Mitigating the Existential Data Breach Risk

A Complimentary LexisNexis® Webinar
March 12, 2014

Oliver Brew, CIPP/US, CIPM, Vice President, Specialty Casualty, Liberty International Underwriters
David Katz, Partner, Nelson Mullins Riley & Scarborough LLP
John Kropf, Senior Counsel Privacy and Information Governance, Formerly with Reed Elsevier
Adam Miller, CIPP/US, Supervising Deputy Attorney General, Office of the California Attorney General

LexisNexis®

About the Speakers

Oliver Brew, Vice President LIU Professional, Privacy and Technology Liability. Based in New York, Oliver runs a specialist national underwriting team. He is a leading underwriter in this field, having presented at numerous industry conferences, including the Department of Homeland Security Cyber Risk Culture event earlier in 2013. Prior to joining Liberty International Underwriters in 2011, Oliver was at Hiscox for 7 years where he held various underwriting and management positions in the technology and privacy area. Before that ran the technology account at CFC Underwriting in Lloyds and started his career at Willis in London. He is a Certified Information Privacy Professional, Certified Information Privacy Manager and Associate of the Chartered Insurance Institute in the UK. He majored in Politics at Cambridge University.

About the Speakers

David Katz is a partner in Nelson Mullins Riley & Scarborough's Atlanta office where he leads the Privacy and Information Security Practice Group. He counsels clients on the development, management, and oversight of privacy and compliance programs. He also assists them in developing policies and procedures, education strategies, implementation of auditing and monitoring controls, reviews of disciplinary and enforcement activities, and risk assessments. He speaks and writes on matters relating to technology, privacy and data security. His tweets can be followed on twitter @KatzFDavid.

About the Speakers

John Kropf has over 15 years of legal and policy experience in privacy and information law in both government and corporate cultures. Most recently, he worked as Deputy Counsel for privacy and information governance for Reed Elsevier. He was previously a member of the Senior Executive Service, and served as the Deputy Chief Privacy Officer for the U.S. Department of Homeland Security's Privacy Office and senior adviser on international privacy policy. Before joining DHS, Kropf worked as an international lawyer with the U.S. Department of State in the Office of the Legal Adviser. Kropf began his federal career as an attorney with the U.S. Department of Justice Honors Program. He earned his law degree and a master's degree in public and international affairs from the University of Pittsburgh and a BA from Denison University. He is a member of the International Association of Privacy Professionals (IAPP) and serves as a member of its Research Advisory Board. He is the author of the *Guide to U.S. Government Practice on Global Sharing of Personal Information* as well as numerous articles on global and strategic privacy issues.

About the Speakers

Adam Miller has worked for the California Attorney General's Office in San Francisco since 1997. He is the inaugural Supervising Deputy Attorney General for the Privacy Enforcement and Protection Unit that was created in 2012. From 1997 until 2001 he worked in the Licensing Section, where he prosecuted hundreds of vocational licensees for professional misconduct. From 2001 through 2012 he worked in the Antitrust Law Section, where he investigated and prosecuted mergers and anti-competitive conduct, involving markets such as computer software (Microsoft) and hardware (flat panels), search advertising, oil and gas refining/retail, and film exhibition. Before joining the State, Mr. Miller was a Deputy County Counsel for Contra Costa County and worked in private practice. Mr. Miller earned his undergraduate degree in computer science from Brandeis University, and his law degree from Golden Gate University School of Law.

Agenda

I. Foundation: Have a Comprehensive Program in Place

II. Reacting to a Breach

III. Cyber Insurance

IV. Regulators

V. Q&A

The Foundation: A Comprehensive Set of Controls and Procedures

LexisNexis®

1. Organizational Commitment to Privacy

2. Personal Data Inventory
   - Where it resides
   - Who has custody
   - Control
   - Sensitivity of the information
   - Applicable law

3. Documented Data Privacy Policies
   - Link policies to external criteria in applicable law

4. Risk Assessment and Mitigation
   - Does the organization conduct regular assessments and mitigation

5. Documented program to regularly train employees about policies, procedures and roles

6. Breach Incident Management Response Plan

7. Service Provider Management

8. External Communication

LexisNexis®

9. Oversight and Review

10. Assess and Revise Controls As Needed

Reacting to a Breach

LexisNexis®

When Bad Things Happen

The Chinese Symbol for Crisis is a combination of the two symbols for Danger and Opportunity

Breach Response

Have a Plan.

