DLA PIPER

#DLAPiperTech18

2018 GLOBAL TECHNOLOGY SUMMIT

AT THE INTERSECTION OF BUSINESS, LAW AND TECHNOLOGY

MORE THAN PLUGGING THE HOLE:

A Discussion About How to Respond to a Cyberattack

TechLaw

**This presentation is offered for informational purposes only, and the content should not be construed as legal advice on any matter.*

Agenda

- Introduction
- Identifying the threat
- Conducting the investigation
- Notification
- Civil liability
- Resolutions
- Remediation

Panelists

- Alisa Bergman, Chief Privacy Office, Adobe
- Jim Halpert, Co-Chair - Global Data Protection, Privacy and Security Practice, DLA Piper
- Jerry Kral, Chief Risk Officer, Brown Forman
- **Moderator** – Brett Ingerman, Co-Chair - Global Compliance and Governance Practice, DLA Piper

Identifying the threat – the first 48 hours!

- Implement incident response plan
  - Convene incident response team and retained service providers (where potentially serious)
  - Contain threat, preserve evidence, identify affected systems and data
  - Internal and external notification of key stakeholders
  - Initiate investigation
- Protect privilege (where it is available)
- Contact law enforcement/ISAC?

Conducting the investigation – Incident Response Team

- In house
  - Legal/CPO/CCO
  - IT/CISO
  - Corporate security
  - Human resources
  - Investor relations/communications
  - Client account leaders
- Outside experts
  - Lawyers
  - Forensic firm(s)
  - Public relations firm
  - Other specialized services

Conducting the investigation – what are you looking for?

- Securing the evidence (logs, documents, witnesses, etc.)
- Determining what occurred, how it happened and the boundary/scope of the incident
- Factual considerations
  - State of logs and other evidence
  - How long was intruder in your systems? What was the last date of access?
  - Were other parties also affected or involved?
  - What data and systems were compromised? Were data exfiltrated?
  - Apparent motivation of the intruder/nature of threat
- Role of a PCI forensic investigator (PFI)

Notification: who to tell?

- Statutory/regulatory requirements
- Contractual obligations
- Constituent management
- Governance obligations (*eg*, to keep board informed)
- Should be set out in Incident Response Plan

Mitigating civil liability

- Protect the privilege
- Remediate, remediate, remediate
- Customer/vendor outreach
- Manage the message carefully

The CCPA is a game changer for data breaches

- Jan. 1, 2020, transforms data breach risk where no reasonable security, even for industries exempt from CCA privacy requirements
- After any data breach of California PII (except account credentials) plaintiffs bar can sue for . . .
  - Statutory damages can be $100 to $750 per violation
- No requirement to prove harm -- greatly simplifies standing and class cert (although 17200 may limit this)
- Only exceptions: (1) the PII were encrypted or redacted, or (2) the breach is "cured" within 30 days of notice from plaintiff
- Otherwise face very expensive eDiscovery into your security program and risk massive damages

CCPA class action risk mitigation

- What to do about CCPA:
  - → Map CA personal and breach notice data
  - → Establish strong information governance
  - → Encryption and redaction
  - → Arbitration clauses (CCPA purports to override FAA, though)
  - → Cyberinsurance
  - → Cybersecurity reviews against an established security standard
  - → If breach notice data is sent to a third party, try to get the data back with a sworn declaration that it was destroyed

Resolutions

- State Attorneys General
- Federal Trade Commission
- International regulators
- Congress
- Civil litigation

Remediation

- Confirm all malware removed
- Implement security recommended upgrades
- Consider carefully whether and what relief to offer affected individuals
  - Offering credit monitoring may bolster plaintiff's case for standing (*eg*, *Zappos* CA 9)
  - Offering protection services to clients may complicate commonality analysis for class certification
- Review incident and response with IR team to develop "lessons learned" and train for those
- Consider if the incident exposed weaknesses in cybersecurity program (*eg* vendor risk management or board communication)

THANK YOU