ACC Association of Corporate Counsel
WASHINGTON

EVERSHEDS SUTHERLAND

Pay the ransom? Not so fast

The intersection between OFAC, ransomware and data security incident handlings

Speakers

Justin Okun
Senior Security Counsel
Chime

Paula Barrett
Co-Lead of Global Cybersecurity and Data Privacy
Eversheds Sutherland

Mark Herlach
US Head of International Trade
Eversheds Sutherland

Sarah Paul
US Head of Corporate Crime and Investigations
Eversheds Sutherland

ACC Association of Corporate Counsel WASHINGTON

EVERSHEDS SUTHERLAND

Agenda

- Protecting against and effectively responding to a ransomware attack
- OFAC implications of making or facilitating a ransomware payment to state actors, as well as other legal and practical considerations
- Critical infrastructure suppliers and contributors: supply chain, trade and sanctions implications
- The new Cybersecurity Executive Order and what it means for the private sector and federal contractors
- US and international regulations and agencies to keep top of mind *(e.g., GDPR, CCPS, CFIUS, FTC)*

Protecting against and effectively responding to a Ransomware attack

ACC Association of Corporate Counsel WASHINGTON

EVERSHEDS SUTHERLAND

Ransomware attacks – the ABCs

- What is ransomware?
  - A form of malicious software
  - Designed to block access to a company's data or other systems
  - Often through encryption

- What is a ransomware attack?
  - Hacker breaches a company's IT infrastructure, uses ransomware to encrypt data or systems
  - Demands that the company pay a ransom in exchange for a decryption key
  - Sometimes, also threatens to publicly disclose sensitive files unless the ransom is paid

- What are some possible consequences of a ransomware attack?
  - Can prevent the company from being able to conduct business operations, in whole or in part
  - Can have ripple effects on other companies or individuals

https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

Recent ransomware attacks

BUSINESS

U.S. Pipeline Cyberattack Forces Closure

Colonial Pipeline carries roughly 45% of gasoline and diesel fuel consumed on the East Coast

By Collin Eaton and Dustin Volz
Updated May 8, 2021 4:54 pm ET

The main pipeline carrying gasoline and diesel fuel to the U.S. East Coast was shut down by its operator after being hit with a cyberattack.

Colonial Pipeline Co. operates the 5,500-mile Colonial Pipeline system taking fuel from the refineries of the Gulf Coast to the New York metro area. It said it learned Friday that it was the victim of the attack and "took certain systems offline to contain the threat, which has temporarily halted all pipeline operations."

ACC Association of Corporate Counsel WASHINGTON

EVERSHEDS SUTHERLAND

WSJ

Recent ransomware attacks

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Consumer Suit Says Pipeline's Lax Security Led To Hack

By **Keith Goldberg**

Law360 (May 19, 2021, 5:23 PM EDT) -- Owners of the Colonial Pipeline have been hit with a proposed class action claiming their inadequate cybersecurity defenses led to the ransomware attack that shuttered the petroleum pipeline for several days and forced consumers to pay more at the pump.

The suit filed in Georgia federal court on Tuesday accuses Colonial Pipeline Co. of failing to implement adequate safety measures to fend off ransomware — a term that describes hacks in which ransoms are demanded in exchange for unlocking frozen networks — and other cyberattacks. The company announced May 7 that it was the victim of a ransomware attack and shut down major portions of the 5,500-mile pipeline system that transports nearly half of the East Coast's supply of diesel, gasoline and jet fuel.

Colonial Pipeline restarted operations on May 12, but the resulting disruption led to gasoline shortages and caused consumers including named plaintiff Ramon Dickerson to pay higher prices, the complaint alleges

"The defendant's unlawfully deficient data security has injured millions of consumers in the form of higher gas prices, and gasoline shortages that exist/existed, due to Colonial's decision to effectively turn off the pipeline," the complaint said.

The suit asserts a negligence claim and seeks a declaratory judgment that Colonial Pipeline's cybersecurity measures are unlawfully ineffective and need to be improved.

"If an injunction is not issued, plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another malicious ransomware hack," the complaint said. "The risk of another such hack is real, immediate, and substantial."

Federal law enforcement officials **pinned the ransomware attack** on a cybercriminal group that calls itself DarkSide and has been based in Russia and Eastern Europe. On Wednesday, Colonial Pipeline CEO Joseph Blount told the Wall Street Journal that the company paid a $4.4 million ransom.

