Cybersecurity In the Energy Sector: What Could Possibly Go Wrong?

April Doss
Chair, Cybersecurity and Privacy
Saul Ewing Arnstein & Lehr
March 5, 2020

SAUL EWING
ARNSTEIN
& LEHR LLP

Cybersecurity in the energy sector: Hypothetical Scenario #1: Cyberattack on a Dam

- A hydroelectric power plant relies on a dam to power its turbines. The dam contains a reservoir that sits above a valley, with a town below the dam.
- A cyber attacker probes the defenses of the power plant and discovers that the dam's supervisory control and data acquisition (SCADA) systems connect to the internet through a cellular modem. The hacker accesses water temperature and water level information through his remote SCADA access. He waits until a time when heavy rains have filled the reservoir to capacity and executes a remote command to open the floodgates.
- The release causes millions in property damage, economic loss to the town, road damage, and environmental cleanup costs.
- Background:
  - In 2016, the U.S. indicted a group of Iranian hackers for attacks on U.S. infrastructure, including a remote penetration of the Bowman Avenue Dam in Rye, New York.
  - Although a small dam and the attack was stopped before physical damage was done, past dam failures demonstrate potential harm.

Hypothetical Scenario #2: Damage to Power Plant Turbines

- A cyber attacker has carried been probing the external network interfaces of a natural-gas power plant for 18 months. The attacker has found an entry into the system and installed software that allowed him to harvest legitimate user credentials to access restricted systems on the network.
- The attacker exploits a Windows vulnerability to access the computer systems that control turbine speed and detect malfunctions. The hacker installs malware that allows him to change the turbine speed and to turn off malfunction notifications. When the malware is activated, the turbine abruptly halts and reverse direction. The turbine seizes up, starts throwing blades, and each blade causes more damage to the expensive machine. Within moments, the damage is irreparable, costing millions of dollars and shutting off energy supply.
- Background:
  - Most power plants – coal, natural gas, hydroelectric – use turbines to generate power. These costly items are essentially jet engines spinning at high rates of speed. They are often controlled by microprocessors, and often have highly sensitive calibrations.
- Two real-world events show how this could happen:
  - The 2010 Stuxnet malware attack demonstrated the ability to control turbines through remote cyberattack on industrial control systems.
  - A 2017 cyberattack on a Saudi petrochemical plant gave hackers control over emergency shut-off systems. The Triton malware compromised a 16-year-old safety control system.

Hypothetical Scenario #3: Cyberattack Exploiting the Water-Hammer Effect

- A hacker carries out a spear-phishing campaign and gains valid user credentials for the internal network of a power plant. The internal network is segmented but not air-gapped – the SCADA and safety systems aren't directly connected to the internet, but they are connected to the overall IT architecture for the plant, which has internet connections.
- Once in the corporate IT system, the hacker is able to access the engineering control systems. He manipulates the carefully calibrated flow rate of water through the plant's cooling systems. A surge in flow causes pipes to burst in key areas of the plant. Turbines suffer catastrophic damage from overheating; power supply to the electric grid is halted; employees are critically injured when the pipes burst.
- Background:
  - Both nuclear and conventional power plants need to cool power generation systems, either cooling a reactor or the turbines used in coal, natural gas, and hydroelectric power plants. Usually done by piping water through heated infrastructure.
  - Steam-hammer and water-hammer are related pressure problems that can cause leakage at joints, burst pipes, and damaged supports and pipe racks.
  - The 2007 and 2018 New York steam pipe explosions were attributed to steam hammer.

Hypothetical Scenario #4: Cyberattack Resulting in Radioactive Contamination

- Hackers carry out a phishing attack to penetrate the business systems of a nuclear power plant. The network contains sensitive information about operations, including plant design, operations files, and email addresses and other job-related information for plant workers.
- Using information stolen from the business side, the hackers launch a successful attack on the operational computer network. Once inside the network, they install software that targets critical safety systems.
- The hackers use this malware to deactivate cooling rods, leading to a meltdown of the reactor's core that destroys the reactor and releases dangerous levels of radioactive contamination into the water and air surrounding the plant.
- Multiple class action lawsuits are filed for the resulting environmental cleanup costs and radiation-related medical conditions that could develop over time. Litigation and other costs are in the hundreds of millions of dollars.
- Background:
  - In 2017, the reports surfaced that Russia had attacked the Wolf Creek nuclear power plant in Kansas City.
  - Separately, researchers have observed "TRISIS" malware that can infect industrial controllers, with the potential effects described in the scenario above.