Be prepared to quickly gather the facts.

Assemble a team to investigate the facts.

Assemble outside experts.

Determine the scope of the investigation.

Establish the Attorney Client Privilege.

Be prepared to communicate.

Be prepared to make a record.

Two Philosophies in Risk Management

Proactive Risk Management: Easy, Controlled, World of Budgets

Reactive Risk Management: Hard, Lack of Control, Expensive. Get me out of trouble now no matter what it costs me.

Things To Do: Review Your Plan

Review Your Plan

If you have a breach response plan, review it and, if necessary, update it immediately.

If you don't have a plan, your company will need to develop one as soon as possible.

Be prepared to conduct a risk assessment within a reasonable time table and with outside counsel to protect the privilege.

Assemble Your Team and Assign Oversight

Your “battlefield commander(s)” must be identified in advance of a data breach. Immediately following a crisis situation, informed decisions affecting the entire company will need to be made quickly to protect the company as well as its customers.

Good crisis management can give rise to numerous conflicts of interest: what the company’s legal team wants may not be what its marketing team wants. Swift decision-making will favor your company.

Things to Do: Be Prepared to Communicate

Be Prepared to Explain Your Actions

At its core, an data breach will be a crisis event.

You will need to work closely with your internal team and most importantly your outside counsel to deal with negative impact to your brand, questions related to the event and any legal or regulatory fallout that may occur as a result of the underlying issues.

You will likely be required to communicate at some level with your customers/investors/the media. A well-developed script will be essential as your company engages the public and the media.

Things to Do: Communicate to Regulators

Be Prepared to Communicate to Regulators

Once a regulatory inquiry is made you should immediately consider your company to be "on the record."

It is important to remember that, from the moment the a potential legal issue is reported, the company is making a record that could be reviewed by a regulator.

Things to Do: Practice the Plan

Practice the Plan

Train your employees to execute the plan. Have your team work through practice scenarios and hypothetical data breach events. Practice makes perfect and frequent training exercises are a crucial aspect of any crisis response. Day One of the crisis is not the time to introduce team members to one another.

Act Now

The sooner you can review your plans and engage your team the better. Budgets matter and planning is important, but delaying a plan or re-prioritizing could be an expensive mistake.

Understanding "the plan" and having the ability to execute it in a crisis can save time, precious dollars and valuable brand equity.

Notification Obligation?

46 States, plus D.C., Puerto Rico, Guam and USVI have data notification statutes for breaches of sensitive information

Notification Obligation?

State Data Breach Statutes:

What are the data elements exposed?