The issue with ransomware

- Hope is not a plan
  - Instead, plan for the worst, and hope for the best
    - Resources about what to include in a plan are available from the Cybersecurity & Infrastructure Security Agency (CISA)
  - The breach, as bad as it is, may not be the **worst-case** scenario—that could be litigation, regulatory enforcement action and reputational damage, particularly if you pay a ransom
- Cybersecurity threats, including the ransomware threat, constantly evolve
  - Now, both exfiltration and encryption
  - Next step, fabrication?

The issue with ransomware

- Ransomware is often enabled through the supply chain and greatly impacts the supply chain
  - Importance of cybersecurity due diligence, vendor risk management, info sharing and insurance
  - Increases the litigation risk
- Paying ransom is not necessarily the “easy button”
  - It might not even work
  - Still need to cleanse systems and close the vulnerability
  - If personal data is impacted, still must report
  - Taxes
  - Sanctions and material support to terrorism restrictions

OFAC implications of making or facilitating a ransomware payment to state actors, as well as other legal and practical considerations

OFAC's Ransomware Advisory

- On October 1, 2020, the Office of Foreign Assets Control ("OFAC") issued an advisory to highlight the sanctions risks associated with ransomware payments (the "Advisory")

- The Advisory:
  - Warns companies that facilitating ransomware payments risks violating OFAC regulations
  - Notes that ransomware payments may also embolden cyber actors to engage in future attacks
  - Explains that OFAC has designated numerous malicious cyber actors under its cyber-related sanctions program and other sanctions programs
  - States that license applications involving ransomware payments will be subject to a presumption of denial
  - Encourages companies to report ransomware attacks to law enforcement
  - Reiterates that OFAC encourages companies to implement risk-based sanctions compliance programs

In general, the Advisory makes clear that exigent circumstances do not relieve companies of their sanctions compliance obligations and emphasizes that OFAC may impose civil penalties based on strict liability

Takeaways from OFAC's Ransomware Advisory

- The FBI recommends against paying the ransom
- Consider the real risk of sanctions violations associated with paying a ransom
- Do not pin your hopes on obtaining a license involving a ransomware payment
- Take steps to prevent ransomware attacks from occurring in the first place
- Develop procedures for conducting sanctions due diligence of the attacker
- Include this sanctions risk in your ransomware crisis plan, and make employees aware of it
- Cooperate with law enforcement, both during and after a ransomware attack

Critical infrastructure suppliers and contributors: supply chain, trade and sanctions implications

ACC Association of Corporate Counsel WASHINGTON

EVERSHEDS SUTHERLAND

Vulnerability has many faces

- Time to step back and adopt a holistic approach
- Ask "What if . . . ?"
- Identify choke points and potential weaknesses
- Anticipate how a state actor or rogue group can gain leverage
- Ransomware attacks are simply one manifestation of larger set of vulnerabilities
- International trade risk has multiple dimensions
- Recent US government actions illustrate breadth of the problem
- Proactive steps required to manage risk

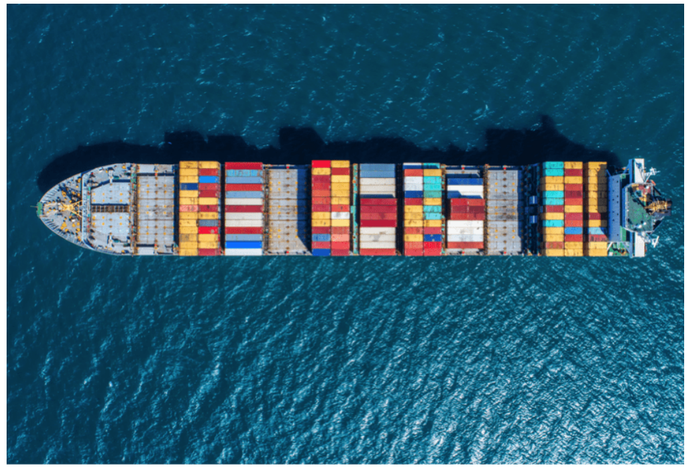
https://www.gettyimages.com/detail/video/hacker-man-typing-code-at-laptop-stock-footage/1089071324

Scope of critical infrastructure expanding

- What is "critical" has evolved
- Points of vulnerability now exist in new contexts
  - Defense and energy are no longer the only concerns
  - Critical technologies and sensitive personal data
- Government controls are becoming more pervasive
  - Restrictions on exports of technology
  - Restrictions on adversaries equipment within critical infrastructure
  - Cheaper is not always better
  - Balance between commercial and national security interests
  - Increased scrutiny of foreign investment and access to critical technologies reflected in the new CFIUS process
- Holistic approach essential to identify potential threats and develop robust systems

