POLSINELLI®
What a law firm should be.℠

Cybersecurity Legalities

Matt Frontz

Introduction

- Incident Response Process
- Attorney/Client Privilege
- Duty of Care of Certain Employees
- Contractual Mitigation Strategies
- Can you pay a Ransom?
- Notification of a Breach

Incident Response Process

- Pre-Breach
- Containment
- Remediation
- Investigation
- Notification

POLSINELLI®

What a law firm should be.℠

Pre-Breach

- Adopt/Update Incident Response Plan
  - Establish/review makeup of Incident Response Team (Incident Lead, Executive Team, HR, PR, Sales and Customer Service, Forensics, Security, **Legal**, Law Enforcement, and Solution Providers)
  - Establish CLEAR communication protocols and defined areas of responsibility
  - Create a matrix of breach notification obligations
  - Draft form notification letters
  - Stress test the plan/conduct response drills

Containment and Third-Party Engagement

- At the same time the organization is taking steps to contain the incident, someone should be notifying your insurance carrier and seeing that **legal counsel** and a forensics vendor are engaged.
  - Engaging forensics at this point can help ensure forensic evidence is properly preserved and endpoint monitoring is promptly deployed.
  - **Involve Legal Counsel early for both legal analysis and privilege purposes**
  - **Legal Counsel should be engaging third parties for privilege purposes**

What is Legal Counsel Doing?

- Legal Counsel
  - Coordinating the Investigation and Response Under Privilege
  - Updating Incident Response Plan to address issues
  - Analyzing Legal Obligations Under the Applicable Law
  - Complying with Notification Requirements
    - During investigation drafting communication for notifications
  - Working with media relations
  - Responding to Regulatory Investigations

What is Attorney/Client Privilege

- Rule 1.6 Confidentiality of Information
- A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation.
- This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct.

What is Protected Under Attorney/Client Privilege

- What is protected?
  - Legal Advice
- Why is this important for a breach investigation?
  - If legal counsel is conducting the investigation with the third party, legal its counsel's investigation and protected under the privilege
  - Criminal Activity
  - Law Enforcement/ National Security
  - Employee Issues

State of the Law

- State of the law (US):
  - Still no single Federal law or regulation addressing privacy or security of PII
  - Notification requirements largely a function of state law and subject to numerous variations and exceptions
  - 50 different state laws on notification
- GDPR - is intended to help strengthen and unify data protection for all individuals within the EU
- EU-U.S. Data Privacy Framework (adopted July 2023 replacing the Safe Harbor)
  - EU prohibits the transfer of Personal Data to countries outside of the EU unless those countries provide "adequate" legal protection with respect to the handling of that information
  - US companies must be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC), the U.S. Department of Transportation (DoT), or other statutory body that can ensure compliance with the Privacy Framework

Other Laws

- Many other Federal data privacy and security laws and regulations:
  - Health Information: Health Insurance Portability and Accountability Act (HIPAA); Health Information Technology for Economic and Clinical Heath Act (HITECH); Office for Civil Rights (OCR) rules
  - Credit Records: Fair Credit Reporting Act (FCRA); Fair and Accurate Credit Transactions Act (FACTA)
  - Financial Transactions: Graham-Leach-Bliley Act (GLBA)
  - Children: Children's Online Privacy Protection Act (COPPA)
  - Identity Theft: FTC's Red Flags Rule
  - Students: Family Educational Rights and Privacy Act (FERPA)
  - Public Companies: Sarbanes-Oxley Act (SOX); SEC Regulations

Do Different Employees Have Different Duties?

- Officers and directors face heightened duties
- Directors owe shareholders two basic fiduciary duties:
  - (1) Duty of Care
    - Failing to manage and monitor cybersecurity violates the Duty of Care
    - Ignoring the potential cybersecurity risks is a breach of the Duty of Care
  - (2) Duty of Loyalty
    - Failure to implement reporting system and controls
    - Failure to monitor and oversee the operations of such controls
    - Failure to act, or to allow a situation to develop and continue

Mitigation Strategies - Contractual

- Ensure compliance with laws and regulations by subcontractors and vendors
- Confidentiality of data/ownership of data/use of data/etc.
- Warranties and covenants should adequately address heightened cybersecurity risks
- Termination rights and adequate transitions
- Indemnification (breach, investigation, notification, remediation, identity theft protection, government imposed penalties)
- Carve-outs to limitations on liability and consequential damages
- Exit strategy/return of data on request/purging and destruction of data

Is it legal to pay a cyber ransom?

- FBI
- "The FBI does not support paying a ransom in response to a ransomware attack."
- Payment does not guarantee an organization will regain access to its data.
- Payment encourages perpetrators to target more victims.
- Entities should report ransomware incidents.

