Cyber Threat Landscape for Critical Infrastructure Sectors

Ransomware Cartels & Jackware

EPIC®

Insurance Brokers & Consultants

AGENDA

- Rate of Change
- Critical Infrastructure
- Evolution of Cyber Crime
- Cyber Insurance
- Insurance Coverage Considerations

MEET THE SPEAKERS

Host:

Nikki Howes
Client Advocate
West Region Energy & Marine Practice
EPIC Insurance Brokers & Consultants

Moderator:

Kelly Geary, Esq. ACP, CCP, CIPP/US
National Practice Leader, Executive Risk & Cyber
EPIC Insurance Brokers & Consultants

Panelists:

Jen Falkenholm
Vice President, National Cyber Practice
EPIC Insurance Brokers & Consultants

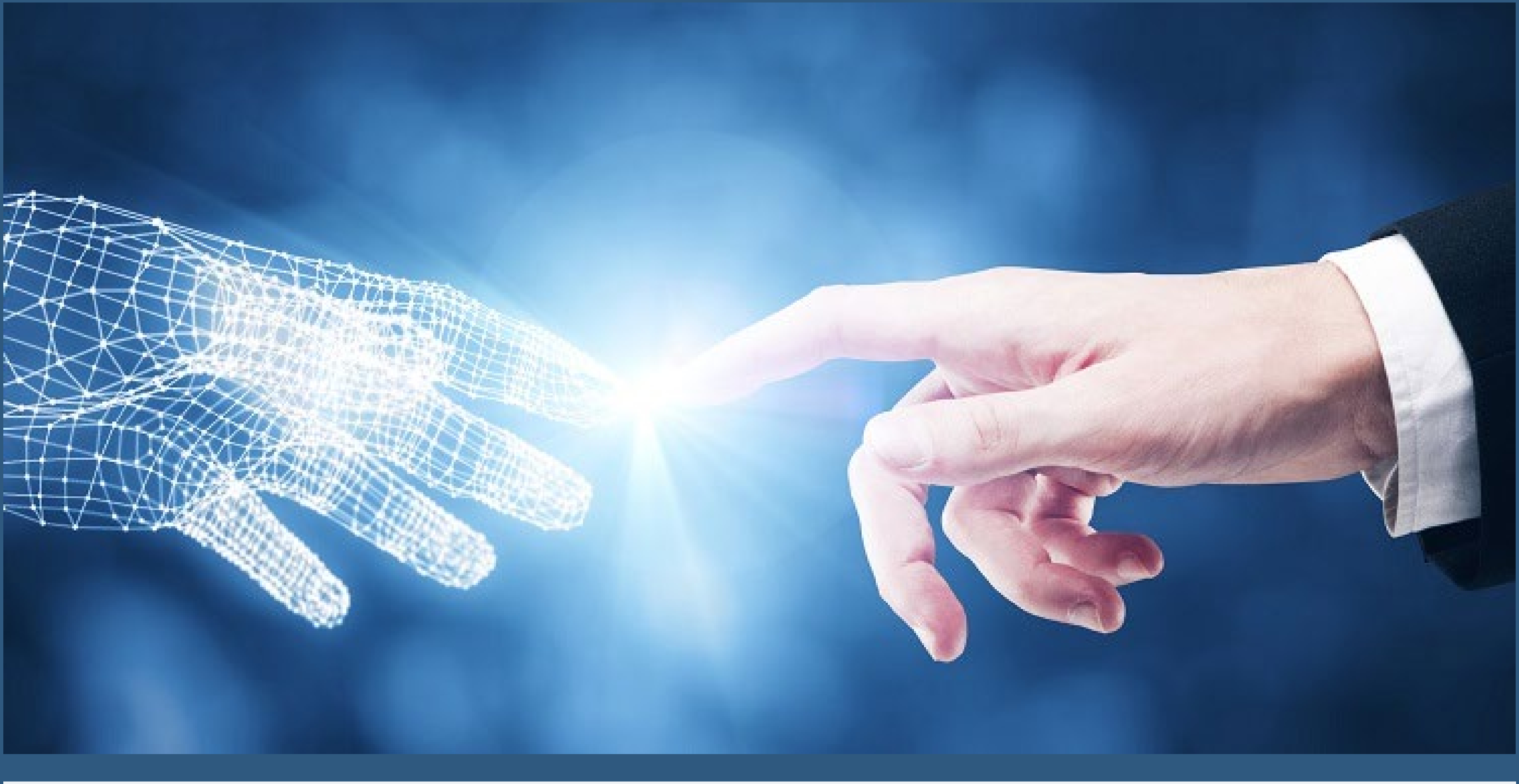
Daniel J. Healy, Esq.
Partner, Co-Chair Cyber Insurance Recovery Group
Anderson Kill, LLP

RATE OF CHANGE

Speed of current technological advances has NO historical precedent!