How Real is the Cyber-Kinetic Threat?

PRO CYBER NEWS

Ransomware Attack Exposes Poor Energy-Sector Cybersecurity

An infection at a pipeline provider caused it to shut down for two days, DHS says

CONGRESS

Battle lines form over pipeline cyberthreat

Blake Sobczak, E&E News reporter • Energywire: Thursday, July 25, 2019

Pipeline Security Guidelines

future tense

A Cyber Attack May Have Caused a Turkish Oil Pipeline to Catch Fire in 2008

By ARIEL BOGLE

DEC 11, 2014 • 5:08 PM

From Election Security to information operations, what do we need to know about hacking now?

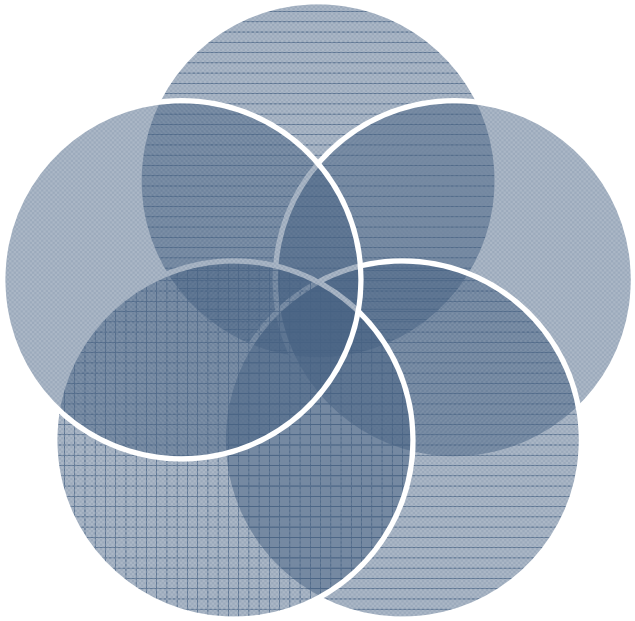
Key drivers:

- The evolution of cyber security threats
- Rapid leaps in technology and interconnectedness
- The growth of big data, machine learning, and artificial intelligence
- The threat of misinformation, disinformation, and manipulation based on data
- New ways of monetizing information – which lead to new incentives to collect, process, and compromise data
- Against a background of increasingly complex data privacy laws

