RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SEM-M03G

Ransom: A Real-World Case Study in Data Theft, Forensics and the Law

R Jason Straight

Sr. VP, Cyber and Privacy Risk
Chief Privacy Officer
UnitedLex Corp.

Objectives

- Expose the limits of what you can accomplish with forensics
- Warn against the lure of false leads and red herrings
- Examine the push-and-pull of working with law enforcement
- Explore challenges of engaging with an attacker in real time
- Describe the impact a major IR effort can have on a company
- Present guidance for engaging with executives and board

Set up and Background

- Case study is a “composite” of several cases I have worked but largely based on one matter
- Engaged by outside counsel to assist with a potential data breach incident
- All work performed at direction of counsel and subject to attorney-client privilege and work product protection

Set up and Background

- US-based, publicly traded marine products manufacturing company
- 20,000 Employees, 10,000 Contractors, 6 Countries 50,000 Hosts on network
- MSSP providing 8X5 network security monitoring
- Highly decentralized IT management

PEQUOD INDUSTRIES

RSAConference2019

Message from the Deep

The hunt begins

DAY ZERO

From: *harpooned@hmamail.com*

Sent: *Thursday, November 15, 2018 1:45 AM*

To: *Carl A Habertson [CEO, MD INDUSTRIES]*

Subject: *Time for some payback*

Ahoy! Congratulations on your Q3 earnings- very impressive! I'm sure your board and investors are very happy with the tremendous financial success of the company. But as we all know, it doesn't take much for things to take a turn for the worse – especially at Pequod. I have some information that could sink your company fast. But don't worry, I'm not planning to put it to use as long as you do what I ask. Attached is a small sample of what I have. Rest assured there is a LOT more where that came from. I'm sure you don't want this stuff to show up on Wikileaks! I will be in touch soon with instructions for you to follow. Have a great day!

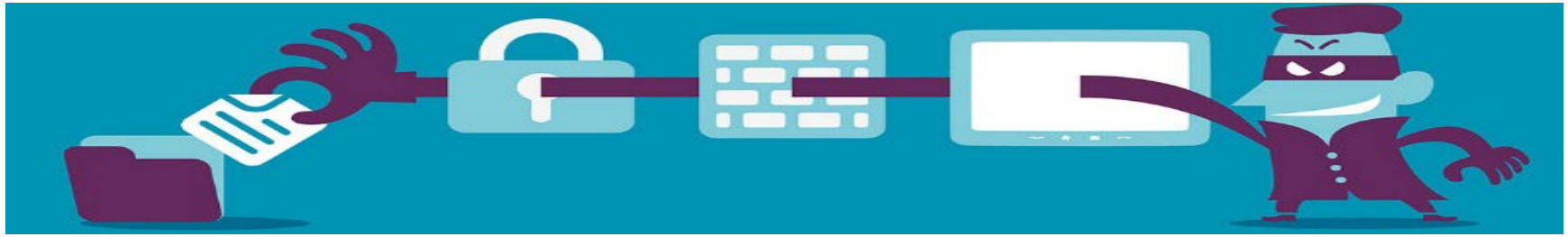
Sincerely,

Harpooned

DAY ZERO

ATTACHMENT IS PDF WITH IMAGES OF FOLLOWING:

- *Results of a ISO 27001 Audit from 2016*
- *5 Employee W-2 Forms (all from Sept. 2017)*
- *3 Slides from Internal PPT deck analyzing a proposed acquisition– dated Dec. 2017*
- *3 Variable Annuity Death Claim Notification Forms*



DAY ZERO

Initial Questions

- Anything odd about this message?
- Should you contact law enforcement?
- Should you reply to the message?
- Do you want to engage outside counsel, forensics firms or communications firm?
- Who should be notified of incident internally?
- Have any statutory or other notification requirements been triggered?
- Is there a need to notify cyber-insurance carrier?
- Document preservation obligations?

