Legal Guide to Ransomware
To Pay or Not to Pay

Mark D. Rasch

May 16, 2022

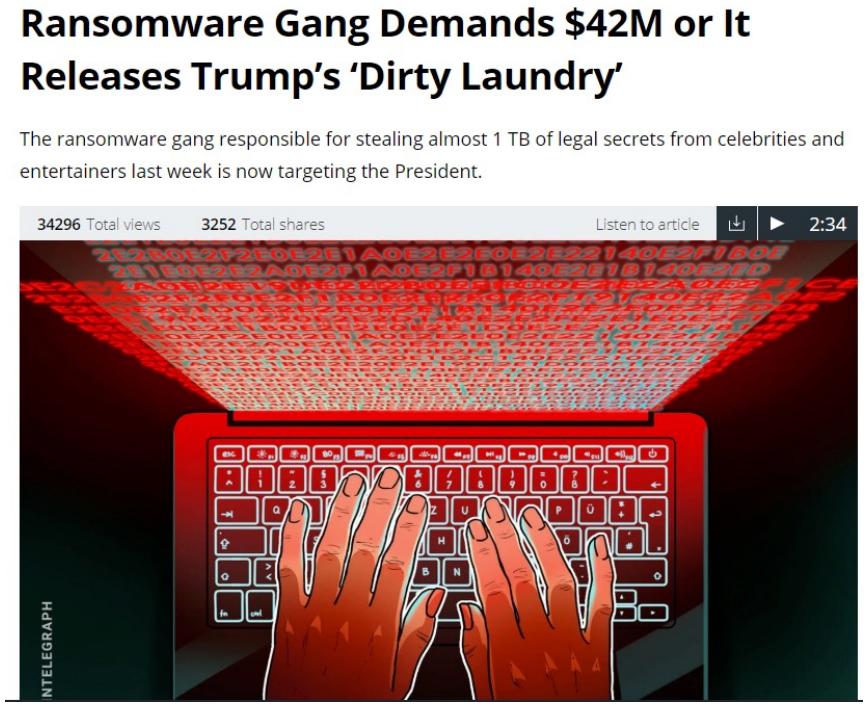
6:30 PM

MarkRasch@Unit221B.com

(301) 547 6925

Ransomware vs. Extortionware

- Most ransomware involves ACCESS to data or networks
- Extortionware is broader – may involve THEFT (and return) of data
- Extortionware may include theft and threat to release information
- Extortionware may include threat to release vulnerabilities
- dDOS threats have characteristics of both



Is A Ransomware Attack a Data Breach?

- What does the LAW say?
  - Breach is the unauthorized acquisition of certain data
    - PII, PHI, SPI
    - Classified Information
    - Confidential Information (by contract)
  - Breach under contract
    - NDA's
    - Other agreements
- Is data "acquired?" in Ransomware?
- Define "breach" and define "incident"