- EU member states can impose fines for paying ransoms under the Security of Network and Information Systems Directive

- OFAC
- U.S. Department of Treasury *Office of Foreign Assets Control*
- Advisory on Potential Sanctions for Facilitating Ransomware Payments (October 1, 2020)
- Potential civil and criminal penalties for facilitating ransomware payments to individuals on OFAC's Specially Designated Nationals and Blocked Persons List
- Strict Liability
- Must report to Gov't when hacked and/or pay ransomware

To Pay or Not to Pay

The arguments for rendering payment include:

- least costly option.
- In the best interest of stakeholders.
- Avoid fines for losing important data.
- Not losing highly confidential information.
- Not going public with the data breach.

The arguments against payment include:

- Payment does not guarantee you get your data back
- Payment enables continued cycle of ransomware crime.
- Payment can damage to a corporate brand.
- Payment may not stop the ransomware attacker from returning.
- If everyone stopped paying, market for ransomware would disappear.

What Happens if a Cyber Ransom is Illegal?

- *Guidance from OFAC (September 21, 2021)*
- Describes three “mitigating” factors OFAC will consider when determining how to respond to an apparent illegal ransom payment:
  - 1. Company’s implementation of a regulatory compliance program.
  - 2. Company’s “meaningful steps” to reduce the risk of cyber extortion
  - 3. Company’s decision to self-report a ransomware attack to OFAC, law enforcement, and other regulatory agencies, and to thereafter fully cooperate with any investigation from these groups.

Joseph Sullivan – Uber Chief Security Officer

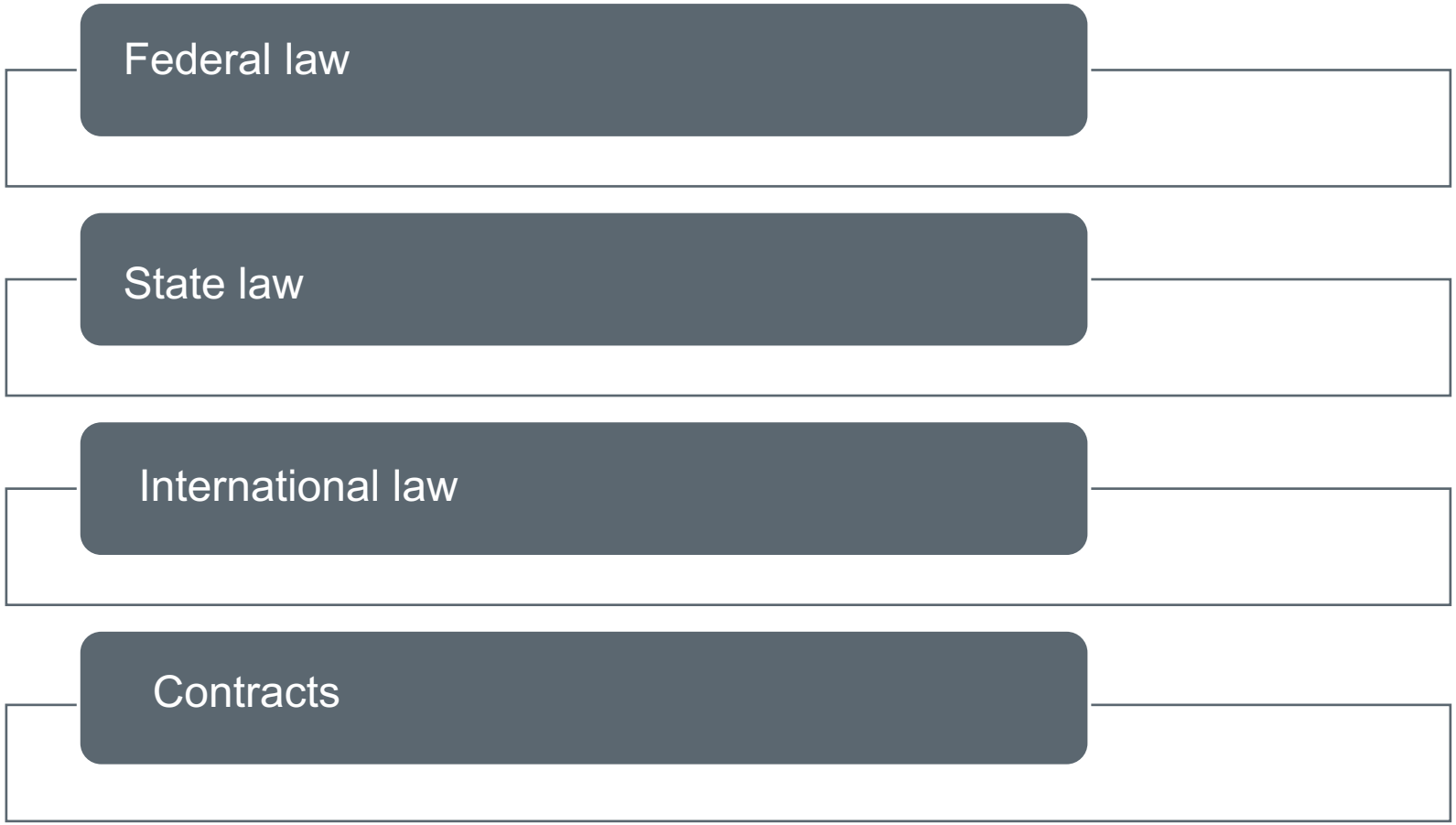
Guilty of Obstruction of the FTC and Misprision of a Felony