The challenges are only becoming more numerous and complex

The Evolving Relationship between Cybersecurity and Data Privacy

Cybersecurity

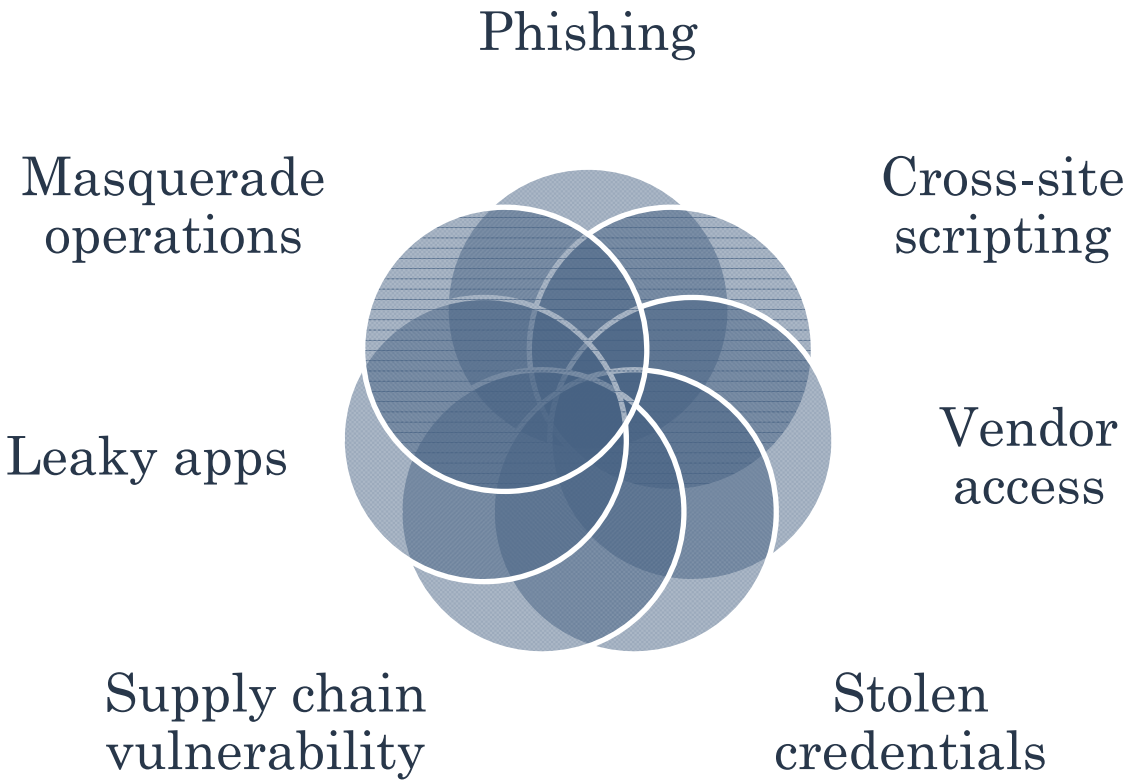


Business email compromise

Confidentiality/ Integrity/ Availability

Information operations

Data Privacy



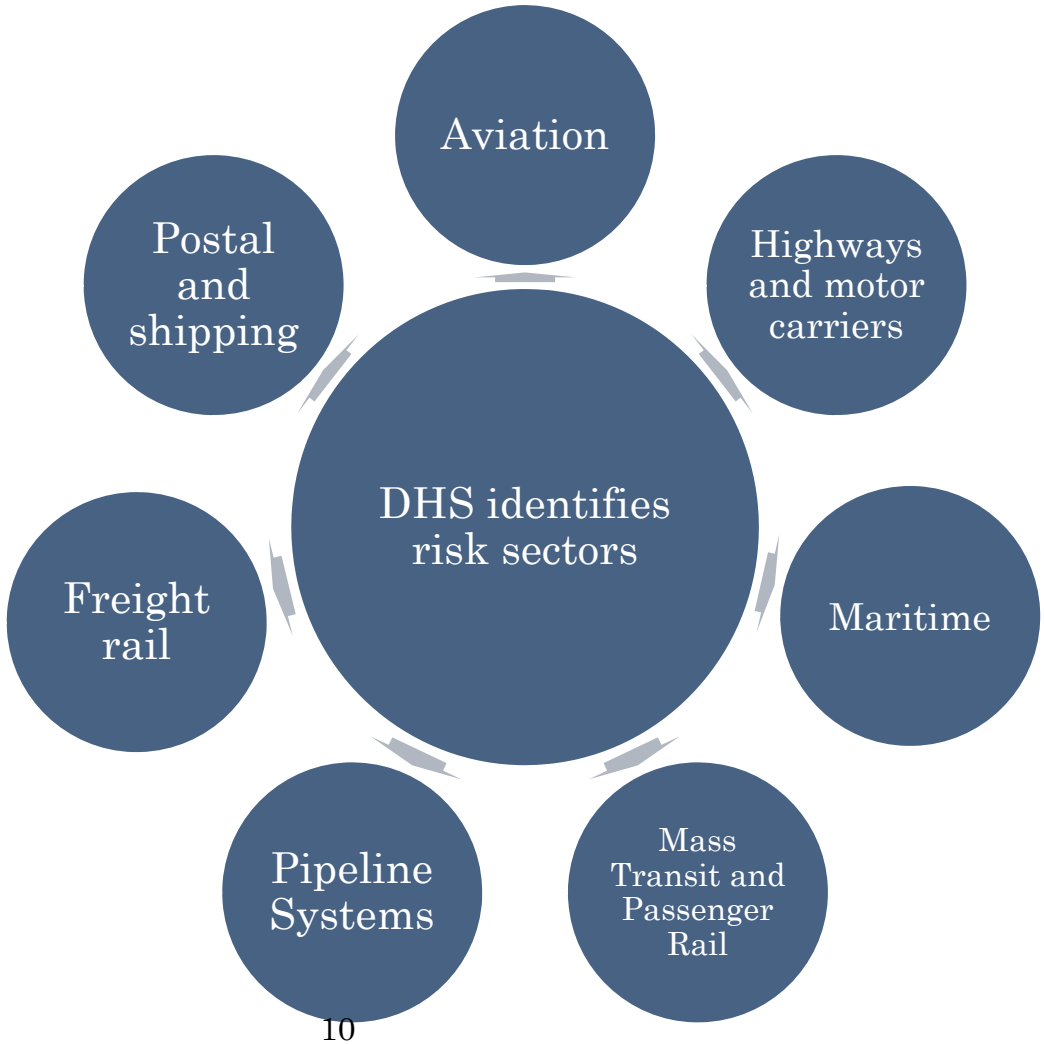
ACCOMPLISHED BY CROSS-CUTTING MEANS