HIPAA Data Breach Rule 45 CFR §§ 164.400-414

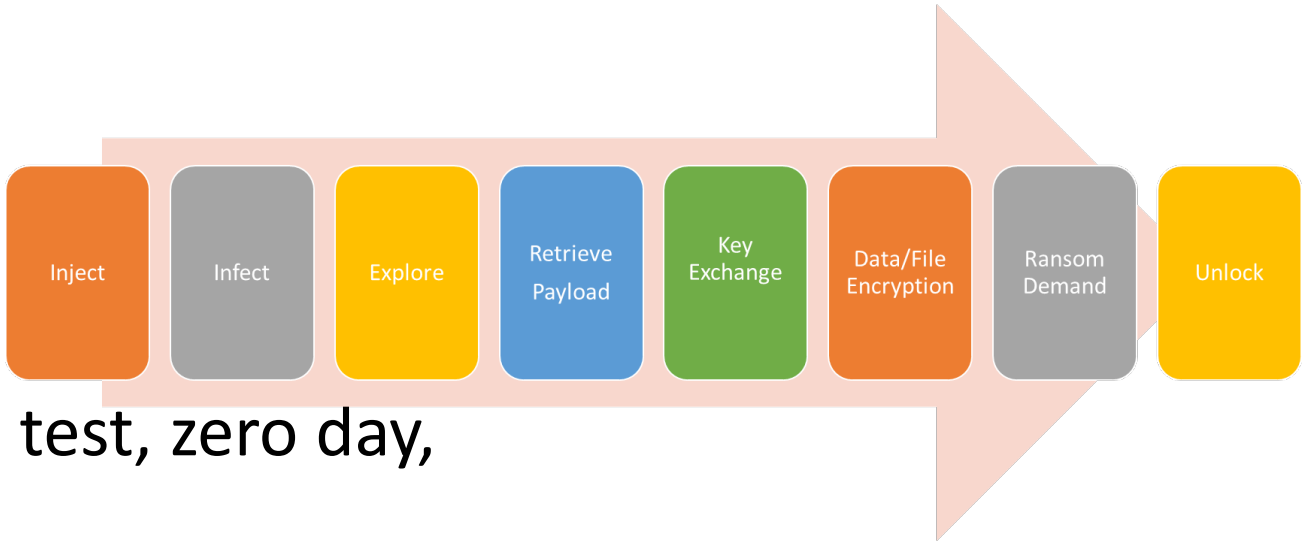
- A breach is, generally, an **impermissible use** or disclosure under the Privacy Rule that **compromises the security** or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

  - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
  - The unauthorized person who used the protected health information or to whom the disclosure was made;
  - Whether the protected health information was actually acquired or viewed; and
  - The extent to which the risk to the protected health information has been mitigated.

Extortion Schemes:

- Double extortion schemes
  - Take sensitive data from the targeted networks
  - encrypt the system files
  - demanding ransom.
  - threaten to publish or sell the stolen data if the victim does not pay the ransom.
- Use the system breach to target additional parties related to the initial victim like business partners and customers as follow-on targets.
- Then threaten to expose original victim as source for follow on

