1

Melissa K. Ventrone

Esq. CIPP, Member

Clark Hill, PLC

- Leads a team of attorneys, forensic investigators, and crisis experts delivering 24/7, end-to-end breach response support
- Managed 5,000+ breaches for clients ranging from small businesses to F500 companies
- Successfully defended numerous organizations in regulatory investigations involving various privacy practices or data breaches
- Delivers training, simulation exercises, and action plans compliant with state, federal, and international laws
- Distinguished 21 years of service in the Marine Corps Reserve

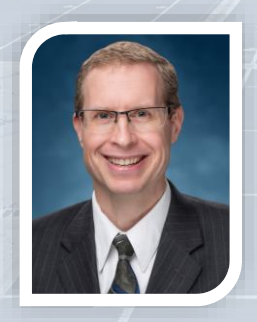
AEGIS 2023
POLICYHOLDERS' CONFERENCE

2

David Batz

Managing Director

Edison Electric Institute



- Leads EEI cyber and infrastructure security efforts
- Leverages a decade of energy regulatory and policy experience
- Facilitated the development of Cyber Mutual Assistance – a program for electric and natural gas companies in North America
- Authored various articles and presented at numerous events domestically and internationally on securing critical infrastructure, industrial systems as well as security baseline and standards topics for prominent industry associations including NIST, the National Academies of Sciences, United States Energy Association and the World Economic Forum
- 20 years experience working for an electric company

AEGIS 2023 POLICYHOLDERS' CONFERENCE

3

Imagine

someone trying to break into your house.

Now imagine it

60,000 times a day.

AEGIS 2023 POLICYHOLDERS' CONFERENCE

4

THE HISTORY OF RANSOMWARE

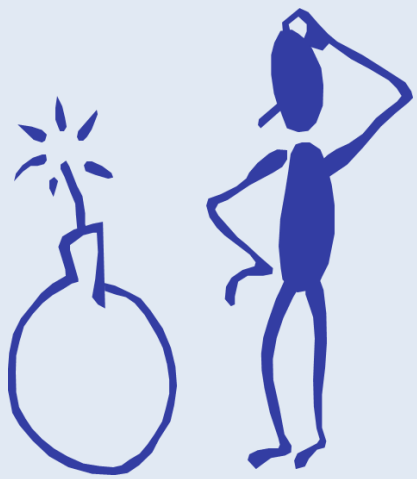
- Earliest Example 1989
- Payment in crypto currency 2013
- Ransomware as a Service 2015
- Migration from single systems to entire networks (Big Game Hunting) 2018
- Encryption of Backups 2019
- Extortion 2019

AEGIS 2023 POLICYHOLDERS' CONFERENCE

5

RANSOMWARE V. EXTORTIONWARE

- What is Ransomware
  - Encryption in place
  - Goal to lock down critical business systems
  - May involve exfiltration of data
- What is Extortionware
  - Exfiltration of data, demanding a ransom to not release it
  - Sell data to other threat groups
  - Weaponize data with customers



AEGIS 2023 POLICYHOLDERS' CONFERENCE

6

DISCOVERY OF A RANSOMWARE OR EXTORTIONWARE ATTACK

- Company receives email from someone purporting to have your data
- IT notices odd or suspicious system activity
- IT receives reports from users of trouble accessing systems and applications
- Company learns its information is posted on the dark web

AEGIS 2023 POLICYHOLDERS' CONFERENCE

7

WHAT DO WE DO?!

A. Call your cyber insurance carrier immediately.

B. Take your systems offline to prevent or mitigate damage.

C. Trigger your incident response plan.

D. Call the FBI or local law enforcement.

AEGIS 2023 POLICYHOLDERS' CONFERENCE

8

WHO IS RESPONSIBLE? FOR WHAT?

- What does your IRP say about?
  - Contacting FBI
  - Contacting insurance
  - Engaging outside counsel
  - Engaging computer forensic investigators, or IT restoration assistance
  - Engaging external crisis communication
- What if someone is on vacation?
- How often do you update the contact information?
- Testing is key (reoccurring theme)

AEGIS 2023 POLICYHOLDERS' CONFERENCE

9

TIME MATTERS

- Follow Incident Response Plan
- Notify insurance and engage Outside Counsel
- Outside Counsel will:
  - Engage computer forensic investigators
  - Ransomware negotiator
  - Crisis communications, if necessary
  - Determine regulatory notification requirements
- What about law enforcement?
- What is insurance involvement at this point?

