

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: LAW-W10

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.

Randy V. Sabett, J.D., CISSP

Special Counsel
Cooley LLP



#RSAC

Objectives

- Stress the importance of preparation prior to an incident
- Expose the limits of what you can accomplish with forensics
- Warn against the lure of false leads and red herrings
- Examine the dynamics 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
- Analyze the appropriate follow up to an incident

Set up and Background

- Case study is a “composite” of several cases we have worked but largely based on one matter
- Jason engaged by outside counsel to assist with a potential data breach incident; this is a follow up interview
- All work performed at direction of counsel and subject to attorney-client privilege and work product protection
- Setup:
 - 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

RSAConference2019

Message from the Deep

The hunt begins



DAYS 0 THROUGH 4

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

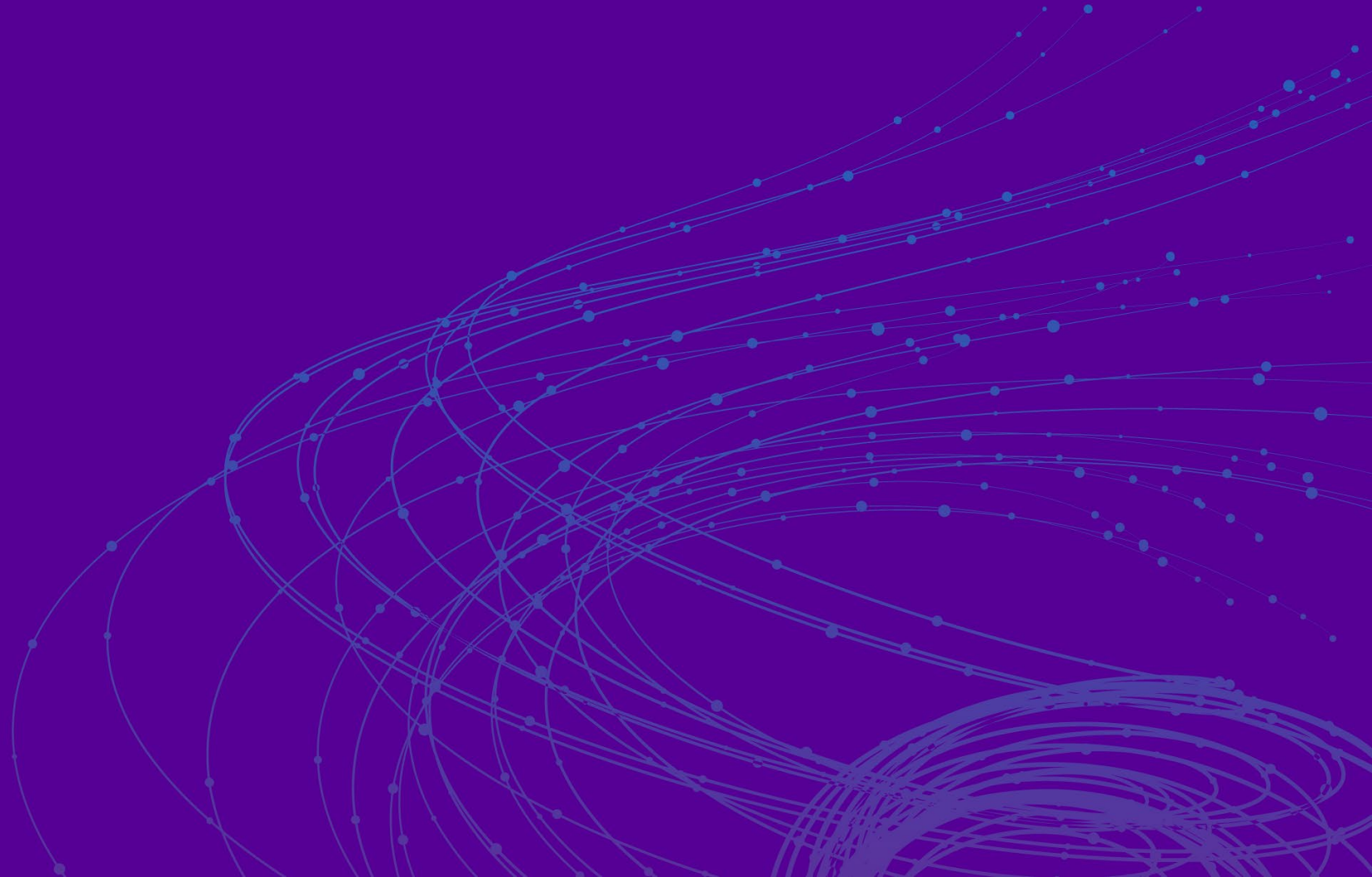


ATTACHED IS PDF WITH IMAGES OF FOLLOWING:

- Ten representative pages from the 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
- Stock grant and employee compensation information for the entire company from 2016 (Prepared by Tax Accountants)

RSA[®]Conference2019

The Demand



DAYS 5 AND 6

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:

1B2S4Nf8jD3fshHodzuYhIamoQsQaZEcZ

1B2S4Nf8jD3gtIpuOeyklAndRtMyywFBVcXvv

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

Sincerely,

Harpooned

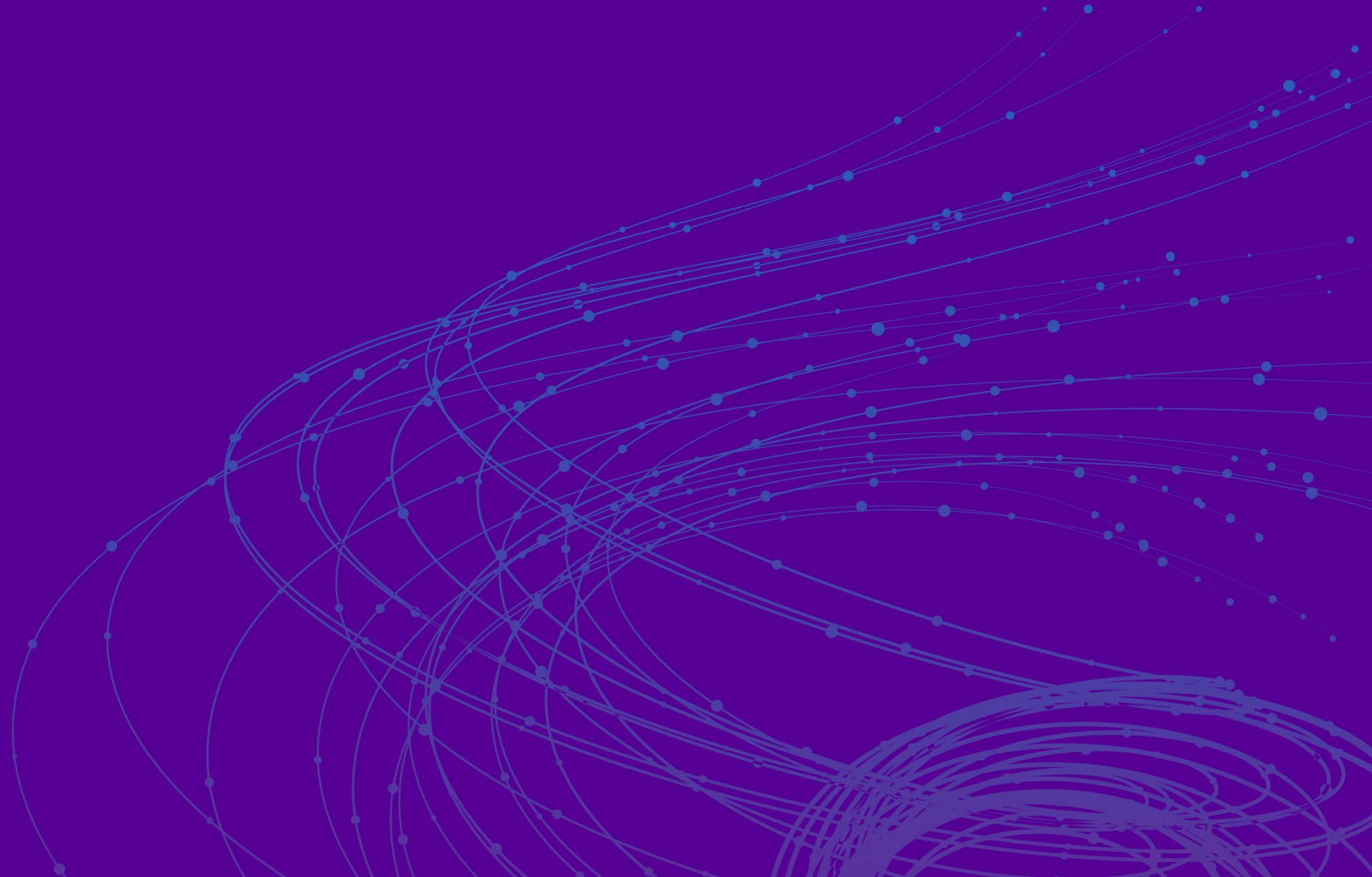


FBI VISIT



RSA[®]Conference2019

