RSAConference2020

Learning Labs

HUMAN ELEMENT

Preplanning the Data Breach Chess Board with External Vendors

Session ID: LAB1-R02

Dr. Chris Pierson

James Shreve

Michael Bruemmer

BLACKCLOAK THOMPSON COBURN LLP experian

Table of Contents

Preplanning the Data Breach Chess Board with External Vendors

Themes

On February 27, 2020, we explored issues around engaging outside resources in addressing security incidents in the RSA Conference Learning Lab "Preplanning the Data Breach Chess Board with External Vendors." The facilitators outlined five primary areas where entities often make mistakes in the engagement of outside resources, which were:

1. Lacking proper governance for the process
2. Failing to appropriately protect strategic decisions making with the attorney-client privilege
3. Engaging resources in the heat of the moment
4. Not selecting a data breach vendor and/or not appropriately involving the vendor in the process
5. Mishandling details involving interactions with consumers

Scenario

The presentation explored these issues through discussions of issues in a scenario involving a ransomware attack. The scenario involved a public company that is a maker of point of sale terminals and software to manage loyalty programs and coupons. The company experiences a ransomware attack that locks up POS terminals at customer locations and encrypts customer loyalty data on company cloud servers. The company received a ransom demand of 1,000 BTC to be paid within eight hours, but the company does not initially pay the ransom. The attackers threatened to release a sample of data exfiltrated during the attack.

Discussion Groups

Participants in the session then discussed the scenario by breaking into groups, each of which had a different role in the company. The groups were:

- In-house legal
- CISO
- Company board and executives
- Public relations and marketing
- Customer service
- Compliance and audit

Each of the six groups was asked to consider:

- What questions they would have about the incident
- What concerns, from their perspective, they would have about the incident
- What outside vendors or other third parties they would like to (or need to) involve in the investigation and response

Results of Discussion Groups

Each of the discussion groups considered the scenario from their assigned perspective and offered the following thoughts.

In-House Legal

Questions

- Regulations that apply/ jurisdictions/ countries/ states, etc.
- Timelines to meet legal and regulatory requirements
- Whether to make the ransom payment and who should decide
- Contractual obligations on the company that may impact response

Concerns

- Involvement of the FBI or other law enforcement
- Types of data impacted in the incident, such as PII/PCI/etc.
- Crafting communications with
    - Customers
    - Press
    - Internal parties
    - Regulators and other government agencies
- Notification of the cyber insurer
- Developing a plan for possible litigation
- Analysis of root cause
- Corrective actions
- Residual Impact/Plan

Vendors

- Outside counsel, as soon as possible
- CISO
- 3rd party vendors
- Insurance company

CISO

Questions

- Determining the cause of the vulnerability and the source of the attack
- How long attack has been going on
- Why is the company still being attacked
    - Address latent vulnerability
    - Close threat vector
- What actions are and will be taken to contain the attack and damage
    - Logs
- Are recovery time objectives being met

- What steps are being taken to prevent future attacks
- Is legal involved in the response
- The scope of data exposed
- Is law enforcement involved
- Is customer response being addressed
- Is the investigation and response in compliance with company policies and procedures
- Can the incident be used to improve overall incident response
- Did the incident create compliance issues
- How did legal/vendor relations function

Concerns

- Getting stores online for sales
- Implementing the incident response plan
- Making sure the company has up-to-date backups
- Following company policies and procedures
- Public relations and outward-facing communications
- Attribution for the attack
- Appropriately addressing customer notification
- The compliance of notifications and meeting other regulatory obligations
- Meeting contractual commitments for the company
- Assisting the company's board and other departments
- Responding to state attorneys general and the FTC
- Evaluating the internal vulnerability assessment

Vendors

- Managed security service provider (MSSP)
- Point of sale terminal hardware and software makers
- Cloud provider that hosts loyalty data
- Forensics provider for the investigation
- Providers of incident response services
- Penetration testing
- Auditors

Board and Executives

Questions

- What steps have we taken in the investigation and response
- Is the incident under control
- What is the plan to contain damage from the attack
- What is the potential liability of the company from the attack
- Who is handling public relations relating to the incident
- Whether the company has a holding statement

Concerns

- The reputation of the company
- Costs to the company and impact on shareholder value
- Impacts on the company's customers and the relationship
- Legal obligations of the company
- Important milestones for legal, regulatory and contractual compliance

Vendors

- Public relations firm
- Outside counsel

Public Relations and Marketing

Questions

- Should the company continue existing promotion campaigns
- Whether the company should engage outside PR or marketing resources
- Does the company require assistance for post-breach campaigns

Concerns

- Align on the decision made by executives on how to respond to the incident
- Whether the company makes statements that admit or deny the incident
- Mounting an aggressive campaign to regain customer's confidence
- Recapturing lost customers using loyalty
- Full collaboration and communication with the legal team

Vendors

- Outside legal
- Public relations

Customer Service

Questions

- To whom should escalations be referred
- When will different iterations of scripting be composed and who should approve
- What versions of scripting be required

Concerns

- Different script/messaging for our partners
- Coordination for different media channels, such as social media
- Escalation procedures
- Global logistics issues
    - Time zones
    - Other teams (ex. sales people)

- Feedback loop to keep other stakeholders informed
- Longer-term logistics issues
    - When vendor rolls off, transitioning calls to in-house resources
    - Staff morale and potential burn out
- Funding for training

Vendors

- Recommend hiring call center/other remediation efforts
- Training for customer service staff to keep our remaining clients

Compliance and Audit

Questions

- How did the incident happen
- What can be determined from logs
- How data be recovered
    - What data, where is it
    - How long will recovery take
- How can we contain the scope of the incident
- What is the extent of the issue
- Is the issue completely or partially covered by insurance
- Does the company have contractual or legal obligations

Concerns

- Have the affected systems been audited for security, such as under PCI
- Do we know what security controls were needed for the involved systems
- Whether patching on involved systems up to date
- Will law enforcement want involved devices to remain in operation
    - Internal interests may be conflicted as some may press for law enforcement cooperation while others seek to contain the incident

Vendors

- Cloud service provider
- Compliance auditor
- Assistance for recovery of systems and data
- Cyber insurance carrier

Common Themes

Participants in the exercise identified several common themes regarding the response to an incident and the engagement of outside resources:

1. Different parts of the enterprise must be in close communication throughout the investigation and response process. An example can be seen in cooperation of legal and PR in drafting external messaging to reflect the company's message, not create unnecessary risk and be understandable by the public.
2. There are significant advantages to having outside resources engaged by counsel. Important among the advantages is the potential to keep strategic decision-making under privilege.
3. Engaging external resources well before an incident allows for:
    - Better comparison shopping
    - The contract to be in place before services are required
    - Improved vetting and on-boarding of the vendor