How it Works



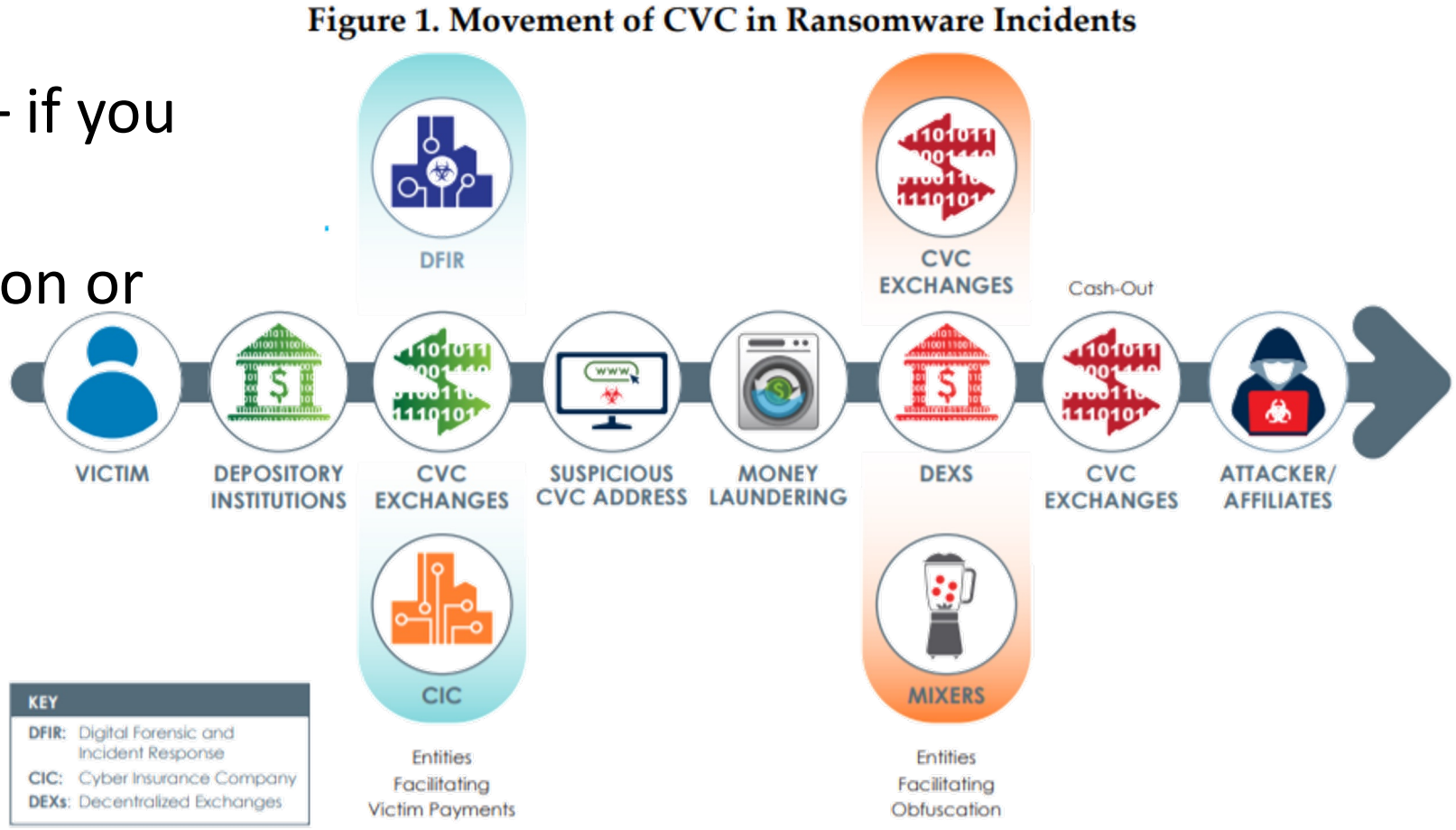
1. Get in (phishing, pen test, zero day, credential theft)
2. Inject lure into network
3. Examine network to select target(s)
4. Phone home – to get malicious payload
5. Exchange encryption Keys
6. Encrypt files or shares or network device
7. Demand ransom, and if paid…
8. Unlock files (provide unlock key)

Targets of Ransomware

- Everyone is a potential target… but
- Time critical applications
  - Healthcare
  - Manufacturing
  - Financial Services
- Mission Critical Applications
  - Municipalities
  - State Agencies
- Biggest factor – ARE THEY LIKELY TO PAY

Ransomware Options

- Repair and rebuild
- Restore from backup – if you have backups
- Ransomware inoculation or diversion
- Hack or locate the key
- Negotiate or pay
- Follow the money



Legal Issues in Ransomware/Extortion

- Is it covered by insurance – “theft or destruction?”
- Is a ransomware attack a reportable data breach?
- Is a ransomware attack a reportable data incident?
- Is payment of ransom legal?
  - OFAC/SDN
  - TWEA
  - Material support/conspiracy/accessory after the fact
  - AML/KYC and Money Transfer Agent Law
  - SAR
- Is it legal to use an agent to transfer funds?

Legal Issues Before Ransomware Hits

- Supply chain of data
- Is ransomware a “force majeure”
- How does ransomware impact Service Level Agreements and duties to perform
- To whom does the duty of due care run (the Palzgraf issue)
- What standard of care do you owe, and do they owe to you?
- What kind of insurance to get, from whom and what language to look for
- Duty to cooperate in investigation and share data?