AEGIS 2023 POLICYHOLDERS' CONFERENCE

10

TO PAY OR NOT TO PAY

- Myths regarding paying a ransom
  - Criminals don't honor promises
  - If you pay, will be hit again
  - Decryption key won't work
  - They sell your data
- Process for verifying payment is an option
  - Proof of life
  - Sanctions check
  - Virtual currency broker
- Can negotiation demand
- Ultimately a business decision
- Management/board should discuss approach to ransomware before attack

AEGIS 2023 POLICYHOLDERS' CONFERENCE

11

PROCESS FOR PAYING A RANSOM

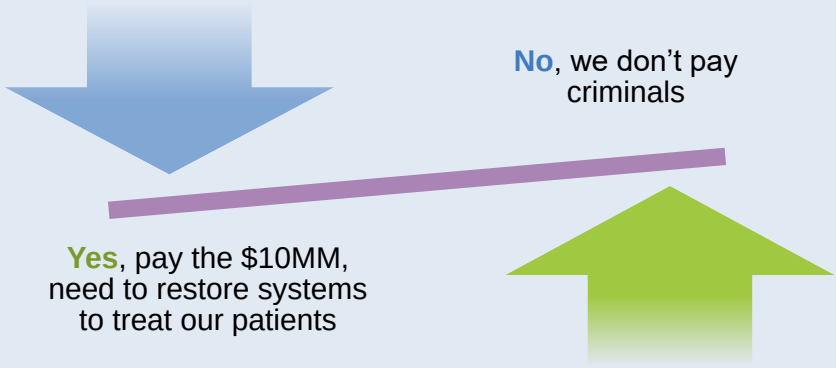
- Outside counsel engages company that communicates with threat group
  - Company contacts threat group, verifies ransom demand and payment terms (timeline, currency, etc.)
  - Company requests "proof of life" from threat group
  - Company negotiates ransom demand
- Proof of life includes decryption key and "proof" data was taken, if applicable
- Payment of ransom
  - Obtain clear sanctions/OFAC check
  - File FBI IC3 report, if not already completed
  - Approval of insurer/company
  - Work with virtual currency broker, who will purchase virtual currency and fund wallet
  - Ransom is paid

AEGIS 2023 POLICYHOLDERS' CONFERENCE

12

DOES YOUR RESPONSE CHANGE?

Demand is $10 Million; do you pay or not?

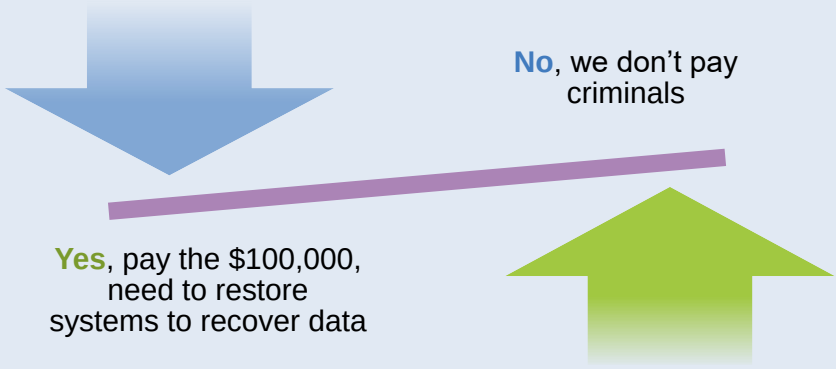


AEGIS 2023 POLICYHOLDERS' CONFERENCE

13

DOES YOUR RESPONSE CHANGE?

What if the demand is $100,000? Do you pay or not?



