Client Cybersecurity Update:

Top 10 Things to Do in the Event of a Data Breach

November 15, 2017

Presented by: Bradley Arant Boult Cummings LLP

Presenter Bios

- Paige Boshell:

Partner, Birmingham

Leader, Cybersecurity and Privacy Team

- Mike Pennington:

Partner, Birmingham

- Alex Purvis:

Partner, Jackson

Bradley

Agenda

Top 10 Practice Pointers

-Team members and roles
-Substantive legal requirements
-Insurance coverages and conditions
-Litigation and prudential considerations

Bradley

1. Mobilize your response team

Internal – IS, Executive, LOB management, Legal, Marketing, HR, Compliance

External – Legal, Security, PR, Cyber insurer

Insurance considerations - Does policy require immediate notice and/or use of approved vendors?

Litigation considerations – Privilege, minimize risk of harm, identification of and compliance with applicable notice requirements: involve outside counsel immediately

2. Stop the breach

-Determine whether or not continuing

-Isolate access vectors

-Identify affected systems

-Implement stop-gaps and work-arounds

-Shore up related systems and access vectors

3. Vendors

Forensic investigators- Coordinate investigation, cease intrusion, collect evidence

Current security vendors- external IT management, hardware vendors, software licensors

Other involved vendors-notice ,cooperation and indemnification contractual terms

PR, customer service, remediation

4. Insurance

Get the right coverage before the breach

Cybercoverage: know your risks; tailored coverage

Other coverage possibilities in the traditional portfolio

Follow the policy instructions: notice; communication; consent

Don't just accept a denial

Bradley

5. Litigation management

Privilege – hire law firm first and involve them in every aspect of the response

Preservation of evidence – litigation hold, change archival or other IT processes

Mitigation – consider unilateral measures to reduce or prevent harm and empower potential victims

6. Notice

-Federal law: HIPAA, FTC

-State law: consumer protection, data breach

-Contractual requirements: customer agreements, vendor contracts

-UDAAP and UDAP

-Litigation considerations

7. Centralization of Response and Remediation

Internal

-Hierarchy for escalation

-Security-by-design – all input welcomed and escalated

-involve counsel for privilege maximization

External

-Coordination through law firm

-Regular meetings

-Centralization of vendor communications and customer response and PR messaging

Bradley

8. Law Enforcement

Local - police

Federal - FBI, USA

State – AGs

Is there an ongoing breach? Is a crime involved? Could this breach be part of a larger pattern or scheme?

Litigation implications of notifying law enforcement

Bradley

9. Unified Messaging

-Determine message

-Designate structure for messaging

-Coordination of internal and external team members

-Litigation considerations

10. Remediation and resiliency

-Remediation : customer and vendor harms

-Remedies: source of breach

-Continuing monitoring: coordination of efforts

-Debriefing: lessons learned

-Correcting gaps: prevention

Bradley

Questions & Contact Information

Paige Boshell

pboshell@bradley.com

205.521.8639

Mike Pennington

mpennington@bradley.com

205.521.8391

Alex Purvis

apurvis@bradley.com

601.592.9923

Bradley