Supply chains – the demise of "just in time"

- Geographic vulnerability
- Dependency
- Timing considerations
- State Actor implications
- Importance of proactive approach and ongoing risk analysis
  - Plan for how you will respond (or even find out about) your vendors being subject to a ransomware attack
- Constructive and defensive perspectives are both important
  - Pros and cons of given suppliers
  - Hedge your bets
  - Monitor sanctions and other international trade developments
  - Rules can change overnight
  - Commercial opportunities for Western companies



https://www.universalcargo.com/how-much-cargo-can-the-largest-shipping-container-ship-really-hold/

https://www.rechargenews.com/transition/hydrogen-can-power-virtually-all-container-ships-crossing-the-pacific/2-1-767073

The new Cybersecurity Executive Order and what it means for the private sector and federal contractors

ACC Association of Corporate Counsel WASHINGTON

EVERSHEDS SUTHERLAND

Cybersecurity developments

President Biden's Executive Order on Cybersecurity – May 12, 2021

- It is not legislation, but it binds federal departments and agencies, impacts federal contractors, leverages the market power of the government, and aims to lead by example

Removes barriers to threat information sharing

Implements stronger cybersecurity standards
- MFA
- Encryption

Cybersecurity safety review board

Software supply chain security

Standardized Incident Response Plan

End-point detection

Event log requirements

White House follow-up memo – June 2, 2021

- Additional recommendations for the private sector on preparing for ransomware with additional steps

Back up and test

Update and patch promptly

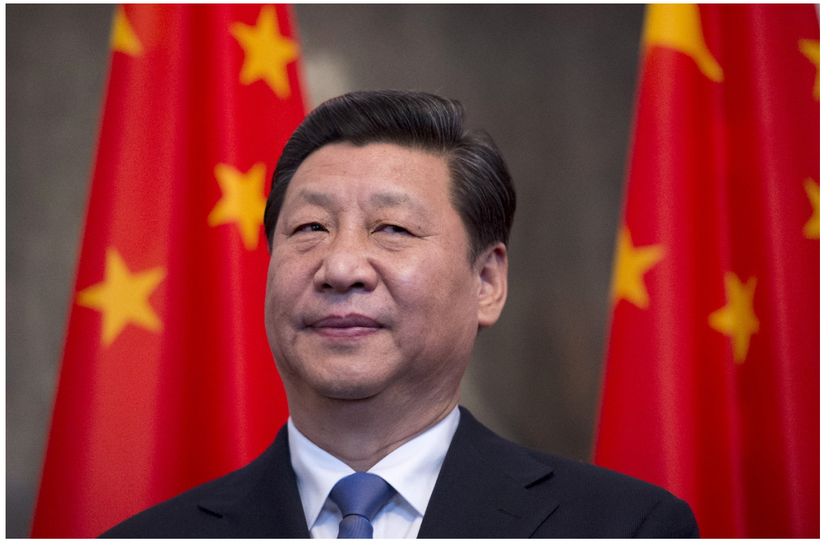
Third-party pen tests

Segment networks

US and international regulations and agencies to keep top of mind *(e.g., GDPR, CCPA, CFIUS, FTC)*

Things to keep top of mind

- Increasing concern over international dependency
  - Pandemic demonstrated serious implications of this concern
  - Buy America/onshoring trend in United States
  - China's efforts to become less dependent on US technology
  - China-US competition
- Domestic control over critical infrastructure
- Foreign investment restrictions on the rise globally
- Access to knowledge and critical technology a new FDI focus
- SOEs present particular challenges
- Disruptive capabilities of state actors
- Ransomware attacks just one manifestation of new challenges to "business as usual"



https://time.com/4284795/panama-papers-xi-jinping/

Questions?

Contact our speakers

PaulaBarrett
Co-Lead of Global Cybersecurity and Data Privacy
paulabarrett@eversheds-sutherland.com
+44 207 919 4638

Mark Herlach
US Head of International Trade
markherlach@eversheds-sutherland.com
+1 202 383 0172

Sarah Paul
US Head of Corporate Crime and Investigations
sarahpaul@eversheds-sutherland.com
+1 212 301 6587

ACC Association of Corporate Counsel WASHINGTON

EVERSHEDS SUTHERLAND