The Financial Services Industry Speaks:
Key Risk Management & Chief Privacy Officer Perspectives

Kimberly Holmes
SVP, Counsel – Cyber Insurance, Liability & Emerging Risks – ID Experts *(Moderator)*
Patrice Brusko
SVP, US Chief Privacy Officer - TD Bank
Ethan Harrington
Director, Insurance & Enterprise Risk Management - H&R Block

SANS Data Breach Summit, Chicago - September 26, 2017

Key Perspectives from the Front Lines…

- Evaluating, revising, monitoring 3rd party vendor relationships
- Navigating best practices for minimum retention and document destruction
- Motivating employees to come forward when something doesn't seem "quite right"

Evaluating, revising, monitoring 3rd party vendor relationships

- Issues are not necessarily “over” when the contract ink is dry
- Entity assurances per contract often are not backed up by capital or resources
  - Key: due diligence review of vendor balance sheet for capacity as well as willingness to make whole
- Due Diligence: HR Policy directing information security training
- Increasing numbers of cloud providers (CPs): shifting the landscape of what contracts look like
  - Does your organization have alternate language or leverage to implement against the CP?
  - Document the risks if your organization has to take “boilerplate” CP language
  - Require Executive Committee, C-Suite and/or GC to sign off and acknowledge risk of accepting CP boilerplate language

Evaluating, revising, monitoring 3rd party vendor relationships

- Need for enterprise risk management to be on board when dealing with CPs:
  - Risks not willing to accept vs. those needing to be escalated?
  - Consistency in analytic process across organization avoids overlap issues/exposure
- Having the right “control partners” at the table:
  - May feel like its “slowing business down”…
  - Consistency in analytic process across organization avoids overlap issues/exposure
- How to get C-Suite/BOD to Listen?
  - As much an art as a science
  - Be persistent, but patient - allow individual thought processes to work
  - Remove emotion from the discussion
  - Focus on CEO guidance “to do the right thing”

Navigating best practices for minimum retention and document destruction

- Can’t Keep Everything (especially cir. 1987!)
- Be Wary – where one department requests a subset of data having a source location and another department requests a different subset of the same data (different slices of same data) – now data rests in multiple locations
- Email: Inboxes and Sent folders
- Dumpster Diving
- Materials Missing in Transport

Motivating employees to come forward when something doesn't seem "quite right

- Not Uncommon Today: the incident "scramble and blame" game
  - Better plan: Have an Escalation Protocol that everyone is familiar with
  - Privacy Playbook & "PAL" Award
- Privacy Training – Make it Mandatory and in-house
  - Remove stigma of "getting something wrong"
- Conduct internal phishing campaigns
  - Makes detecting "frequent flyers" of mistake easier
- Trend today - Employees are:
  - Finding more mistakes themselves
  - More aware that attacks are getting more sophisticated
  - More cautious now when incoming emails ask for credentials

QUESTIONS?

- Kimberly Holmes
  - kimberly.holmes@idexpertscorp.com
- Patrice Brusko
  - Patrice.Brusko@td.com
- Ethan Harrington
  - ethan.harrington@hrblock.com