The Reply



DAY 7 THROUGH 12

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



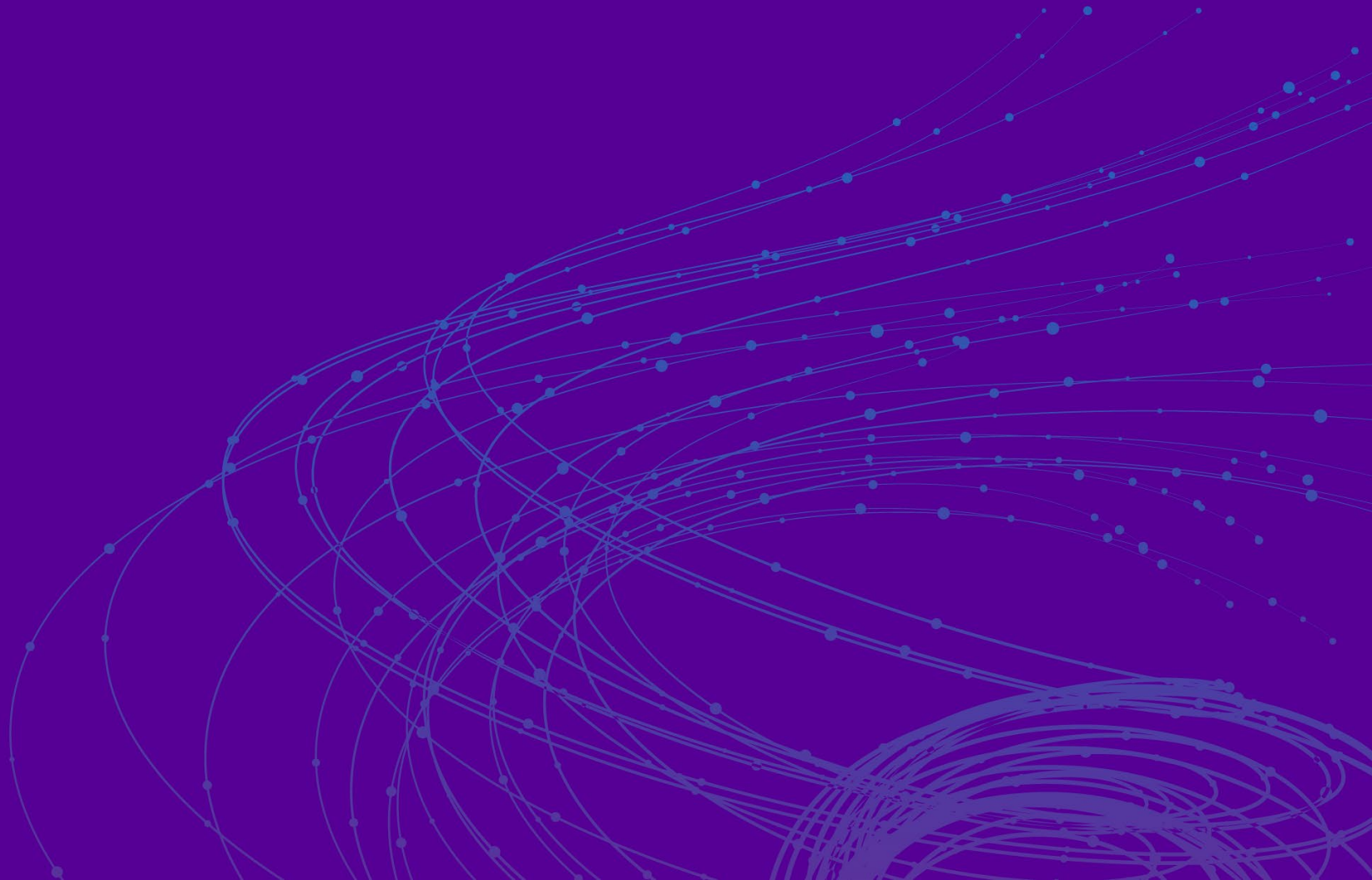
FBI Update:

- 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 and consider installing a network sniffer for them
- No further updates at this time



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

UPDATE

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

RSA[®]Conference2019

Thank you

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

Randy V. Sabett, J.D., CISSP
Cooley LLP
rsabett@cooley.com