Morgan Lewis

WHY ME? LEGAL IMPLICATIONS OF STATE-SPONSORED CYBERATTACKS ON CRITICAL INFRASTRUCTURE CONTROL SYSTEMS

Daniel Skees
Arjun Ramadevanahalli

May 3, 2018

State-Sponsored Hacking

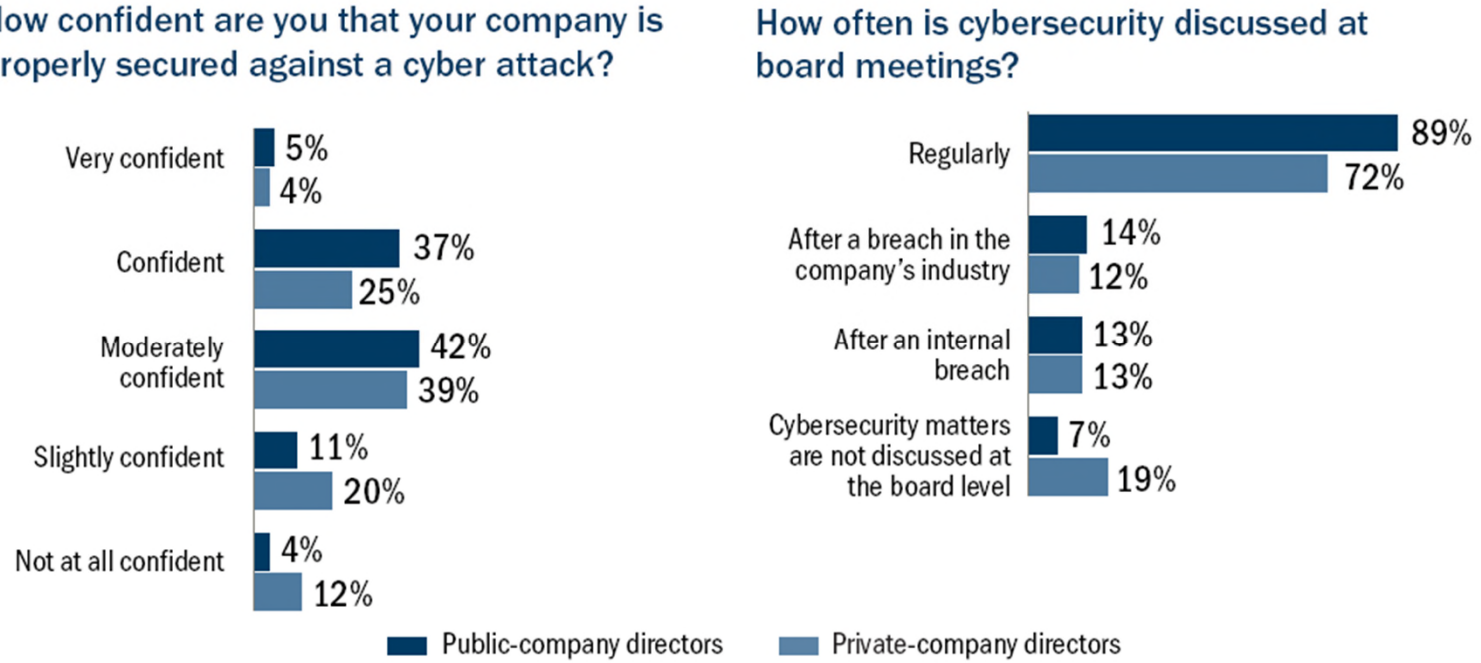
- Professional groups or individuals working on behalf of a sovereign nation state.
  - Different objectives than Black Hat hackers after financial gain and "hacktivists" seeking to make a point.
  - Often have access to more resources than freelance hackers.
- The problem with attribution:
  - Can be difficult to trace the source, even when using digital forensics.
  - Attackers can cover or spoof their digital footprints (e.g., botnets).
  - Intelligence community may not be able to publicly divulge information due to operational security, legal, or other reasons.

Why Me?