Use the Force (Majeure)

- Force Majeure. A Party shall not be considered to be in default or breach of this Agreement, and shall be excused from performance or liability for damages to any other party, if and to the extent it shall be delayed in or prevented from performing or carrying out any of the provisions of this Agreement, arising out of or from any act, omission, or circumstance by or in consequence of any act of God, labor disturbance, sabotage, failure of suppliers of materials, act of the public enemy, war, invasion, insurrection, riot, fire, storm, flood, ice, earthquake, explosion, epidemic, breakage or accident to machinery or equipment or any other cause or causes beyond such Party's reasonable control, including any curtailment, order, regulation, or restriction imposed by governmental, military or lawfully established civilian authorities, or by making of repairs necessitated by an emergency circumstance not limited to those listed above upon the property or equipment of the Party or property or equipment of others which is deemed under the Operational Control of the Party. A Force Majeure event does not include an act of negligence or Intentional Wrongdoing by a Party. Any Party claiming a Force Majeure event shall use reasonable diligence to remove the condition that prevents performance and shall not be entitled to suspend performance of its obligations in any greater scope or for any longer duration than is required by the Force Majeure event. Each Party shall use its best efforts to mitigate the effects of such Force Majeure event, remedy its inability to perform, and resume full performance of its obligations hereunder.

To Pay or Not to Pay… That is the Question

- ITAR/OFAC
- KYC
- AML
- 18 USC 1956 – Money Laundering
- Aiding and Abetting
- Material Support
- Conspiracy – 18 USC 371
- Other crimes

Ransomware Legal Consideration OFAC

- Responsible for enforcing US and some UN Sanctions Regimes
- Against people, countries, and entities
- AND some IP addresses or hacker groups
- Prohibited to engage in “transactions” with these entities
- November 9, 2021 advisory on facilitating ransomware payments
- https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

OFAC May Prosecute Those Who Pay

- **OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was**

Aiding and Abetting

- 18 USC 2
  - 18 U.S. Code § 2 - Principals
  - (a)Whoever commits an offense against the United States or **aids, abets,** counsels, commands, **induces** or procures **its commission, is punishable as a principal.**
  - (b)Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal.

Conspiracy

- 18 U.S. Code § 371 - Conspiracy to commit offense or to defraud United States
- If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.

Money Laundering

- 18 U.S. Code § 1956 Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States—
- (A)with the intent to promote the carrying on of specified unlawful activity; or
- (B)knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part—
- (i)to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or
- (ii)to avoid a transaction reporting requirement under State or Federal law,

State Money Transmitter Laws

- Section 641(1) of the NY Banking Law
- "No person shall engage in the business of selling or issuing checks, or engage in the business of receiving money for transmission or transmitting the same, without a license therefor obtained from the superintendent as provided in this article, nor shall any person engage in such business as an agent, except as an agent of a licensee or as agent of a payee…."

Ransomware Payment Consideration (Practical)