DAY ONE – SIRP TEAM MEETING

Key Investigative workstreams

- Identify source documents, locate on network and conduct access audit
- Assess potential impact if documents were released
- Determine whether there is an active compromise
- Monitor open, deep and dark web for documents and/or references to attack
- Explore potential insider involvement

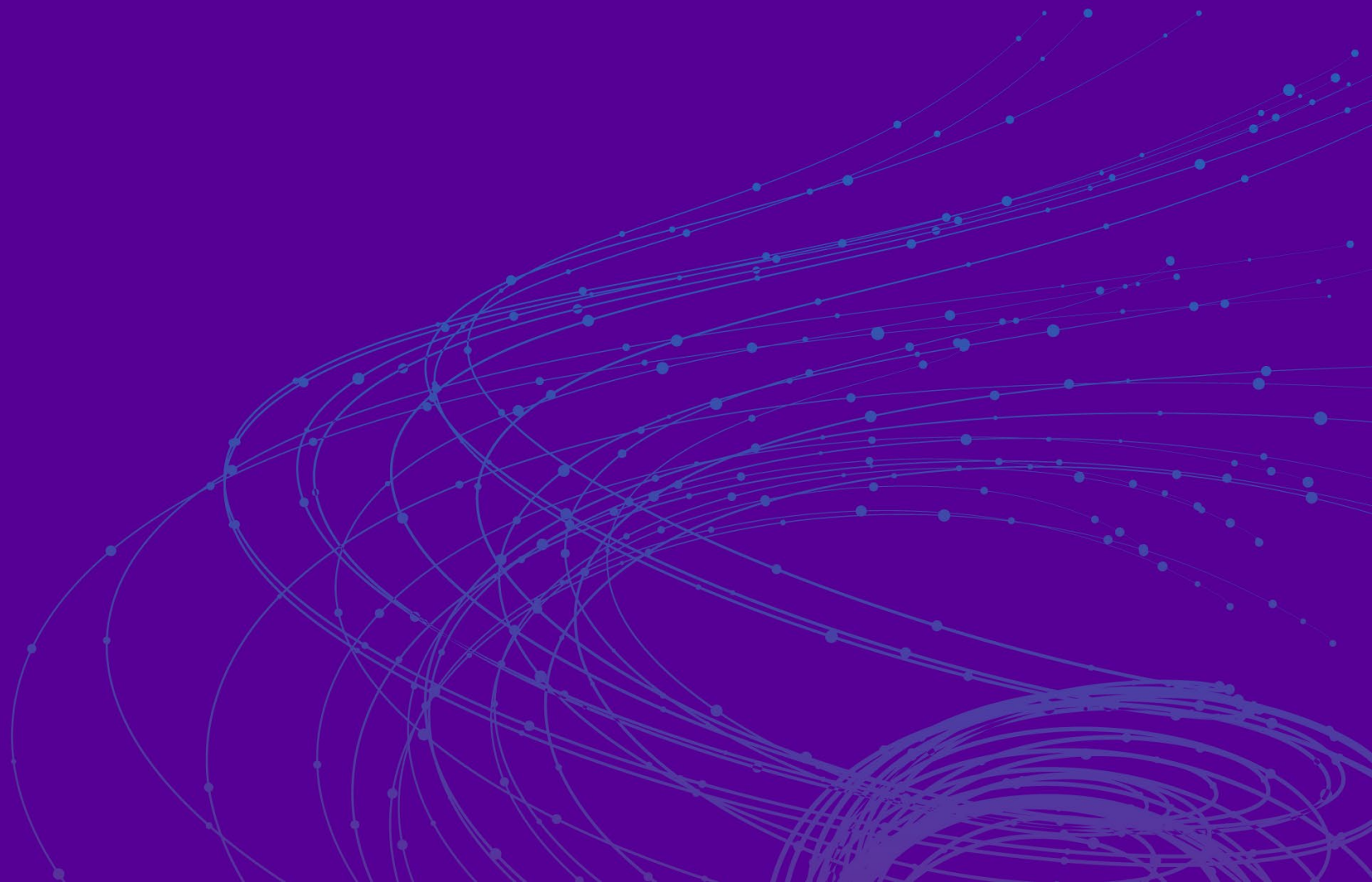
DAY 2 – INVESTIGATION UPDATE

Preliminary Investigative Results

- Source documents identified – each on different source system.
- Results of compromise assessment, inconclusive. BUT, some unusual communications with an IP address in a “bad neighborhood”
- No reference to documents found online (open, deep or dark).