Cyber actors are using common tools to gain network access and launch a variety of attacks.

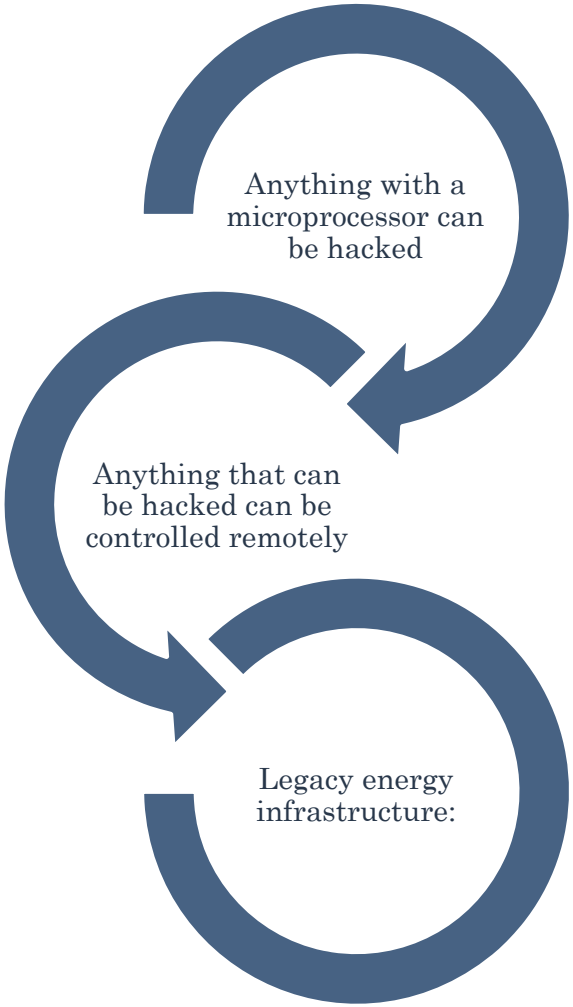
The same technique can be used for many purposes and result in many different kinds of cyber outcomes

While nation-states are hard to defend against, the biggest risks come from human error.

Where do Vulnerabilities Exist In critical infrastructure?