Notification formats

Timing Requirements

Data Breach

State Data Breach Statutes

Statistics

26 States where definition of PII is broader than general definition

3 State trigger notice by access alone

39 States require a risk of harm analysis

17 States require notice of the Attorney General

7 States require notice within a certain time frame

17 States permit a private cause of action

42 States have a safe harbor encryption exception

Data Breach

Other Notification obligations

- Board/audit committee
- Clients
- Regulators
- Insurers

Contract Requirements

Law Enforcement and Regulators

Data Breaches: How-To

Internal Communications

One Voice

Document Hold notice

External Communications

Inquiry Response Plan

Notification Plan

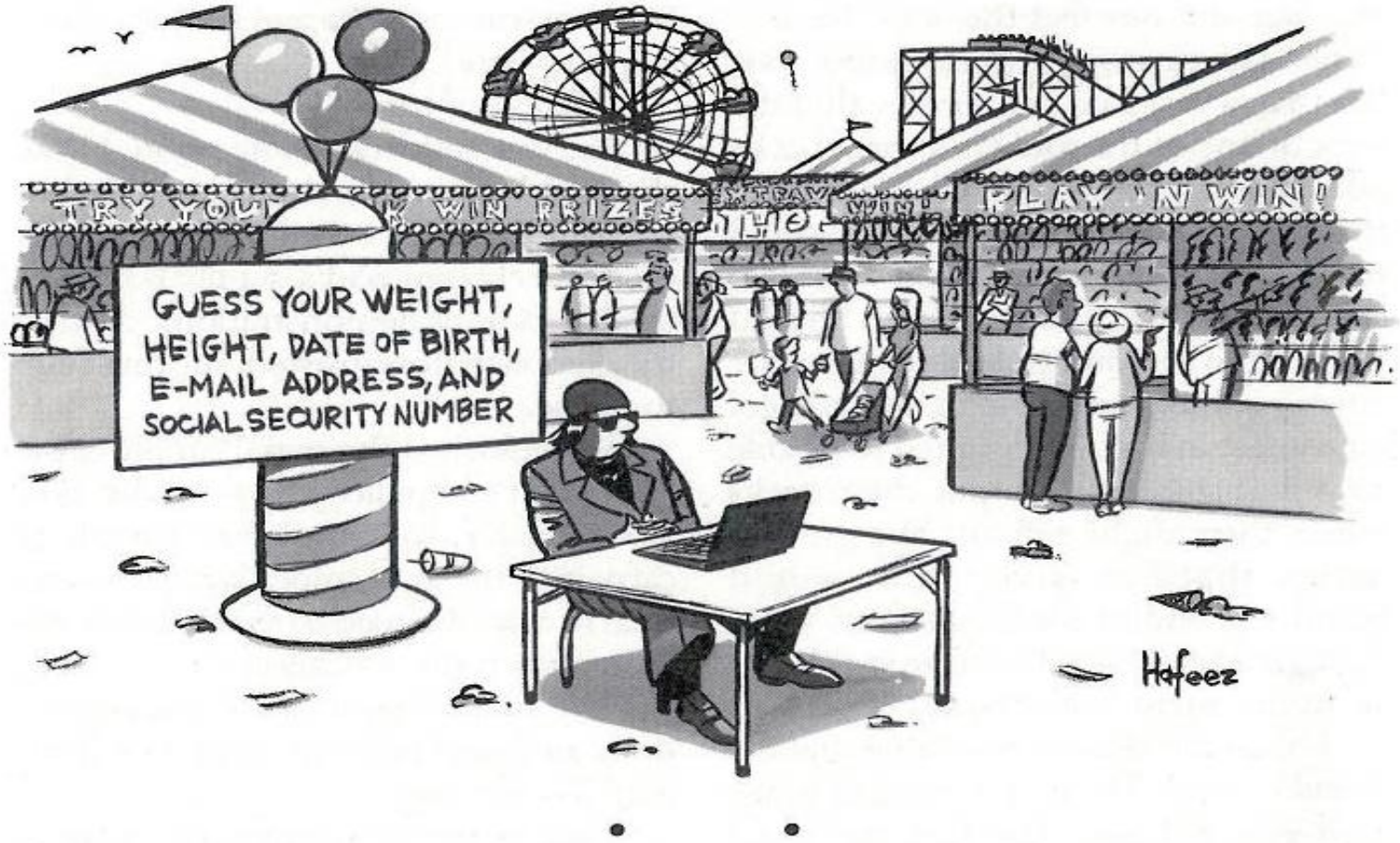
Data Breaches: DOs and DON'Ts

DO:

Identify and empower a breach response team
Establish the Privilege
Investigate and preserve the evidence
Prevent further exposure of data
Develop a communications plan
Contact the insurance carrier
Analyze notification obligations promptly
Involve technology and forensic experts as needed