RSAConference2019

The Demand



DAY 5 – YOU'VE GOT MAIL

From: *harpooned@hmamail.com*

Sent: *Tuesday, November 20, 2018 10:30 PM*

To: *Carl A. Habertson*

Subject: *Time to pay*

Hello. I hope by now you have had a chance to look at the package I sent last week and know that I am very serious. You are probably wondering what I want. I've been thinking about that too. I know you've got plenty of money so that shouldn't be an issue. I will want to be paid in Bitcoin though so you will need to go buy some of that. I want 2000 BTC deposited into two different wallets (1000 BTC in each) with the following IDs:

1B2S4Nf8jD3fshHodzuYhlamoQsQaZEcZ

1B2S4Nf8jD3gtIpuOeyklAndRtMyywFBVcXvv

I will give you one week from today to make the deposits – or I start releasing info.

Sincerely,

Harpooned

DAY 6 – FBI VISIT

DAY 6 – FBI VISIT

FBI Meeting Summary:

- ➢ Email address untraceable so far, not associate with any other known attacks.
- ➢ Bitcoin wallets also unknown to law enforcement
- ? FBI wants to know about any “difficult” employee separations in recent months
- ? FBI asks company to respond with offer to make a down payment to buy some time.
- ? FBI asks company to include a tracking beacon in attachment sent to attacker
- ? FBI asks for an update on compromise assessment and overall investigative progress