Cyber Risk Fundamentals

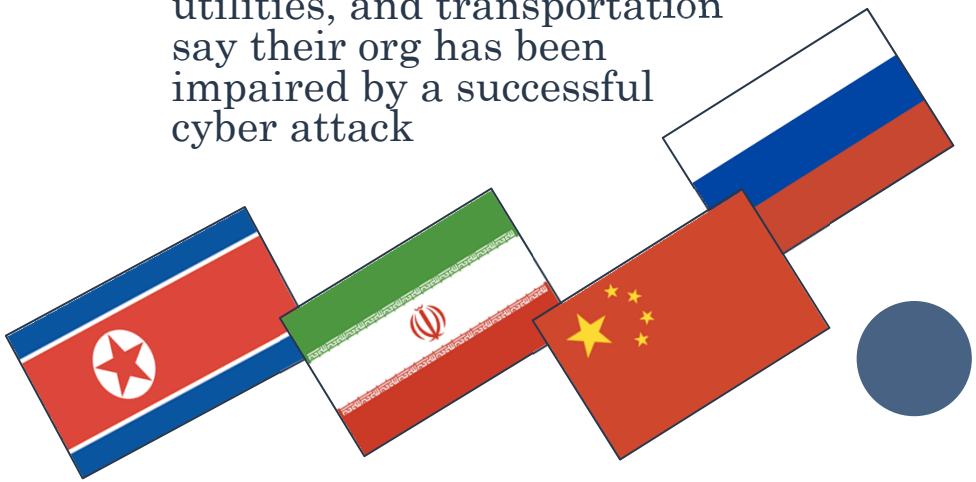


- Energy sector infrastructure:
  - Frequently built on hard-coded industrial control systems that require physical access to hack. *But*
  - Frequently retro-fitted to allow remote monitoring and/or operation
  - Often controlled from or connected to computer systems connected to internet-enabled devices
  - These upgrades introduce new vulnerabilities to cyber attacks carried out from afar.

Cyber Attacks on Critical Infrastructure*

*A non-exhaustive list

- 2014:
  - DHS reports hackers target 23 pipelines, gathering data that could be used for sabotage
- 2015:
  - Polish national airline cancels flights due to cyber intrusion
  - Flights at Swedish Airports cancelled because of attack on air traffic control
  - Attack on Ukraine's power grid leaves large areas without electricity
- 2017:
  - Breach of state-owned utility in Ireland
  - GCHQ warns state-sponsored hackers likely breached ICS of UK energy companies
- 2019
  - Nuclear power plant in India hit with nation-state cyber attack
  - Ransomware attack on Cleveland airport results in customer-facing disruptions
  - NERC warns of ongoing cyber recon of electric utilities by state-sponsored hackers
  - Ponemon: in 6 countries, 90% of security pros in energy, utilities, and transportation say their org has been impaired by a successful cyber attack



WHAT ARE SOME OF THE MAJOR CYBERSECURITY THREATS TODAY?