Insurance for Privacy and Cyber Risks

LexisNexis®


GUESS YOUR WEIGHT, HEIGHT, DATE OF BIRTH, E-MAIL ADDRESS, AND SOCIAL SECURITY NUMBER
PLAY 'N WIN!
Hafeez

Underwriting Cyber and Privacy Risk

Standard lines insurance do not affirmatively cover privacy risks:

- General Liability
  - Advertising Injury / Personal Injury
- Kidnap and ransom
  - Extortion
- Crime

Network and Privacy Insurance – What is Covered

First Party Coverage

- Breach Notification & Services
- Data Restoration/Recreation & Systems Restoration
- Public Relations
- Business Interruption

Third Party Coverage

- Breach Liability – Civil & Regulatory
- Network Security Liability – virus
- Media Liability

Underwriting Factors

Industry

Size

Type and volume of data

Risk management

- People
- Process
- Technology

Incident response

History

The application process

1. Broker review and assessment
2. Bring stakeholders together
3. Application
4. Obtain quotations
5. Select most appropriate coverage
6. Finalize terms and any outstanding items
7. Bind coverage

More complex risks

For larger or more complex risks underwriters use a variety of tools to assess them:

1. Conference calls
2. Technical assessments – e.g. penetration tests
3. Benchmarking against industry compliance standards
4. Ongoing risk management services

Coverage Hotspots

- In event of an ‘incident’ - when should an insured client notify the insurer?
- Deliberate / malicious acts
- Contract indemnification

How to succeed in responding to data breaches

- Don’t panic!
- Maintain open dialogue with insurer
- Protect and preserve evidence
- Be proactive with regulators where appropriate

Regulators

LexisNexis®

Notifying Consumers and Dealing with Regulators

- Notify consumers and regulators as early as possible
- Cal. Civ. Code § 1798.82 = "disclosure shall be made in the most expedient time possible and without unreasonable delay" subject to L.E. needs
- Consider rolling notices to consumers as soon as id'd

  e.g., see *People v. Kaiser Foundation*
- May consider combination of substitute (web and media) plus direct consumer notice
- Consider proactively contacting local or HQ AGO
- Protect and preserve evidence

How Do Regulators Assist With Breach Responses

- California AGO publishes best practice guides:
- See https://oag.ca.gov/privacy/business-privacy

  "Cybersecurity in the Golden State, February 2014: How California Businesses Can Protect Against and Respond to Malware, Data Breaches and Other Cyberincidents."
- Companies are often the victim of data breach
- But regulators are concerned with consumer victims
- Not acceptable for companies to contend that breach is inevitable
- Companies must protect consumer PII, and anticipate and protect against potential breach

What Do Regulators Want During Investigations

- "When a breach occurs, attorney generals [sic] look for encryption, response and a good attitude"
- Does company have policies and procedures in place in anticipation of potential incident?
- Is company notifying and updating consumers and regulator?
- Are consumer breach notices "in plain language?"
- Is focus of company on assessment, repair and protection of consumers PII?
- Or defending business plan and minimizing exposure?

What Should Companies Expect During Investigations

- Who is in charge of privacy/security and incident response?
- What training, programs, security was in place?
- Do you have adequate privacy policies in place?
- Are your practices consistent with your policies?
- Are you managing your data vendors' access?
- Cyber-insurance may be useful, but only if it encourages better security and privacy
- Regulators will not necessarily accept limits of coverage

Q&A

LexisNexis®

Thank You!

Adam Miller, CIPP/US, Supervising Deputy Attorney General
Privacy Enforcement and Protection Unit
Office of the California Attorney General
Adam.miller@doj.ca.gov

David Katz, Partner, CIPP/US, CCEP
Nelson Mullins Riley & Scarborough LLP
david.katz@nelsonmullins.com

Oliver Brew, CIPP/US, CIPM
Vice President, Specialty Casualty
Liberty International Underwriters
oliver.brew@libertyiu.com

John Kropf
Senior Counsel Privacy and Information Governance
Formerly with Reed Elsevier
kropferama@gmail.com