- Critical infrastructure networks are attractive targets.
  - Once compromised, they can potentially interrupt operations for essential services, causing significant financial losses.
- Corporate networks may also be targeted for economic reasons (i.e., data).
  - Sensitive business information;
  - Contracts;
  - Employee log-in credentials;
  - Employee, contractor, and customer lists and personal information; and
  - Facility information and equipment schematics.

Source: 2017 NACD Cyber-Risk Oversight Handbook

Private Industry Preparedness



Source: 2017 NACD Cyber-Risk Oversight Handbook

Critical Infrastructure Sectors

- In 2013, President Obama issued Presidential Policy Directive 21 (PPD-21), advancing the national policy on critical infrastructure security and resilience.
- PPD-21 identifies 16 critical infrastructure sectors and designates associated federal agencies as the Sector-Specific Agencies responsible for providing day-to-day engagement and specialized support capabilities in response to an incident.


Chemical


Commercial Facilities


Communications


Critical Manufacturing


Dams


Defense Industrial Base


Emergency Services


Energy


Financial Services


Food & Agriculture


Government Facilities


Healthcare & Public Health


Information Technology


Nuclear Reactors, Materials, and Waste


Transportation Systems


Water and Wastewater Systems

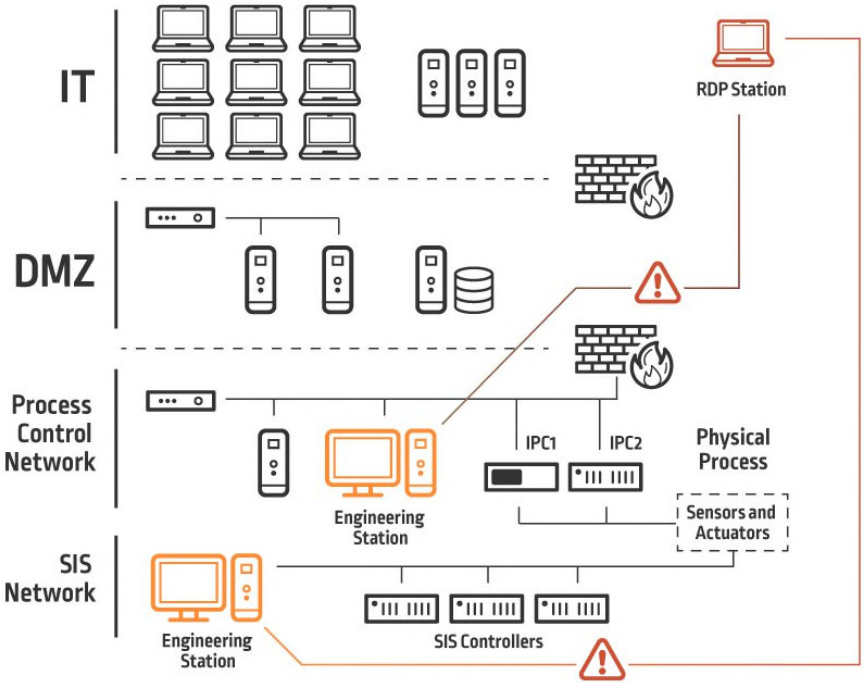
DHS/FBI Alert

- On March 15, DHS and the FBI issued a joint alert describing ongoing attacks on critical infrastructure by hackers associated with the Russian government.
  - Described as "multi-stage intrusion campaign by Russian government cyber actors" that targeted the energy, nuclear, water, aviation, and critical manufacturing sectors.
- Report alleges Russian-linked actors targeted "staging targets," such as trusted third-party supplier networks, in order to set up malware repositories, then used targets as a pivot point into "intended target" networks (government and private sector ICS operators).
- Wide range of techniques used to infiltrate target networks, ranging from sophisticated spear-phishing and open-source reconnaissance to host-based exploitation.
  - For example, planted scripts used to create local accounts disguised as legitimate backups that could be used for remote access to energy sector networks.
  - Misuse of everyday applications, such as Microsoft Word, to capture user credentials.

