RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **LAB1-R02**

Preplanning the Data Breach Chess Board with External Vendors

Dr. Chris Pierson

CEO
BLACKCLOAK
@DrChrisPierson
@BlackCloakCyber

James T. Shreve

Partner & Cyber Chair
Thompson Coburn, LLP
@ThompsonCoburn

Michael Bruemmer

VP, Global Data Breach
Experian
@Experian_DBR
@BruemmerMike

Agenda

- Introductions
- Top 5 Things to do Wrong
- Scenario I
  - Groups
  - Review
- Big Three
- Scenario II
  - Groups
  - Review
- Questions

Chatham House Rules

RSAConference2020

Top 5 Things to do Wrong

#1 Thing to do wrong

- Lacking proper governance
  - Investors
  - Board
  - Executive Leadership Team
  - Team
  - Employees
  - Customers

#2 Thing to do wrong

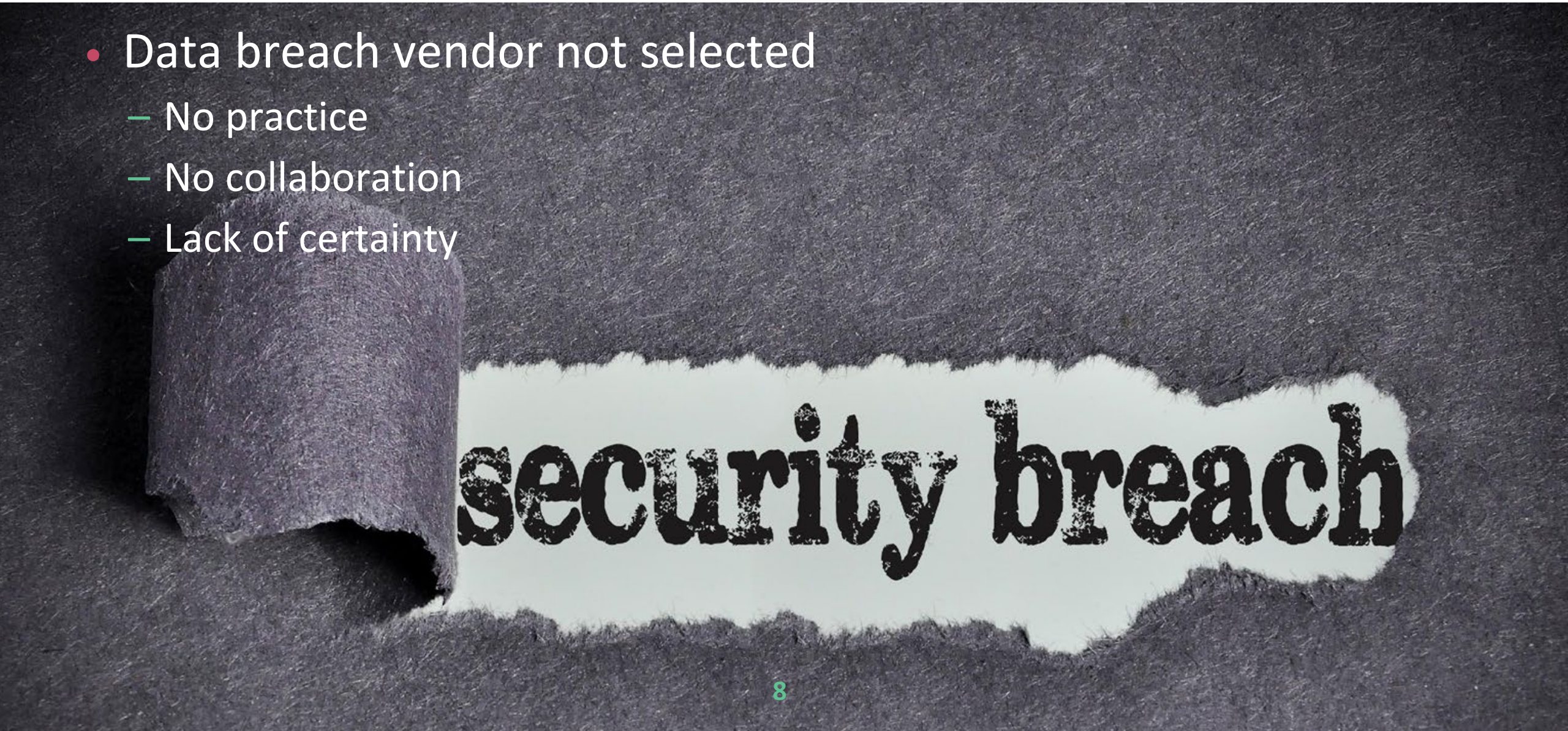
- Attorney/Client Privilege
  - Failing to preserve the privilege
  - Failing to educate the team
  - Not using both inside/outside counsel