*"We won't experience 100 years of progress in the 21st Century – it will be more like **20,000 years of progress**."*

Futurist, Ray Kurzweil (2001)



5G Revolution/IoT

More speed, more connectivity, more power & reliability

Allow for more autonomous driving, virtual/augmented reality, AI

Will usher in a **massive transition** to device connections to the internet → "IoT"

“SMART” Devices

Thermostats: A thermometer in a lobby aquarium at a Casino

Group of hackers managed to access the Casino’s network via an internet-connected thermometer in an aquarium and extract its high-roller database with all sensitive details.

Locks: Ransomware disables “smart” hotel door system in Austria

A four-star resort hotel in Austria; ransomware attack that crippled the electronic “smart locks” on guest rooms. Hackers compromised the hotel’s electronic key system, as well as all of its computers.

Cars: Rely heavily on computer systems

Hacking into an unsecured smart vehicle system is akin to hacking into a standard IoT device. Hackers use the smart car’s infotainment system via diagnostic services to take control of the car’s functions or gain insight into passwords, voice controls and more. Hackers can do a lot of damage:

- ✓ Cut the engine.
- ✓ Initiate or disable brakes.
- ✓ Disable airbags.

Critical Infrastructure

EPIC

What is Critical Infrastructure

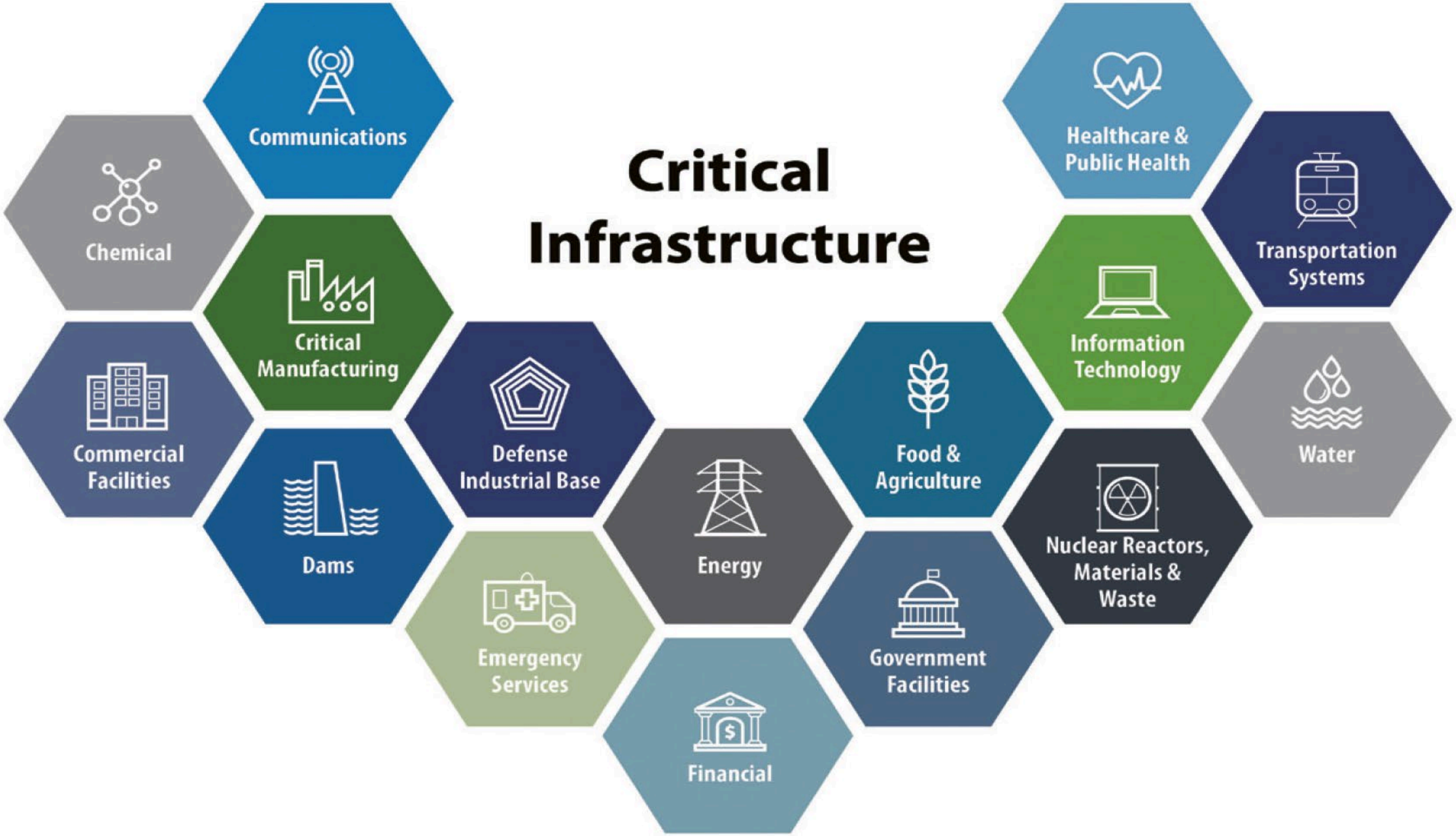
- ✓ The nation's critical infrastructure provides the **essential services** and assets that serve as the ***backbone*** of the nation’s economy, security, and health.