TRITON

- A report issued in December 2017 by cybersecurity firm FireEye reported that a new malware—dubbed "TRITON"—triggered the emergency shutdown capability of an industrial process within a critical infrastructure ICS.
- Malware targeted controllers for the Triconex Safety Instrumented System (SIS), an autonomous control system that monitors the critical systems and takes immediate actions if an operational threshold is exceeded.
- Attackers attempted to remotely control the SIS controllers, which entered a failsafe mode and "tripped" industrial processes, allowing the plant to detect and investigate the attack.
- Believed to be the work of state-sponsored attackers.

TRITON Execution



Source: Nimrod Stoler, CyberArk, Anatomy of the Triton Malware Attack (Feb. 8, 2018), https://www.cyberark.com/threat-research-blog/anatomy-triton-malware-attack/.

Atlanta Ransomware

- In March, local government systems in Atlanta were attacked using the SamSam ransomware.
  - Ransomware is a form of malicious software that enables an attacker to deny access to data, usually by encrypting it, and demanding a ransom for the data's "release".
- The attack caused disruption to a number of different government services.
  - Systems controlling court filings, water utility bill payment, sewer infrastructure requests, police reports, and airport wifi were rendered unavailable.
- No critical infrastructure facilities themselves were taken offline or significantly affected.
- However, the incident demonstrates the risk posed by poor security controls on government networks interconnected to elements of critical infrastructure.
- High cost of mitigation: Atlanta has spent over $2 million responding to an incident involving a $51,000 ransom.

And Many Others . . .

- 2017: DHS/FBI warn that foreign malicious actors (thought to be Russian) accessed corporate networks of energy companies, including a nuclear power operator.
- 2017: DHS/FBI joint technical alerts detail tools and infrastructure used by North Korea to target aerospace, financial, and other critical infrastructure sectors in the United States.
- 2015: ICS-CERT reported that the critical manufacturing sector had 97 incidents during the year, which accounted for 33 percent of all incidents reported, due to spear phishing campaign.
- 2013: Hackers believed to be operating on behalf of a state-actor managed to take partial control of the Bowman Avenue Dam near Rye Brook, New York.

WORKING WITH FEDERAL AND STATE AGENCIES

As a Critical Infrastructure Owner, You're Never Alone

Law Enforcement	• Role: Investigate and identify criminal actions, identify perpetrators, seek arrests • Examples: FBI, DOJ, State & Local Police
National Security	• Role: Identify threats, prevent or end attacks, recommend protective measures • Examples: NSA, DOD, DHS
Sector-Specific Agencies	• Role: Partnerships with private sector, provide expertise, assessments, coordination on responses • Examples: DHS, DOE, EPA, Treasury, HHS

Public-Private Partnerships and Industry Partners

- Non-Industry Specific Organizations/Agencies include:
  - Industrial Control Systems Cyber Emergency Response Team
  - National Cybersecurity and Communications Integration Center
  - Networking and Information Technology Research and Development Subcommittee of the National Science and Technology Council
  - National Institute of Standards & Technology
- Electric critical infrastructure owners
  - Electricity Subsector Coordinating Council
  - Electricity Information Sharing and Analysis Center
  - DOE Office of Cybersecurity, Energy Security, and Emergency Response