---

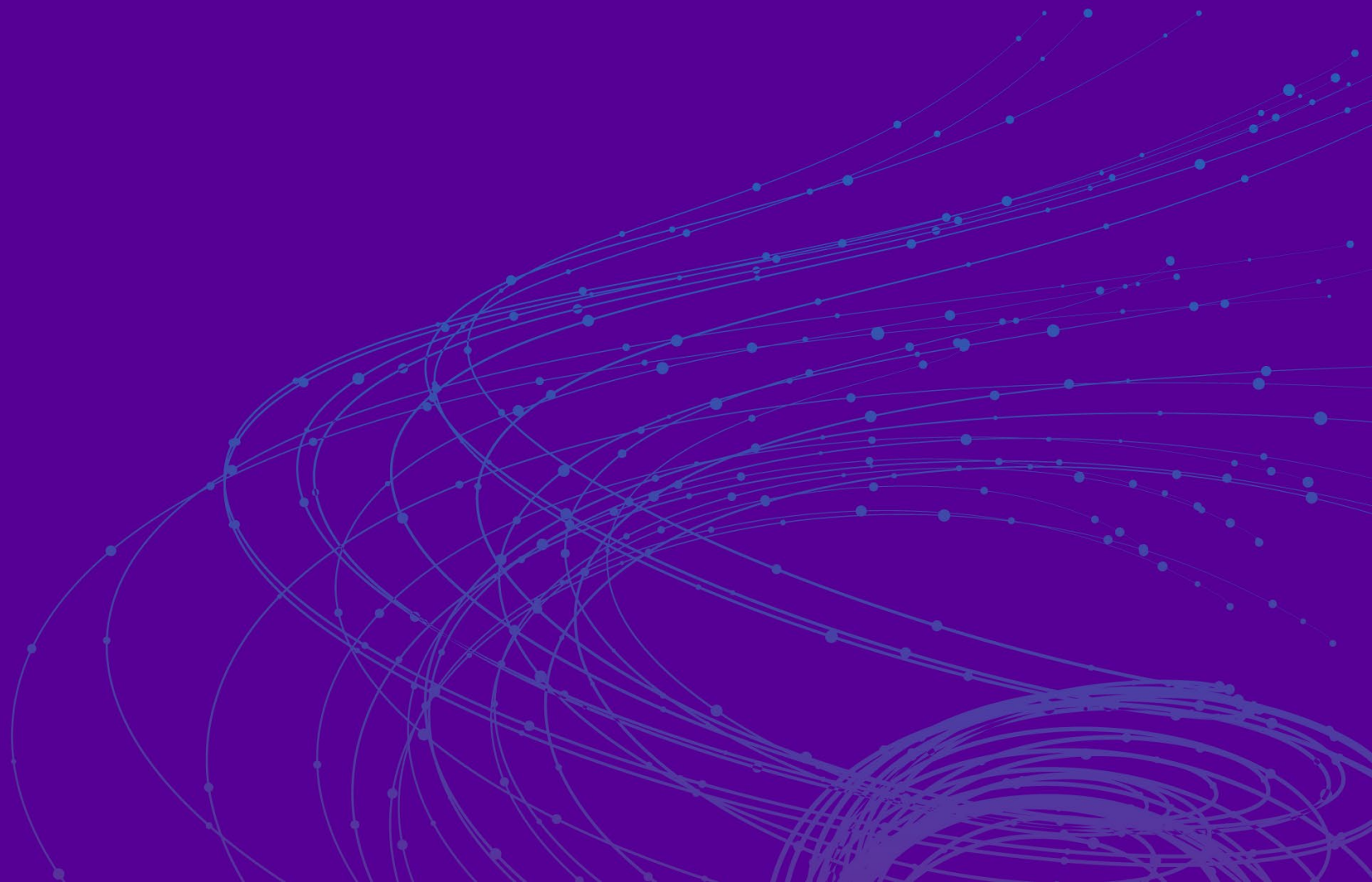
DAY 6 – FBI VISIT

Strategic Questions:

- ?? Do you respond to requests in the meeting?
- ?? How do you respond?
  - ?? Employee separations
  - ?? Initial payment
  - ?? Beacon
  - ?? Investigative update
- ?? Do you tell them about the unusual communication?
- ?? What questions do you have for FBI?

RSAConference2019

The Reply



DAY 8 – THE REPLY

From: ***Bob Ishmael [MD General Counsel]***
Sent: *Friday, November 23, 2018 6:07 PM*
To: *harpooned@hmamail.com*
Subject: *RE: Time to Pay*

Call me Bob. I am the General Counsel and will be taking responsibility for communications with you on behalf of the company so please direct future messages to me.

We need more time to make payment arrangements. There are a number of approvals we need to get internally and we also need to work with our bank to figure out the best way to acquire bitcoins. It is not easy to buy that much BTC in one shot so we will have to break up the purchases. To show that we are working in good faith on this, please see the attached screenshot from Coinbase explaining their limit on daily BTC purchase volume. We will need at least 30 days to get this figured out.

We may be willing to make an initial payment as a further showing of good faith.

We ask that you show your good faith by sharing the totality of the data you have stolen from us.

- Bob Ishmael

DAY 10 – INVESTIGATION UPDATE

- Identified 6 current employees and 2 former employees who visited Wikileaks more than 5 times in past 180 days.
- Identified 35 employees who regularly visit websites that track bitcoin trading price.
- Overlap of 5 employees between those two groups.
- 2 left the company in past 6 months. One voluntarily and one terminated for poor performance.
- The employees worked in different departments but started with the company around the same time 5 years ago and briefly worked together in IT.
- Devices assigned to both employees are associated with communications with suspicious IP address.

DAY 10 – INVESTIGATION UPDATE

Next Steps

?? Do you conduct any employee interviews or review employee communications?

?? Do you pull the HR files for the 2 separated employees? Do you speak to their managers?

?? Do you share names with FBI?

?? Do you cut off communications with suspicious IP address?

DAY 12 – THE FBI RETURNS

FBI Update:

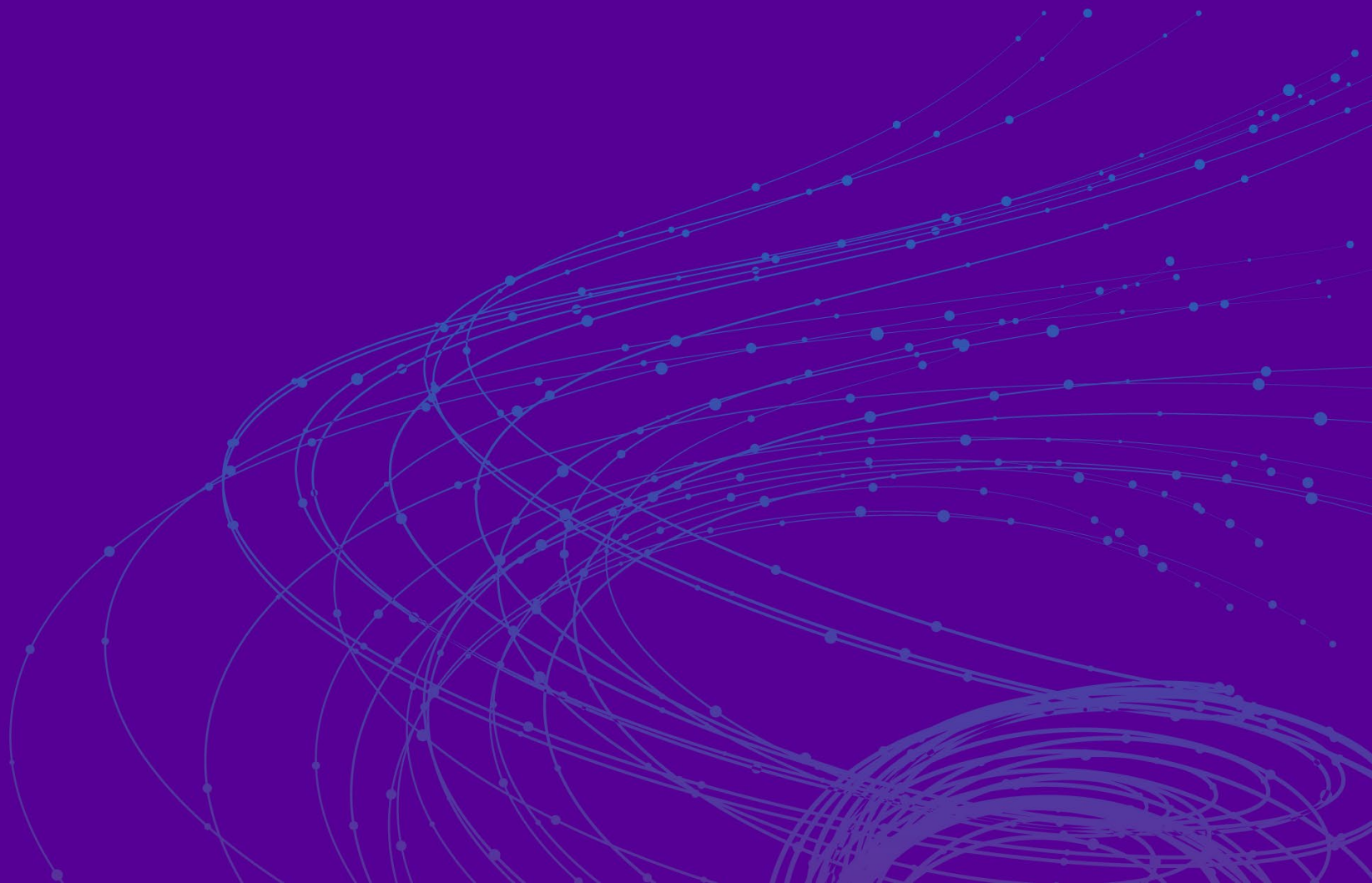
- Agents have identified some leads and have opened an investigation.
- Will not indicate whether beacon has been activated
- Request log data for employees named previously as well as IP addresses of any other device known to have communicated with suspicious IP
- Ask that you NOT block traffic to/from the IP
- No further updates at this time

HOW DO YOU RESPOND?

RSAConference2019

The End. . .

Or is it?



DAY 45 – INVESTIGATION UPDATE

Status Update:

- No further messages from adversary
- No updates from FBI
- Nothing conclusive in employee investigation
- Communications to IP address have ceased
- No sign of compromised data on the web
- Compromise assessment inconclusive – no confirmed evidence of data exfiltration

---

DAY 45 – IS IT OVER?

Close-Out:

- ?? How do you prepare to close out investigation?
- ?? What kind of report do you want?
- ?? What is final position on notification?
- ?? What changes do you make in your security program or response plan as result of this incident?
- ?? Do you continue web monitoring?
- ?? What is communicated to execs? The board?
- ?? Necessary to include a reference in SEC disclosures?

Apply What You Have Learned Today

- Next week you should:
  - Outline how your organization would respond to an incident like this
- In the first three months following this presentation you should:
  - Define roles and responsibilities in your IR plan to enable an effective response to a ransom incident
  - Propose strategic guidelines around key areas like working with law enforcement, responding to attackers and risk tolerance
- Within six months you should:
  - Conduct a tabletop exercise using a scenario similar to Pequod Industries

RSAConference2019

Thank you

R Jason Straight
UnitedLex Corp.
jason.straight@unitedlex.com