- ✓ Critical infrastructure describes the ***physical and cyber systems and assets*** that are so **vital** to the United States that their incapacity or destruction would have a **debilitating** impact on physical or economic security, public health or safety.

Cyber and Infrastructure - CISA

- Established in **2018**
- **Cybersecurity and Infrastructure Agency**
- Cybersecurity and Infrastructure **Security** Agency (**CISA**) is a *standalone* United States federal agency, an operational component under Department of **Homeland Security** (**DHS**) oversight.
- **Mission**: Lead the National effort to understand and manage **cyber and physical** risk to our critical infrastructure.

Critical Infrastructure



Communications

Chemical

Critical Manufacturing

Commercial Facilities

Dams

Defense Industrial Base

Emergency Services

Energy

Financial

Food & Agriculture

Government Facilities

Healthcare & Public Health

Information Technology

Nuclear Reactors, Materials & Waste

Transportation Systems

Water

© US Cybersecurity & Infrastructure Security Agency (CISA)

Evolution of Cyber Crime

Cyber Crime is BIG BUSINESS

***MULTI-TRILLION** DOLLAR INDUSTRY:*
*MATURE & **HIGHLY PROFITABLE** BUSINESS MODEL*

- Same level of **professionalism, discipline and structure** as a legit business.
- Not just "Freelancers" anymore:
  - Organized Groups some w/as many as 80,000 people and a "global footprint"
  - Average age of hacker today is 35
- Exhibit "*corporate behavior*" – Supply Chains, Call Centers, Help Desks!
- Selling Goods: hacking software - $30-40 kit
- Selling Services: Ransomware-as-a-service; you can literally outsource an attack.
- Hacking Courses available at reasonable cost

- Emergence of **Ransomware Cartels**
  - **Group of independent market participants who collude w/each other to improve profits & dominate market**

Ransomware & Jackware

Ransomware:

Primary purpose is to encrypt, lock, hold hostage your **computer system and data**

Jackware:

Ransomware + Internet Connected Devices

Primary purpose is to encrypt, lock, hold hostage **an Internet Connected Device**.

Why is this concerning now?

PERFECT STORM!

- 5G Revolution
- Cyber Crime
  - Largely Anonymous
  - No Geographic Limitations
  - HIGHLY Profitable/Financial Motivation
  - Law Enforcement & IT Professionals *Overwhelmed* and Lack Necessary Tools (skills, training, laws, resources)
- Exhaustion/Complacency/Defeat
  - Breach Fatigue
  - Ransomware Fatigue