Legal Basis for Government Coordination Efforts

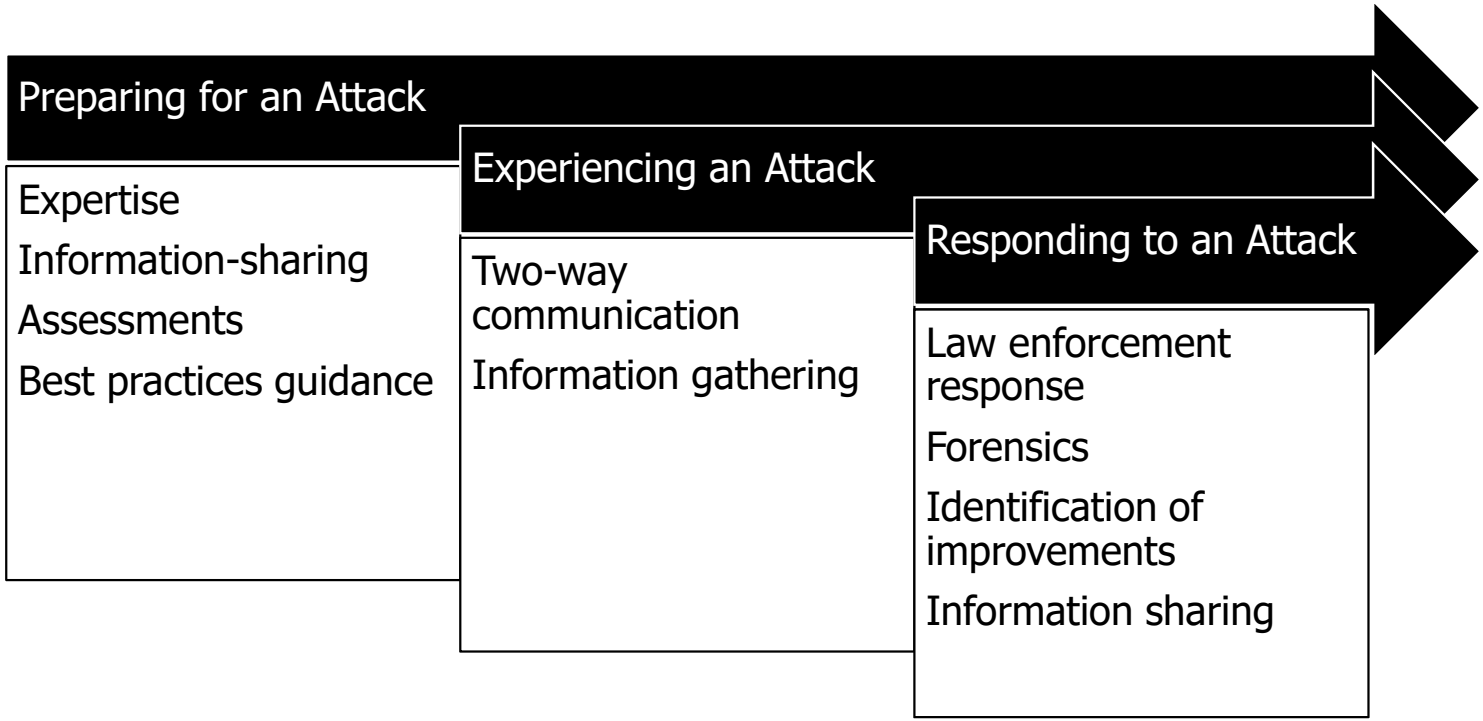
Statutory

- Computer Fraud and Abuse Act (CFAA) (18 U.S.C. 1030)
- Wiretap Act (18 U.S.C. 2511(1)(a))
- Various state computer crime laws
- Federal terrorism laws

Non-Statutory

- Presidential Policy Directive 21 (Critical Infrastructure Security and Resilience)
- National Infrastructure Protection Plan 2013
- Executive Order 13800 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)
- Executive Order 13636 (Improving Critical Infrastructure Cybersecurity)

What to Expect Through Coordination Efforts



When It's Not Optional: Grid Security Emergencies

- DOE authority for "Grid Security Emergencies" in Section 215A of the Federal Power Act (16 U.S.C. 824o-1), final rule published January 2018

