


Data Breach Response: Preserving the Privilege

April 13, 2018

Presenter

- James Melendres, Partner, Snell & Wilmer
- Co-chair - Cybersecurity, Data Protection, and Privacy Practice
- Chair – White Collar Defense and Investigations Practice



Presentation Overview

1. The Reality of Data Breaches
2. Attorney-Client Privilege & Work Product Doctrine
3. Best Practices to Preserve the Privilege

3 © 2018 Snell & Wilmer



THE REALITY OF DATA BREACHES

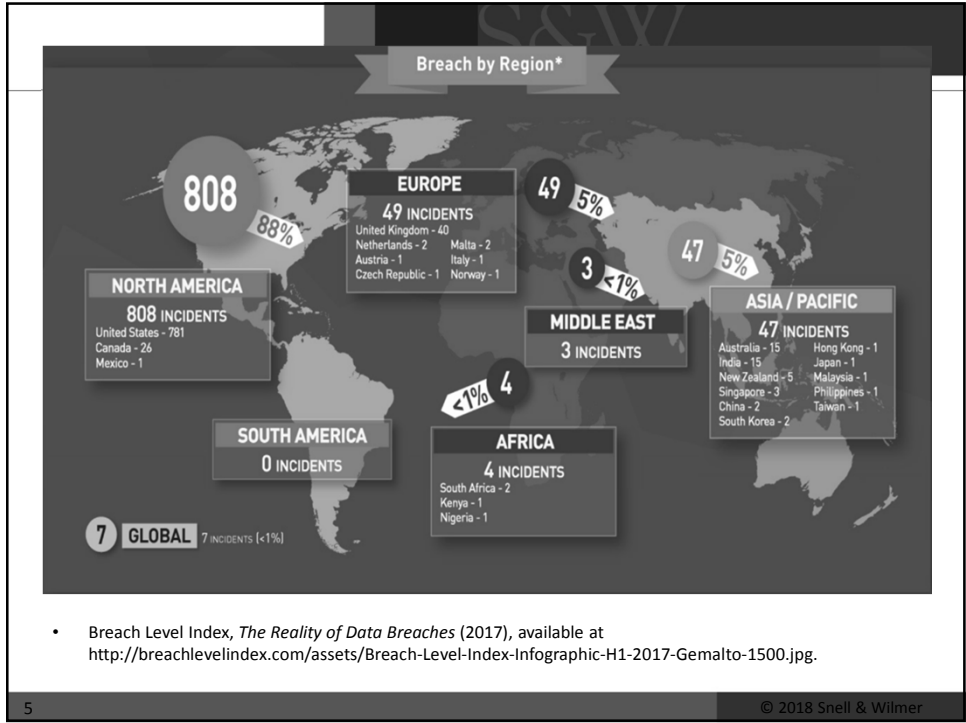
DATA RECORDS COMPROMISED IN FIRST HALF OF 2017

1,901,866,611

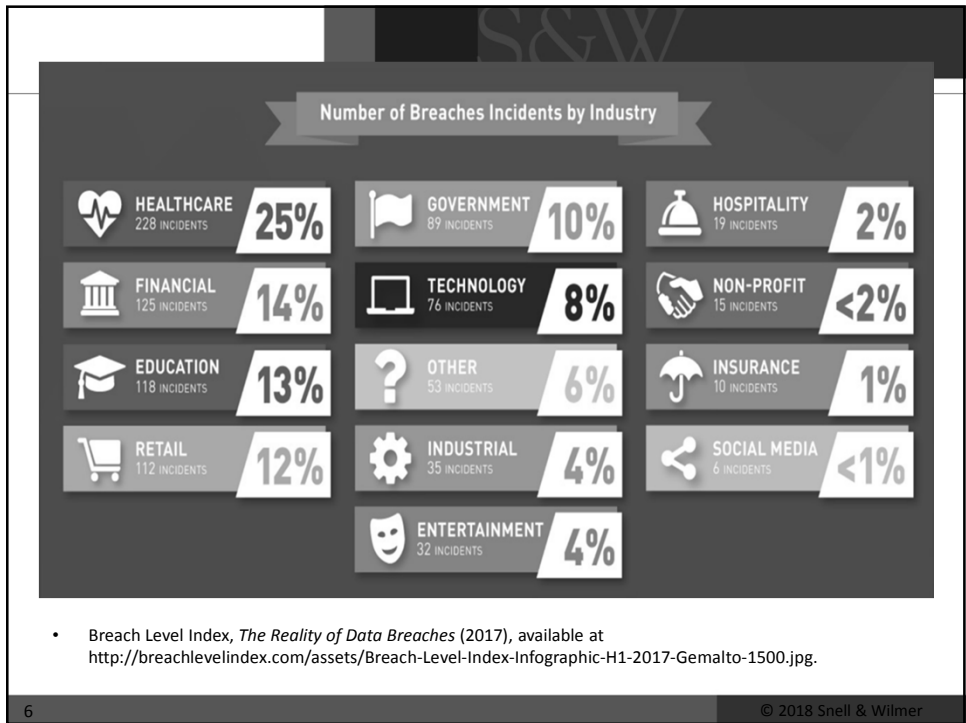
| | | | |
|---|----------------------------------|----------------------------------|--------------------------------|
| 10,507,550 records lost or stolen every day | 437,815 records every hour | 7,297 records every minute | 122 records every second |
|---|----------------------------------|----------------------------------|--------------------------------|