- Uber suffered a data breach in 2014. The FTC commenced an investigation into Uber's data security program.
- In April 2015, Uber hired Joseph Sullivan as its Chief Security Officer. In May 2015, the FTC served a detailed Civil Investigative Demand on Uber, which demanded information about any other instances of unauthorized access to user personal information and information regarding Uber's broader data security program and practices.
- Sullivan played a central role in Uber's response to the FTC and testified under oath to the FTC on November 4, 2016, regarding Uber's data security practices. Sullivan's testimony included specific representations about steps he claimed Uber had taken to keep customer data secure.
- Ten days after Sullivan's FTC testimony, he learned that Uber had sustained a second breach (same vulnerability).
- The threat actors reached out to Sullivan directly, via email, on November 14, 2016, claimed that they had stolen Uber user data and demanded a ransom payment from Uber in exchange for deletion of that data. Sullivan's team verified the threat actor's claims and identified unauthorized acquisition of records for approximately 57 million Uber users and 600,000 driver license numbers.
- Sullivan had the threat actor enter into an NDA saying that it never acquired documents, which was not true.
- Sullivan did not inform Uber management, and Uber did not notify impacted individuals or the FTC.
- Sentenced to three years probation on May 4, 2023

Joseph Sullivan – Uber Chief Security Officer Lessons Learned

- Take seriously requests from, and agreements with, any government agency and consider the ongoing nature of certain requests and disclosure obligations.
- The FTC is taking an active role in investigating significant data breaches. While there is no generally-applicable federal law that requires notice to the FTC of a data breach, the FTC uses its broad authority under Section 5 of the FTC Act to challenge unfair or deceptive practices that arise from, or are exposed by, a data breach.
- There continues to be a growing list of reasons to promptly notify law enforcement of criminal activity arising from a data breach.
- Delayed reporting of a data breach significantly increases the risk to the organization and its decisionmakers.
- Cybersecurity and privacy professionals within an organization should be transparent with leadership about potential incidents and should document the incident, the steps taken in response, and any decisions made in accordance with an established incident response plan.

Notification - a data incident trigger legal obligations?



Notify Affected Individuals and Regulators (As Necessary)

- Discuss Forensic Findings*
- Legal Counsel will Assist with Analyzing Notification Obligations
- Notifications may be Necessary if Personal Information has been Accessed or Exfiltrated
- May Need to Notify Regulators Depending on State Law
- Credit Monitoring
- Notification Vendors

Why would a data incident trigger legal obligations? – *State laws*

- Applicable state law determined by the state(s) of residency of involved individuals.
- State laws vary on topics such as:
  - Definition of personal information and breach
  - Timing and Content of notification
  - Notification to state Attorney General or other regulators
  - Applicability to paper records
  - Exemptions for regulated entities
- Owners – Duty to notify affected individuals, regulators, and consumer reporting agencies.
- Service Providers – Duty to notify the owner.
- Regulators include state attorneys general, consumer protection divisions, and others.
- Regulators use data breaches as an opportunity to audit privacy practices.
- Regulators often rely on consumer fraud statutes, so it is important to be cautious in public facing statements about the organization's data security.

Ransomware Event – Notification Considerations

- State breach notification laws focus on data access or acquisition.
  - In a traditional ransomware incident, there has been no data access or acquisition.
  - Oftentimes the only information impacted are user credentials
  - For this reason, ransomware incidents may be widely underreported.
- Note, however, that HHS's ransomware guidance states that access is presumed.
- Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)
  - Will require reporting of cyber incidents to the Cybersecurity and Critical Infrastructure Agency (CISA) within 72 hours of a substantial cyber incident and within 24 hours of paying a ransom.

Where great work and great people come together.

POLSINELLI®

What a law firm should be.℠

Am Law 100 firm with
1,000 attorneys nationwide
23 offices from LA to NY
170+ services/industries
polsinelli.com

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements. Copyright © 2022 Polsinelli PC. Polsinelli LLP in California, Polsinelli PC (Inc) in Florida.

POLSINELLI®

What a law firm should be.℠

Polsinelli PC provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

© 2022 Polsinelli® is a registered trademark of Polsinelli PC. Polsinelli LLP in California. Polsinelli PC (Inc.) in Florida.

polsinelli.com