Attacks on Critical Infrastructure

2015

Cyber attack on power grid in Ukraine, using spear phishing emails

Took out power for 225,000 people

2016

Attack by Iranian State Actors on Dam in Rye Brook, NY

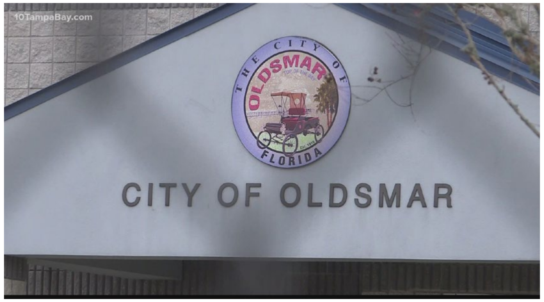
Hackers accessed Industrial Control Systems

2017

Attack on Equifax – 4 members of Chinese Military Charged in 2020

143M records/44% of the American Population

Recent Attacks on Critical Infrastructure



SUPPLY CHAIN ATTACK

Kaseya:

- Provides software/tech services to Managed Service Providers
- Based in Dublin/HQ in Miami
- 40,000 Customers

Kaseya VSA is a commonly used solution by Managed Service Providers; remote monitoring/mgmt of networks & endpoints

FBI described the incident as a *"supply chain ransomware attack leveraging a vulnerability in Kaseya VSA software against multiple MSPs and their customers.“*

REvil offered blanket decryption for all victims of the Kaseya attack in exchange for $70 million

Cyber Insurance

Cyber Insurance

- Includes Third and First party coverages
- What might trigger in response to a Ransomware or Jackware event?
  - ✓ Breach Response
    - – Breach Counsel
    - – Forensics
    - – Ransom Negotiator
  - ✓ Ransom Demand
  - ✓ Crisis Management / Public Relations
  - ✓ Business Interruption
  - ✓ Liability/Regulatory

State of the Cyber Insurance Market

- Rates/Retentions ***increasing*** substantially
  - Even companies with strong controls and no claims are seeing substantial increases: (80%+ rate increases and retentions)
- Capacity and competition is ***constricting***
  - Markets have become more selective: willing to *walk away from* risks and are *reluctant to compete* depending on cybersecurity maturity.
  - Reductions in capacity
  - Carriers Exiting the Market
- Coverage is ***tightening***
  - Ransomware Coinsurance/Sublimits – becoming more common
- Underwriting is more ***comprehensive*** and sophisticated
  - Increased use and reliance on security scans
  - Introduction of Ransomware Supplements
  - Subjectivities/Non-renewals based on underwriting

Coverage Considerations & Challenges

Definition of Computer System

Definition of Computer System/Network

- Would a Jackware attack trigger your policy? Are IoT Devices a part of your Computer System?

Computer System means computer hardware, software, Telephone System, firmware, and the data stored thereon, as well as associated input and output devices, data storage devices, mobile devices, networking equipment, and storage area network, or other electronic data backup facilities. The terms referenced herein include Industrial Control Systems.

Insured's Computer System means a **Computer System** leased, owned, or operated by an **Insured** or operated solely for the benefit of an **Insured** by a third party under written contract with an **Insured**.

Deeper Dive – Ransom/Jackware Coverage

Potential Limitations on Coverage

- Coverage of Business Interruption
  - Wait times/Retention/Co-insurance
- Bodily Injury/Property Damage Exclusion
  - Bricking Coverage v. Pure BI/PD
- War/State Actor Exclusions
  - Are you only covered for "targeted" attacks
- Co-Insurance/Sub-limits - Ransomware
- OFAC
- Other Insurance? Overlap/Gaps: Property and CGL Policies

TIPS AND TAKEAWAYS

Review and understand the **definition of Computer System/Network** in your cyber policy – is it broad enough?

Review and understand your **uninsured exposure** by conducting a gap analysis on your *entire* insurance portfolio.

Give notice, **promptly**, under all applicable insurance policies.

Be **proactive**! Pay close attention to changes in technology your business relies upon. Evaluate the risk and risk transfer mechanisms you have in place frequently.

CONTACT THE PANELISTS

Kelly Geary, Esq. CCP, CIPP/US,

National Practice Leader, Executive Risk & Cyber

***kelly.geary@epicbrokers.com* or 917-468-1459**

Jen Falkenholm

Vice President, National Cyber Practice

***Jennifer.falkenholm@epicbrokers.com* or 312-613-6623**

Daniel J. Healy, Esq. – Partner, Anderson Kill, LLP

***dhealy@andersonkill.com* or 202-416-6547**