- Breach Level Index, *The Reality of Data Breaches* (2017), available at <http://breachlevelindex.com/assets/Breach-Level-Index-Infographic-H1-2017-Gemalto-1500.jpg>.

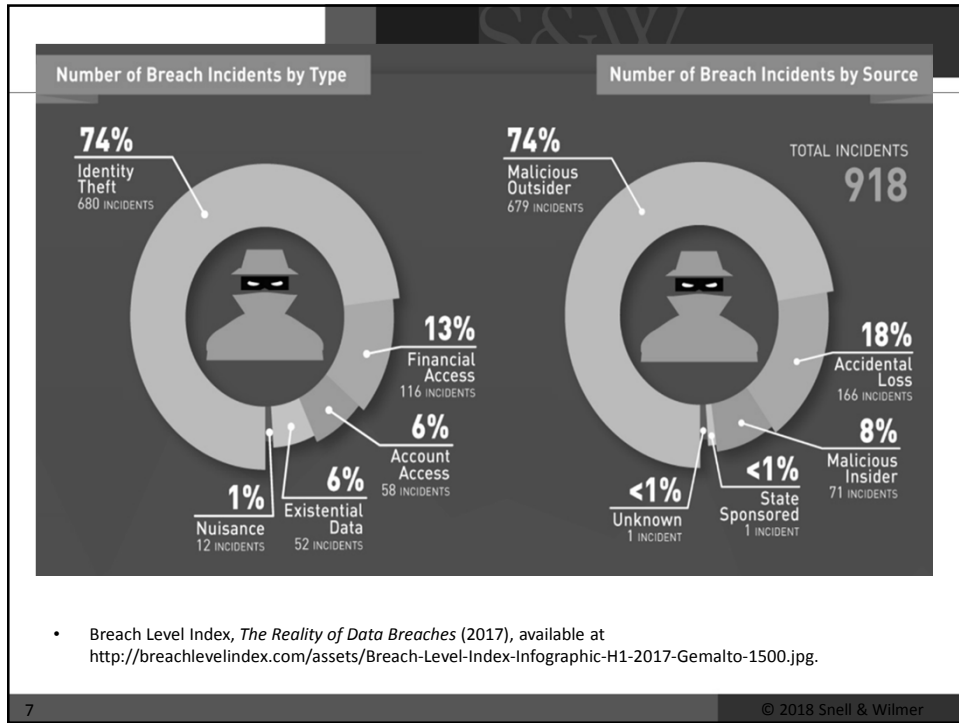
4 © 2018 Snell & Wilmer



5




6



The Reality of Data Breaches


- Data breaches are a real threat
- This could happen to your company
- The best time to prepare is now, before a breach occurs



Presentation Overview

1. The Reality of Data Breaches
- 2. Attorney-Client Privilege & Work Product Doctrine**
3. Best Practices to Preserve the Privilege


9 © 2018 Snell & Wilmer



Assume Potential Disclosure

- U.S. Supreme Court in *United States v. Bryan*, 339 U.S. 329(1950):
 - “There is a general duty to give what testimony one is capable of giving, and any exemptions which may exist are distinctly exceptional, being so many derogations from a positive general rule.”
- You are required to disclose communications or reports unless an exception applies
- Treat everything as potentially subject to disclosure


10 © 2018 Snell & Wilmer



Information Generated

- Responding to a cyber event might generate several types of communications or reports that you may want to consider seeking to protect from disclosure
- These include:
 - Assessment of network vulnerabilities
 - Suggestions for improvements of cybersecurity
 - Previous incidents
 - Management knowledge of previous incidents
 - Consumer complaints
 - Proof of negligence
 - Failure to notify of incident
 - Employee error (phishing)


11 © 2018 Snell & Wilmer



Disclosure Risk

- Goal: Minimize disclosure risk in responding to cyber incident
- Several adverse parties might seek to discover/make public information that a company or its agents generate in response to a cyber incident:
 - Opposing Lawyers
 - Regulators
 - Press