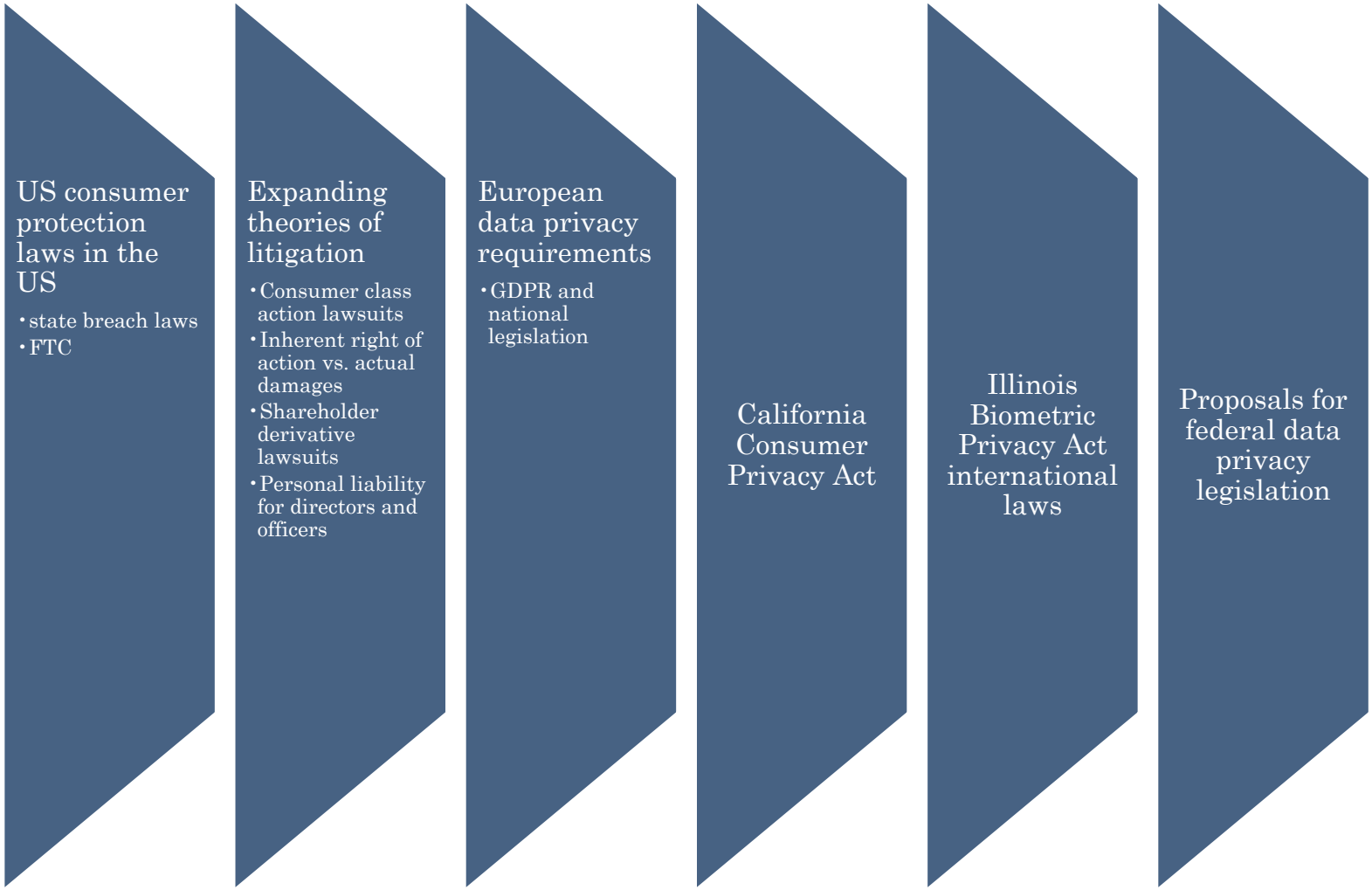
Enduring Threats

- Data breaches
  - PII
    - Biometrics
  - PHI
  - Intellectual property
    - Customer lists
  - Financial data
- Business email compromise
- Ransomware
- Website defacement

