUNTON ANDREWS KURTH

A) Absolutely ready
B) Has participated in drills/exercises
C) Aware of crisis management plan
D) Not included in preparations
E) Still in the dark…

15

Results of Poll

HUNTON ANDREWS KURTH

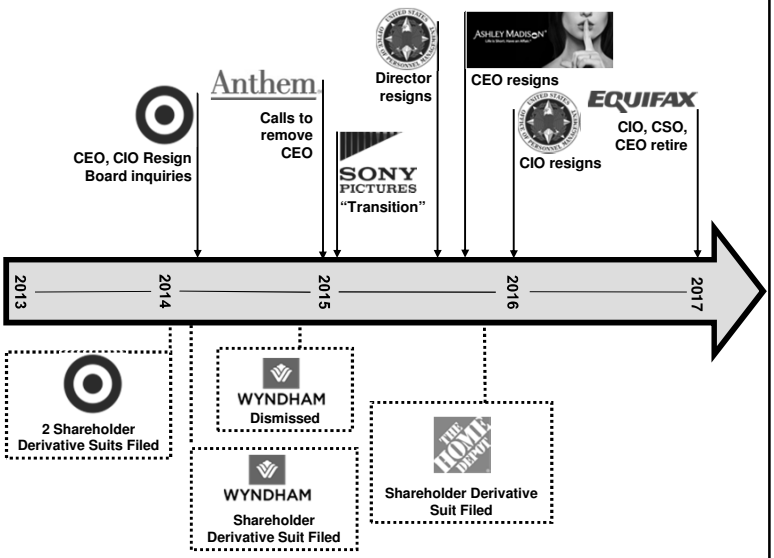
16

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



17

Cyber Incident Response Timeline

HUNTON ANDREWS KURTH

18

Have you been involved in a response to a cyber incident?

HUNTON ANDREWS KURTH

A) Yes
B) No, not my responsibility
C) No, we have not had a cyber incident
D) No, but we have conducted incident response drills

19

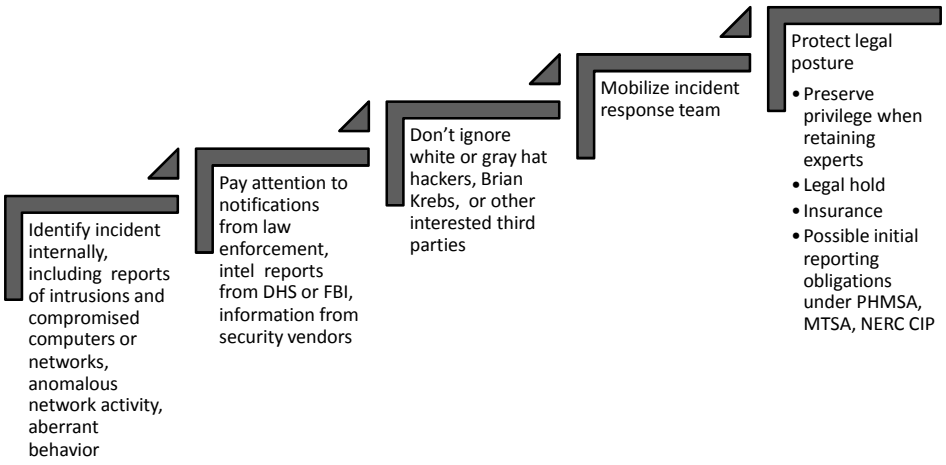
Results of Poll

HUNTON ANDREWS KURTH

20

Cyber Attack: First Steps

HUNTON ANDREWS KURTH



21

To what extent does your company have a collaborative relationship with the FBI, DHS, or other parts of the intelligence communities?

HUNTON ANDREWS KURTH

A) Very involved
B) Good lines of communication established
C) Not as involved as we should be
D) Only when required
E) I don't know – not my responsibility

22

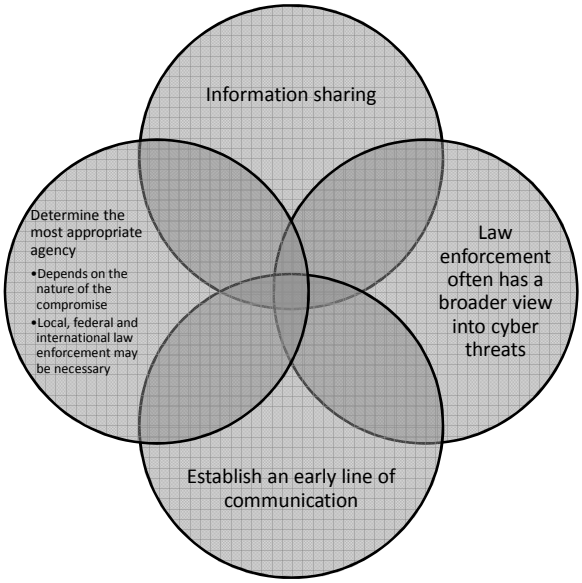
Results of Poll

HUNTON ANDREWS KURTH

23

Coordinate with FBI, DHS, Intel Community

HUNTON ANDREWS KURTH



24

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

25

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 notices • Reports to regulators • Public disclosure