#3 Thing to do wrong

- Hiring in the heat of the moment
  - Not having the client be outside counsel
  - Not well articulated
  - Not very drafted well
  - Lacking protections

#4 Thing to do wrong

- Data breach vendor not selected
  - No practice
  - No collaboration
  - Lack of certainty



#5 Thing to do wrong

- Messing it all up
  - Bad 1-800#
  - People
  - Training
  - Wrong URLs
  - Documents unclear

RSAConference2020

Scenario I.

Data Breach Scenario

Scenario I

- Groups of Participants:
  - Tables 1, 7 – Legal
  - Tables 2, 8 – CISO
  - Tables 3, 9 – Board/Execs
  - Tables 4, 10 – PR/Marketing
  - Tables 5, 11 – Customer Service
  - Tables 6, 12 – Compliance/Audit

Scenario I

- The company
  - Maker of point of sale terminals and software to manage loyalty programs and coupons (data stored on your cloud server)
  - Public company
- The attack
  - Ransomware locks up POS terminals and encrypts customer loyalty data on your cloud servers
  - Receive a ransom demand of 1000 BTC to be paid within 8 hours
  - Initially do not pay and attackers threaten to post some exfiltrated data on dark web sites
  - Brian Krebs sends an email saying he has heard about the attack and asking for comment

RSAConference2020

Big Three

Lawyers, Monitoring, Forensics

Big Three - Forensics

- Pre-positioning/planning
- 24hr response
- Knows the team
- Toolkits

Big Three - Lawyers

- Inside v. Outside
  - Hiring
  - Team
  - Practice
  - Relationships

Big Three – Consumer Response

- Who, what, when and how to protect yourself
  - Websites
  - Communication
  - Assistance/ 1-800
  - Regulators

RSAConference2020

Scenario II.

Operationalizing what you designed

Scenario II.

- Groups of Participants:
  - Tables 1, 7 – Legal
  - Tables 2, 8 – CISO
  - Tables 3, 9 – Board/Execs
  - Tables 4, 10 – PR/Marketing
  - Tables 5, 11 – Customer Service
  - Tables 6, 12 – Compliance/Audit

Scenario II.

- Opt not to pay the ransom
  - Reset POS terminals
  - Restore loyalty data from backups
- IS reports several similar attempted attacks in the following days
- The attack is in the press
- Shares lose 20% of value initially, but regain 10% in 3 months
- 15% of customers leave, many remaining customers apply enhanced oversight
- FTC and a few state AGs send letters asking questions about security practices

RSAConference2020

Parting Thoughts & Questions

Themes

- C-Suite & The Board
- Operational Authority Guidance
- Working with Outside Vendors (non-legal)
- Role of Outside Counsel
- Practice Makes Perfect
- Keeping up w/ Laws & Regulators

Back at Home . . .

- Based on the perspectives of others in the organization, consider what they will need and want to know in an attack and investigation
- Have you adapted your response plan appropriately for mistakes/weaknesses in response?
- Are all needed parties involved not only in the response, but in adapting the process in the aftermath of an incident?

RSAConference2020

Contact Us

Dr. Chris Pierson

CEO

BLACKCLOAK

@DrChrisPierson

@BlackCloakCyber

chris@blackcloak.io

James T. Shreve

Partner & Cyber Chair

Thompson Coburn, LLP

@ThompsonCoburn

jshreve@thompsoncoburn.com

Michael Bruemmer

VP, Global Data Breach

Experian

@Experian_DBR

@BruemmerMike

michael.bruemmer@experian.com