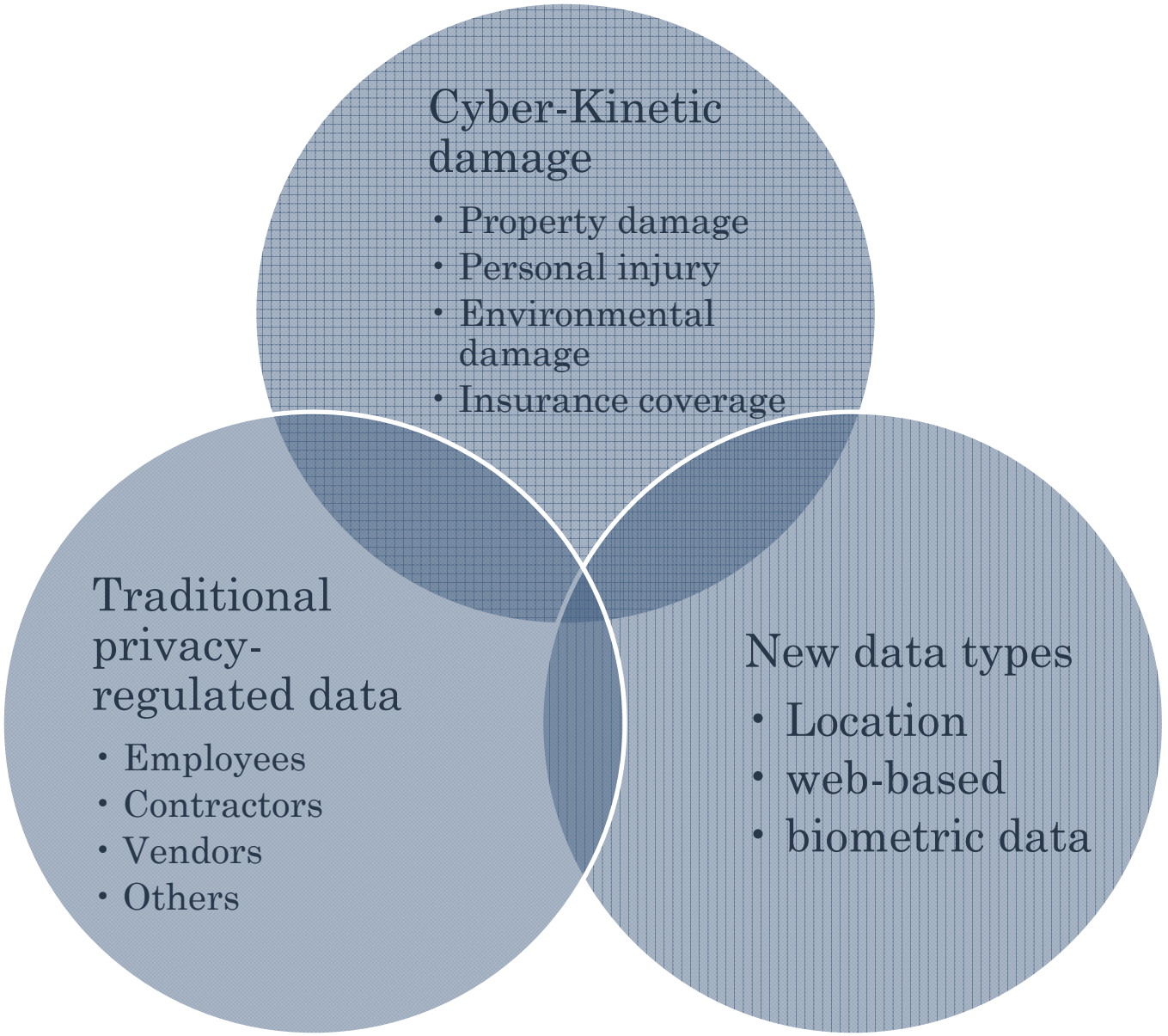
Emerging Threats

- Information operations
  - Influence
  - Harassment
  - Weaponization of information – corporate and personal
- Internet of Things
  - Increased attack surface
  - Potential for kinetic harm
- Kinetic consequences
  - Personal injury
  - Property damage
  - Environmental harm

A Sampling of Privacy-Related Legal Liability



Areas of Legal Risk and Uncertainty



What Can Be Done? What Should Be Done?

For organizations

- Cybersecurity programs
  - People
  - Process
  - Technology
  - Preparation and Response
- Privacy programs
  - Data governance
  - Training and awareness
- Interdisciplinary approach
  - Vendors
  - Compliance
  - Risk mitigation
  - Insurance

For policymakers

- Current issues:
  - Cybersecurity guidelines:
    - CISA
    - TSA
    - NIST
  - Updates to legislation
    - Terrorism Risk Insurance Act
- Will old approaches work?
  - Incentives for information sharing
- Achieving effective inputs
  - Interdisciplinary expertise

Cyber Risk in the Energy Sector: Back to practical concerns

- How to think about cyber defense
  - Nation-states v. smash-and-grab
- Enterprise approach
  - Including Board-level engagement
- Legal frameworks
  - Know your exposure
- Cyber preparedness
  - Pay now, or pay more later
- Privacy programs
  - Start with the basics
- Vendor liability
  - Contract review
- Risk tiering
  - Focus on crown jewels first
- Risk mitigations
  - Can be cost-effective and practical