12 © 2018 Snell & Wilmer



Opposing Lawyers Seeking Info

- 1. FTC and State Attorneys General**
 - Consumer Financial Protection Bureau: prohibits unfair, deceptive, or abusive practices
- 2. SEC**
 - Disclosure requirements for public companies
- 3. Shareholders**
 - Securities fraud (alleged impact on stock price)
 - Derivative actions (alleged breach of fiduciary duties of care or oversight regarding management of cyber risks or adequacy of public reporting)
- 4. Business parties**

Litigation not common; usually handled via negotiation

 - Contract claims (e.g., compliance with law, notification, etc.)
 - Other alleged duties (duty of care owing to “special relationship” or statutory obligations)
- 5. Private plaintiffs**
 - Tort law (e.g., negligence, invasion of privacy, etc.)
 - Statutory (e.g., FCRA, state laws, etc.)
 - Contract claims (e.g., customer agreement, privacy policy, etc.)
 - Misrepresentation of practices

13 © 2018 Snell & Wilmer



Regulators Seeking Info

- Regulators seeking information may include:
 - State Attorneys General and state agencies
 - Federal Trade Commission
 - Department of Health and Human Services
 - Securities and Exchange Commission
 - Federal Bureau of Investigation
 - U.S. Secret Service

14 © 2018 Snell & Wilmer

Protected Information

- Neither federal nor state courts recognize a stand-alone privilege for cybersecurity communications or work product
- Categories of information protected from disclosure:
 1. Attorney–client privilege
 2. Work product doctrine
- Goal is to keep information generated in Incident Response efforts in these protected categories

15

© 2018 Snell & Wilmer

Attorney-Client Privilege

- Strongest form of protection
- Protects communications between attorneys and clients in seeking and providing legal advice
- May include non-lawyers who are assisting the attorney in representing the client
- Protects
 - Communications between a client and attorney
 - For the purpose of rendering legal advice
 - Made in confidence

16

© 2018 Snell & Wilmer

Work Product Doctrine

- Unlike attorney–client privilege, which covers communications, the work-product doctrine covers work prepared by attorneys or representatives
- Federal Rule of Civil Procedure 26(b)(3)
 - “Ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent).”

17

© 2018 Snell & Wilmer

Work Product Doctrine

- Weaker form of protection
- Protects information
 - prepared in anticipation of litigation
 - by or for a party or its representative
- Might still be subject to disclosure if another party
 - has a substantial need for the information and
 - cannot get it elsewhere without undue hardship

18

© 2018 Snell & Wilmer

Protections Applied

- *Genesco v. Visa*, 302 F.R.D. 168 (M.D. Tenn. Mar. 10, 2014)
 - Retailer’s GC retained cybersecurity consultant.
 - Agreement with consultant stated that engagement was “in anticipation of potential litigation and/or legal or regulatory proceedings.”
 - In litigation, opposing party sought work product of consultant and deposition of consultant and GC.
 - Court largely denied discovery requests.

19


© 2018 Snell & Wilmer

The Danger of Implicit Waiver

- *Leibovic v. United Shore Financial Services, LLC*, 2017 WL 3704376 (E.D. Mich. Aug. 28, 2017)
 - The privilege cannot be used as both “a sword and a shield.”
 - United Shore disclosed the conclusions from its forensic firm’s reports, but asserted work product protection over the reports.
 - The court found that United Shore implicitly waived privilege to the reports when it disclosed its conclusions.

20


© 2018 Snell & Wilmer



Presentation Overview

1. The Reality of Data Breaches
2. Attorney-Client Privilege & Work Product Doctrine
- 3. Best Practices to Preserve the Privilege**

21 © 2018 Snell & Wilmer



Best Practices

1. Consider adding outside counsel to **ALL** internal and external correspondence, including phone calls, e-mail and text messages
2. Consider directing all internal and external correspondence to outside counsel
3. Consider marking attorney correspondence with “attorney–client privilege/confidential”
4. Consider marking reports generated in anticipation of litigation with “work product” on each page

22 © 2018 Snell & Wilmer

S&W

Best Practices

5. You may want outside counsel to retain and direct the work of the cybersecurity consultants
6. You may want to exercise caution when sharing information about Incident Response with third parties
7. Consider limiting employees with access to privileged information

23 © 2018 Snell & Wilmer

THANK YOU

S&W



James P. Melendres, Partner
Co-Chair, Cybersecurity, Data Protection, and Privacy Practice
Chair, White Collar Defense & Investigations
602.382.6555 | jmelendres@swlaw.com

www.swlaw.com/blog/data-security

24 © 2018 Snell & Wilmer