AEGIS 2023 POLICYHOLDERS' CONFERENCE

14

THREAT ACTOR TACTICS CHANGING

- More Ransomware as a Service (Raas) attacks
- Less consistency with threat actors
- More aggressive with negotiations
- Will weaponize data

AEGIS 2023 POLICYHOLDERS' CONFERENCE

15

INVESTIGATION PROCESS

- Forensic investigation takes time
  - Identifying impacted systems
  - Collecting logs and relevant forensic evidence
  - Process may be lengthy, depending on scope of incident
  - Identification of compromised data usually time consuming, if not impossible to determine forensically
- Investigation to determine compromised data
  - Anti-forensics can impact investigation
  - Data is usually unorganized, making identification difficult
  - Data compromise triggers legal obligations

AEGIS 2023 POLICYHOLDERS' CONFERENCE

16

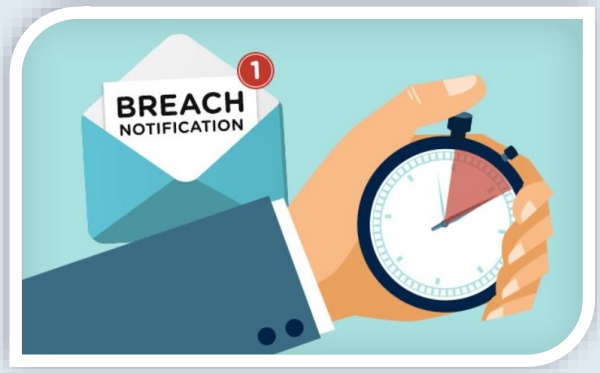
DATA ANALYSIS

- Usually need to hire a third-party vendor to review the data
- Can take months, depending on the amount and type of data
- If you don't pay the ransom, data will be posted on the dark web or sold to another group

AEGIS 2023 POLICYHOLDERS' CONFERENCE

17

NOTIFICATION REQUIREMENTS



- Contractual notice
- Statutory notice
- Business notice
- Mend and repair relationships

AEGIS 2023 POLICYHOLDERS' CONFERENCE

18

LESSONS LEARNED

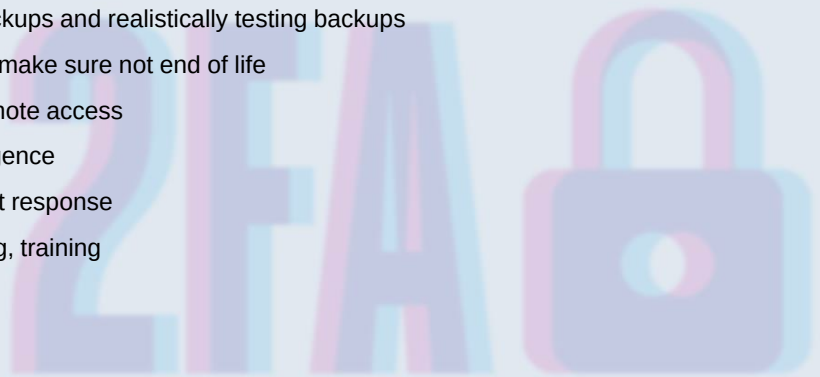
- Preparation is key
  - Create incident response plan – in addition to IT, management must be included
  - Discuss response priorities and ransomware approach
  - Identify external resources and pre-negotiate contracts
  - Understand organizations approach to ransomware
  - Think about logistics
- Training is important
  - Test the plan – test different portions, keep the plan updated
  - Ensure everyone understands their roles

AEGIS 2023 POLICYHOLDERS' CONFERENCE

19

BEST PRACTICES

- Segmenting backups and realistically testing backups
- Patch systems, make sure not end of life
- MFA on any remote access
- Vendor due diligence
- Practice incident response
- Training, training, training



AEGIS 2023 POLICYHOLDERS' CONFERENCE

20

AVOID COMMON RESPONSE PITFALLS

- Don’t panic (no really, don’t panic)
- Keep a physical copy of plan and update it
- Follow your plan
- Bring in the right team
  - Notify your carrier
  - Consult with experienced privacy counsel
  - Identify qualified computer forensic firm
- Be mindful of communications

21

22

PRESENTER CONTACT INFORMATION

Melissa K. Ventrone

Clark Hill, PLC

+1 **312.360.2506** (office)

+1 **312.517.7572** (fax)

mventrone@clarkhill.com

www.clarkhill.com

David Batz

Edison Electric Institute

+1 **202.508.5586** (office)

dbatz@eei.org

www.eei.org

CH Incident Response 24/7 Hotline:

(877) 912-9470

AEGIS 2023 POLICYHOLDERS' CONFERENCE

23

AEGIS

24