RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: LAW-R05

Preserving the Privilege During Breach Response

Jeff Kosseff

Assistant Professor, Cybersecurity Law
United States Naval Academy
@jkosseff
(views are only those of presenter and not of Naval Academy or DOD)

#RSAC

Overview

- What information is produced after a data breach?
- Why do you want this information to be kept confidential?
- What evidentiary privileges might prevent you from being forced to disclose this information in court?
- How do you increase the chances of a privilege protecting your cybersecurity investigation?

Presenter's Company Logo – replace on master slide

Types of Cybersecurity Services

- Prophylactic
  - Policy Development
  - Audits/Assessments
  - Incident Response Plan Development
- Remedial
  - Responding to Incident (technical, forensics, legal, PR)

Presenter's Company Logo – replace on master slide

Cybersecurity communications/reports may contain…

- 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)
- Criminal acts of employees

Presenter's Company Logo – replace on master slide

- From: Joe Consultant
- To: CIO
- Re: Big Problems!

I have completed my initial assessment of your systems after last week's incident. I highly recommend that you immediately switch CRM software vendors. I have detected a number of significant vulnerabilities that could easily expose more customers' unencrypted payment card information, names, and addresses.

Also, your firewall has more holes in it than swiss cheese.

This is urgent!

Presenter's Company Logo – replace on master slide

- From: CIO
- To: Mid-level IT manager
- Fwd: Big Problems!

FYI. I'm sure he's overreacting. Our CRM vendor is top-notch. I should know – my brother is the VP of sales. I hired this consultant to appease a few over-anxious board members, not to create more work for us. Just keep an eye on this, but I don't think that you need to do any follow-up immediately.

Presenter's Company Logo – replace on master slide

Who would like this information to be public?

- Plaintiffs' lawyers
- Regulators
- The press
- Plaintiffs' lawyers

Presenter's Company Logo – replace on master slide

Always assume that evidence is subject to discovery in court

- U.S. Supreme Court in *United States v. Bryan* (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.”
- In other words, you have to testify or turn over emails or reports unless a privilege applies

Presenter’s Company Logo – replace on master slide

But cybersecurity reports and emails are automatically privileged, right?

- No

Presenter's Company Logo – replace on master slide

Even if they contain *really* confidential information?

- Really, no.
- Neither federal nor state courts recognize a stand-alone privilege for cybersecurity work product or communications

Presenter's Company Logo – replace on master slide

What about other privileges?

- Three privileges *might* apply to cybersecurity communications and work product:
  - Attorney-client privilege
  - Work product doctrine
  - Non-testifying expert privilege

Presenter's Company Logo – replace on master slide

Overview of Privileges that Might Apply to Cybersecurity

Subhead if needed

Attorney-Client Privilege

- Protects communications between attorneys and clients in the course of seeking and providing legal advice
- May include non-lawyers who are assisting the attorney in representing the client
- When it applies, offers nearly absolute protection
- Only protects
  - *Communications* between a client and attorney
  - *For the purposes of rendering legal advice*
  - *That are made in confidence*

Presenter's Company Logo – replace on master slide

Attorney-Client Privilege

- Only protects communications, not the underlying evidence
- Attorney must be involved and central to the communications
- Does not apply to communications that further crime or fraud

Presenter's Company Logo – replace on master slide

Work Product Doctrine

- Unlike attorney-client privilege, which covers communications, the work product doctrine covers an attorney's work product
- 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)."

Presenter's Company Logo – replace on master slide

Work Product Doctrine

- More likely to apply to cybersecurity professionals' work product
- Courts have held that the work product doctrine applies to materials prepared by environmental consultants, medical device safety consultants, and insurance claims investigators

Presenter's Company Logo – replace on master slide

Work Product Doctrine

- But unlike the attorney-client privilege, the work product doctrine is not absolute
- Discovery of work product is allowed if “the party shows that it has **substantial need** for the materials to prepare its case and cannot, **without undue hardship**, obtain their substantial equivalent by other means” or if a court otherwise finds good cause to order the disclosure of relevant work product

Presenter’s Company Logo – replace on master slide

Non-Testifying Expert Privilege

- Fed. R. Civ. P. 26(b)(4)(B): “a party may not, by interrogatories or depositions, discover facts known or opinions held by an expert retained or specially employed by another party in anticipation of litigation or to prepare for trial and who is not expected to be called as a witness at trial”
  - **unless** the party can demonstrate “exceptional circumstances under which it is impracticable for the party to obtain facts or opinions on the same subject by other means.”

Presenter’s Company Logo – replace on master slide

Genesco v. Visa: Applying the Privilege to Cybersecurity

- Hackers accessed customer payment card information that was stored on a retailer's systems
- 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

Presenter's Company Logo – replace on master slide

Ten Tips to Increase the Odds that Your Work Will be Privileged

Subhead if needed

Ten Tips

- 1. Engage any third-party cybersecurity consultants through an outside attorney.
- 2. Contract and Statement of Work should be signed by attorney and consultant, not only by client and consultant.
- 3. Contract and statement of work should state that work is being performed in conjunction with legal advice. In the case of an investigation after an incident, the contract and statement of work should state that work is being performed in anticipation of litigation.

Presenter's Company Logo – replace on master slide

Ten Tips

- 4. Internal point of contact at company should be general counsel, not CIO.
- 5. Attorneys should be included on ***every*** email and other correspondence that involves company and cybersecurity consultant.

Presenter's Company Logo – replace on master slide

Ten Tips

- 6. Emails, memoranda, and other communications should have "**ATTORNEY-CLIENT PRIVILEGE/CONFIDENTIAL**" at the top of every page.

  Reports and other work product should have "**ATTORNEY WORK PRODUCT**" at the top of every page.

  But do not overuse these designations; only label material that could arguably be privileged.

Presenter's Company Logo – replace on master slide

Ten Tips

- 7. To the greatest extent possible, attorneys should direct the work of the cybersecurity consultant. Their involvement should not be formalistic. Attorneys must have final say over ***all*** statements to outside parties, including customers, vendors, regulators, and the press.

Presenter's Company Logo – replace on master slide

Ten Tips

- 8. Be careful about sharing information with third parties, particularly vendors that may have been the root cause of a data security incident.
- 9. Limit the employees with access to the communications and work product to those who have a need to know.
- 10. Educate all employees about privilege issues.

Presenter's Company Logo – replace on master slide

Bonus Tip

- NEVER assume that an email or report will be privileged.

Presenter's Company Logo – replace on master slide

Apply What You Have Learned Today

- In the next week, you should:
  - Determine the actors in your organization who generate or oversee cybersecurity reports and information
- In the next month, you should:
  - Determine how these actors designate confidential communications and work product
- In the next six months you should:
  - Develop a plan to increase the chances that an existing privilege will apply to your cybersecurity reports and communications, using the ten tips above

Presenter's Company Logo – replace on master slide

Questions?

- kosseff@usna.edu

Presenter's Company Logo – replace on master slide