26

Notification Process

HUNTON ANDREWS KURTH

Prepare for notification and public disclosure

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

Craft formal notification and reporting documents

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

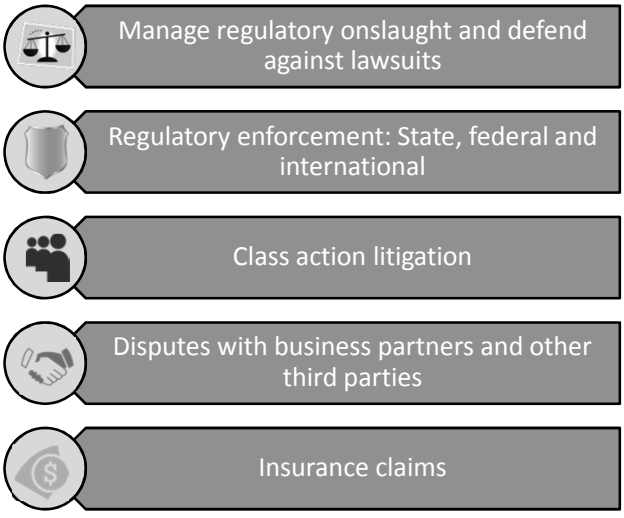
Issue notices and manage responses

- Address questions from individuals
- Manage media response

27

Risk and Dispute Management

HUNTON ANDREWS KURTH



28

Reduce Financial Risk

HUNTON ANDREWS KURTH

Cybersecurity Insurance

- In general
- Operational technology

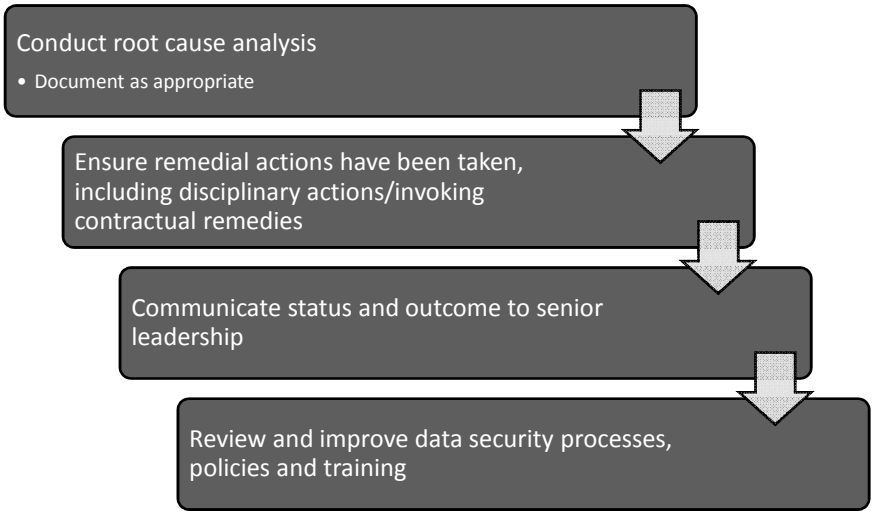
SAFETY Act

- Background
- Homeland Security Act of 2002
- Qualified anti-terrorism technology
- Certification and Designation – How to Apply
- Reputational Protection
- Legal Defenses
- Liability Cap

29

Review and Improve

HUNTON ANDREWS KURTH



30

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

31

Update Incident Response Plan and Conduct Table Top Exercises

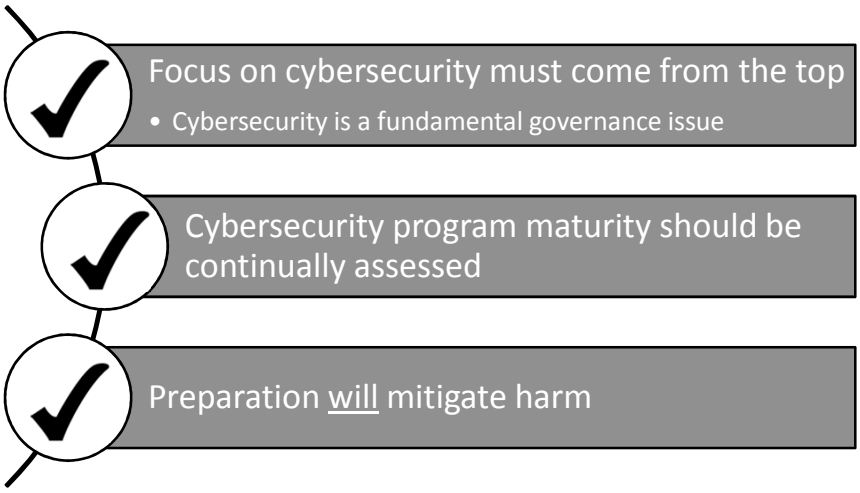
HUNTON ANDREWS KURTH

Incident Response Plan	Tabletop Exercises
• 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	• 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

32

Lessons Learned

HUNTON ANDREWS KURTH



33

QUESTIONS?

HUNTON ANDREWS KURTH

THANK YOU!

34