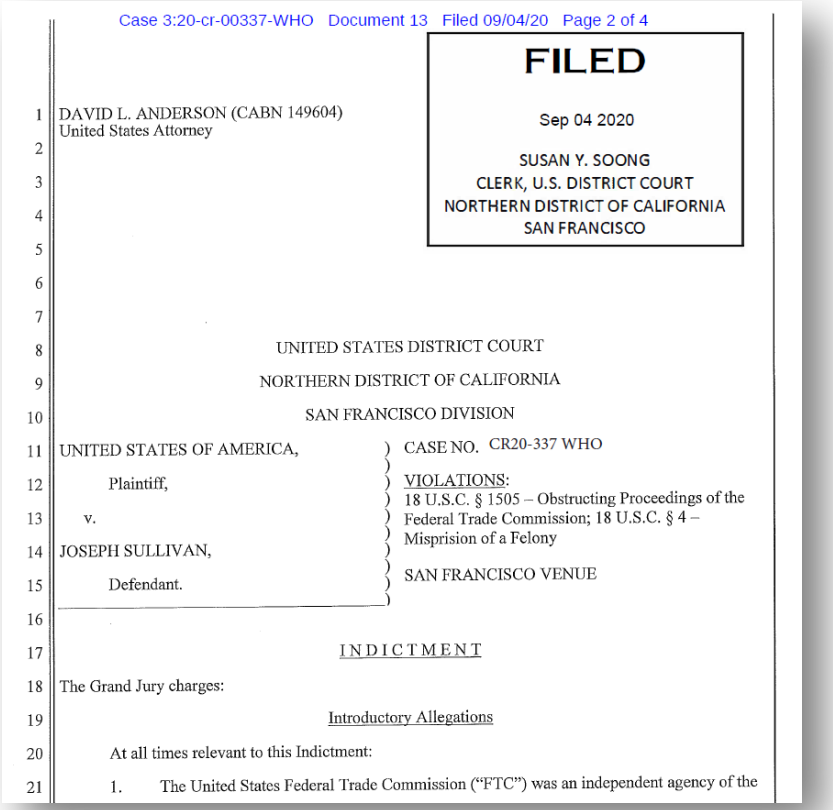
- Do you have access to cryptocurrency?
- Do you have access to cash to convert to cryptocurrency?
- Do you have insurance?
- Bitcoin tumbling
- Escrow agent?
- Threat actor engagement?
- Key testing?

Scenario

- Hacker attacks system, takes data which is NOT PII (trade secret data, emails, or encrypted PII, etc.)
- Threatens to release the data as well as the vulns and exploits unless you pay.
- You negotiate a payment under corporate bug bounty program provided that you get assurances that the data has not and will not be disclosed to third parties.
- Legal issues??

USA v. Sullivan (Uber CISO)

- Extortionware case – Uber hacked, data taken, but not disseminated
- Uber CISO – former DOJ Cybercrime prosecutor negotiates return of data and all copies
- Pays hackers from bug bounty program.
- Does not disclose the “hack”
- 18 USC 4 – misprison of a felony – knowledge of a felony conceals and does not report.



Case 3:20-cr-00337-WHO Document 13 Filed 09/04/20 Page 2 of 4

FILED
Sep 04 2020
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

DAVID L. ANDERSON (CABN 149604)
United States Attorney

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,
Plaintiff,
v.
JOSEPH SULLIVAN,
Defendant.

CASE NO. CR20-337 WHO

VIOLATIONS:
18 U.S.C. § 1505 – Obstructing Proceedings of the Federal Trade Commission; 18 U.S.C. § 4 – Misprision of a Felony

SAN FRANCISCO VENUE

INDICTMENT

The Grand Jury charges:

Introductory Allegations

At all times relevant to this Indictment:

1. The United States Federal Trade Commission (“FTC”) was an independent agency of the

Active Response?

- Ping back
- Hack back
- Destructive code?
- Infrastructure attack?
- Legality, efficacy, morality
- Collateral damage

Ransomware Risk Mitigation (Insurance)

- Check your policy
- Check your policy again
- Data breach policies likely will not cover
- Cybersecurity policies may cover
- Make sure you have coverage for
  - Data loss
  - Data loss of accessibility
  - Costs of investigation/response
  - Costs of data recovery/rebuilding
  - Costs of ransom payments
  - Extortion and publicity costs
- May be covered by publicity policies, KRE policies, GCL policies

Future of Ransomware

- Newer and evolving threats
- Including mobile and IoT
- More persistent and more virulent
- Attacking cloud based networks (more bang for their buck)
- More class action litigation
- COVID-19 makes networks (and people) brittle

Key Takeaways

- Have the RIGHT insurance
- Review ALL your contracts
- Have forensics, IR, and threat intelligence company on retainer
- Make friends in law enforcement
- Know your broker
- Backup data properly (with procedures to restore)
- Have access to cryptocurrency
- Test your IR plan (you do have an IR plan, right?)

For More Information

Mark D. Rasch, Esq.
MarkRasch@unit221B.com
(301) 547 6925