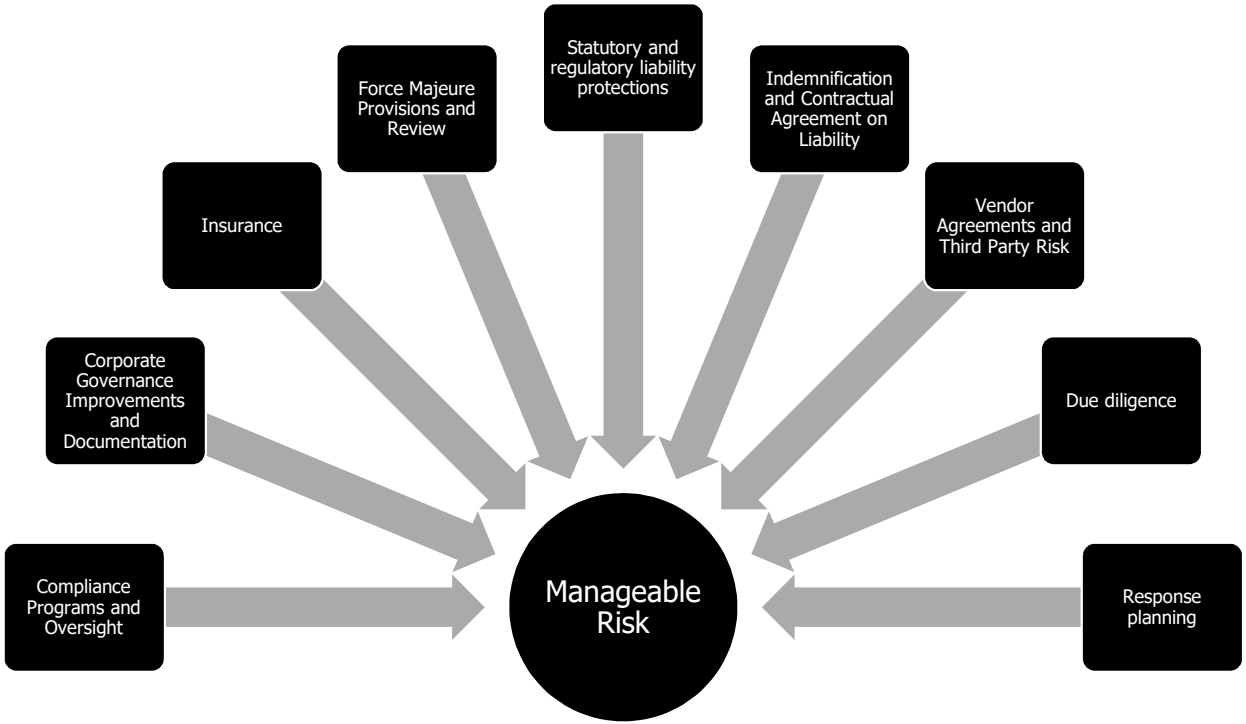
1. President determines the existence of a "grid security emergency"
2. Emergency & Incident Management Council makes recommendations
3. Appropriate stakeholder consultation under the circumstances
4. Secretary issues emergency order; information may be declassified or temporary access to classified information granted to "key personnel"
5. Order is implemented (requiring "measures necessary in the judgment of the Secretary to protect or restore the reliability of critical electric infrastructure")
6. Entities subject to order may be required to demonstrate compliance
7. Entities protected from liability for noncompliance with the Federal Power Act, Reliability Standards, and "environmental law or regulation" except for gross negligence

LEGAL ISSUES FOR CRITICAL INFRASTRUCTURE OWNERS VICTIMIZED BY STATE-SPONSORED ATTACKS

Buckets of Legal Liability (Setting Aside Costs Incurred)

Consumer Protections	•State Notification Requirements (e.g., Tex. Bus. & Com. Code §§ 521.002, 521.053) •Federal Consumer Protection (e.g., Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1))
Corporate Issues	•Securities Disclosures (SEC Corporation Finance Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011)) •Officer & Director Liability (*In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996))
Tort Liability under State Law	•Direct harms (loss of power, water, gas, telephone communications, etc.) •Indirect harms (widespread economic damages resulting from loss or misuse of critical infrastructure, *Pac. Bell v. So. Cal. Edison Co.* 208 Cal.App.4th 1400 (2012))
Contract Liability	•Security commitments in contracts with customers, vendors, counterparties •Confidentiality commitments
Mandatory Cybersecurity Obligations	•NERC Critical Infrastructure Protection Standards (18 CFR Part 39; 16 USC 824o) •Defense Federal Acquisition Regulation Supplement (DFARS) minimum security standards (48 CFR 204.73)
Loss of Regulatory Rights/Exemptions	•Franchise rights •Regulatory liability limitations (*e.g. Lee v. Consolidated Edison Co.*, 413 N.Y.S.2d 826, 828 (N.Y.Sup.Ct. 1978))

