What is your role?

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

Roadmap

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

- Destructive malware attacks on Saudi Aramco and Qatar RasGas
- Iranian cyber attacks on control systems of oil and gas companies
- PRC cyber espionage targets 23 natural gas pipeline companies
- Black Energy, Havex and Sandworm malware attacks on energy ICS
- Cyber attack on Ukraine power grid
- Ransomware attacks on midwest utility company
- Cyber attacks on Wolf Creek Nuclear and other energy companies
- DHS/FBI report on Russian cyber attacks on energy and other companies
- Cyber attack on Energy Transfer Partners electronic data interchange
### Who do you think is your company’s biggest Threat Actor?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Terrorists</td>
</tr>
<tr>
<td>B</td>
<td>Nation States</td>
</tr>
<tr>
<td>C</td>
<td>Hacktivists</td>
</tr>
<tr>
<td>D</td>
<td>Organized Crime</td>
</tr>
<tr>
<td>E</td>
<td>Insiders</td>
</tr>
<tr>
<td>F</td>
<td>Other</td>
</tr>
</tbody>
</table>

### Results of Poll

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**What do you think is most at risk for your company due to cyber threats?**

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

---

**Results of Poll**

---
### Cyber Risks

<table>
<thead>
<tr>
<th>Threat Actors</th>
<th>Cyber Attacks</th>
<th>What's at risk?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorists</td>
<td>Unauthorized Access</td>
<td>Service Delivery</td>
</tr>
<tr>
<td>Nation States</td>
<td>Theft of Data</td>
<td>Infrastructure</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>Destruction of Data</td>
<td>Sensitive Company Information</td>
</tr>
<tr>
<td>Organized Crime</td>
<td>Misappropriation or Misuse</td>
<td>Customer Service</td>
</tr>
<tr>
<td>Insiders</td>
<td>Unauthorized Disclosure, Disposal, Transmission</td>
<td>Personal Information</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Encryption of Data for Ransom</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Denial of Service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrity Loss (Unauthorized Changes)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privilege/Access Escalation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Impersonation</td>
<td></td>
</tr>
</tbody>
</table>

### What's at risk?
- Service Delivery
- Infrastructure
- Sensitive Company Information
- Customer Service
- Personal Information

### US Cybersecurity Regulatory Landscape

#### 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

- 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

Global Cybersecurity Legal Developments

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Absolutely ready</td>
</tr>
<tr>
<td>B</td>
<td>Has participated in drills/exercises</td>
</tr>
<tr>
<td>C</td>
<td>Aware of crisis management plan</td>
</tr>
<tr>
<td>D</td>
<td>Not included in preparations</td>
</tr>
<tr>
<td>E</td>
<td>Still in the dark…</td>
</tr>
</tbody>
</table>

Results of Poll
Harsh Realities at the Top

“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

Cyber Incident Response Timeline
**Have you been involved in a response to a cyber incident?**

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

**Results of Poll**
**Cyber Attack: First Steps**

Identify incident internally, including reports of intrusions and compromised computers or networks, anomalous network activity, aberrant behavior.

Pay attention to notifications from law enforcement, intel reports from DHS or FBI, information from security vendors.

Don’t ignore white or gray hat hackers, Brian Krebs, or other interested third parties.

Mobilize incident response team.

Protect legal posture.
- Preserve privilege when retaining experts
- Legal hold
- Insurance
- Possible initial reporting obligations under PHMSA, MTSA, NERC CIP

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

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
Results of Poll

Information sharing

Law enforcement often has a broader view into cyber threats

Establish an early line of communication

Determine the most appropriate agency

• Depends on the nature of the compromise
• Local, federal and international law enforcement may be necessary

Coordinate with FBI, DHS, Intel Community

Information sharing

Law enforcement often has a broader view into cyber threats

Establish an early line of communication

Determine the most appropriate agency

• Depends on the nature of the compromise
• Local, federal and international law enforcement may be necessary
**Conduct an Investigation**

- 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**

- 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
Notification Process

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

Risk and Dispute Management

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
Reduce Financial Risk

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

Review and Improve

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
## Cybersecurity Preparedness Measures

- 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
- Continuously assess status of technical and physical protections
- Manage vendor risks
- Manage employee risks
- Train employees and increase awareness
- Assess cyber insurance, SAFETY Act

## Update Incident Response Plan and Conduct Table Top Exercises

<table>
<thead>
<tr>
<th>Incident Response Plan</th>
<th>Tabletop Exercises</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Work with cybersecurity team to update incident response plan</td>
<td>• Prepare a detailed scenario that includes multiple incidents</td>
</tr>
<tr>
<td>• Define triggers for mobilizing the response team</td>
<td>• Identify participants</td>
</tr>
<tr>
<td>• Set out key roles and responsibilities</td>
<td>• Conduct a tabletop exercise on-site, with discussion to follow</td>
</tr>
<tr>
<td>• Provide a clear roadmap for company to follow when an incident occurs</td>
<td>• Prepare a summary of issues identified during the exercise</td>
</tr>
</tbody>
</table>
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

THANK YOU!