Legal Mechanisms to Handle Liability Risk



Biography

J. Daniel Skees
Washington, D.C.
T +1.202.739.5834
F +1.202.739.3001
daniel.skees@morganlewis.com

J. Daniel Skees represents electric utilities before the Federal Energy Regulatory Commission (FERC) and other agencies on rate, regulatory, and transaction matters. He handles rate and tariff proceedings, electric utility and holding company transactions, reliability standards development and compliance, and FERC rulemaking proceedings. The mandatory electric reliability standards under Section 215 of the Federal Power Act are a major focus of Dan's practice. He advises clients regarding compliance with reliability standards, and helps them participate in the development of new standards.

Biography

Arjun Ramadevanahalli
Washington, D.C.
T +1.202.739.5913
F +1.202.739.3001
arjun.Ramadevanahalli@morganlewis.com

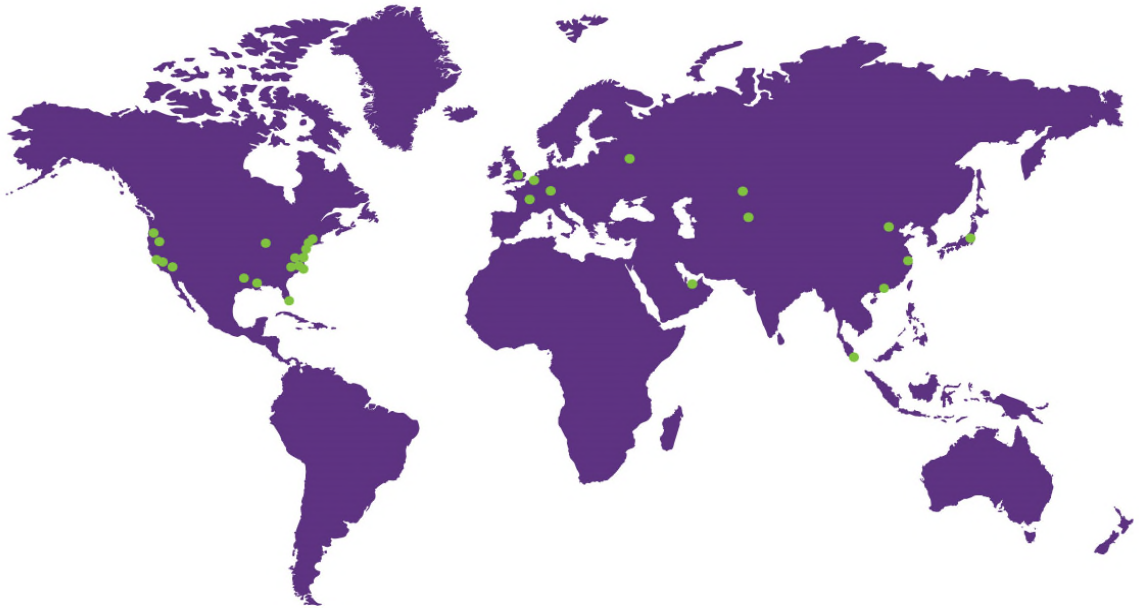
As the US energy business continues to evolve, Arjun Prasad Ramadevanahalli represents key industry participants in regulatory, transactional, and litigation matters, including investigations and enforcement proceedings. Arjun represents electric power, natural gas, and other energy industry participants before the Federal Energy Regulatory Commission (FERC), the US Commodity Futures Trading Commission (CFTC), and the North American Electric Reliability Corporation (NERC). When necessary, his representations extend to court appeals.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.

THANK YOU