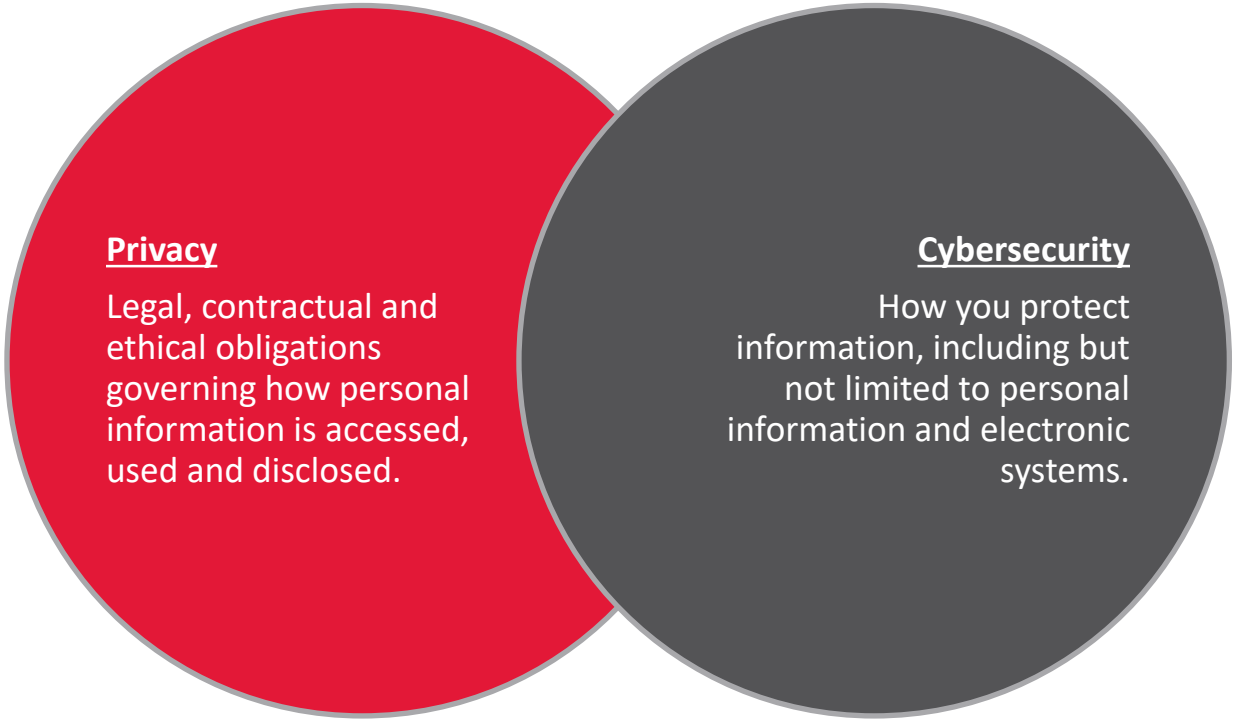
DIGITAL TRANSFORMATION (DT) Supply Chain Risk Management: a Legal Imperative for Cybersecurity and Data Privacy

OCTOBER 26, 2021

Jeff Schultz
Romaine C. Marshall
Dustin Berger

Always exceed expectations through teamwork and excellent client service.

Simple Definitions



Governed by a patchwork of legal, industry and regulatory standards

ATDT Fall Series: Session 1 Recap

- ***Navigating the Patchwork of Cybersecurity and Data Privacy Laws that Govern***
- **"Common Threads" Emerge**
  - Cybersecurity
    - Incident Response Plans (IRPs)
    - Risk Assessments (RAs)
    - Written Information Security Programs (WISPs)
  - Data Privacy
    - Privacy Policies and Procedures
    - Privacy Reviews, Data Privacy Impact Assessments (DPIAs)

ATDT Fall/Winter Series

- ***Supply Chain Risk Management: a Cybersecurity and Data Privacy Imperative***
  - Tuesday, Oct. 26, 2021
- ***The Internet of Things, Emerging Technologies, and the Cybersecurity and Data Privacy Laws Implicated***
  - Wednesday, Dec. 8, 2021
- ***ATDT Winter Series preview***
  - February, March, April 2022 (dates TBD)
  - Blockchain, AI, drones, *etc.,* cybersecurity and legal risks
  - Data privacy readiness, *e.g.*, Cal. Privacy Rights Act *et al*

DT and The Pandemic

- ***The process of leveraging technology, people and processes to innovate and stay competitive.***
- ***"We've seen two years' worth of [DT] in two months."***
  - Satya Nadella
- **DT has led to businesses managing more than 10 times the quantity of data they did five years ago per poll of 1,000 execs.**
- **DT has increased reliance on third parties. Last year, of the 883 IT Security and C-Suite executives surveyed:**
  - 58% say their primary change is increased cloud migration
  - 56% find it challenging to ensure third parties have P&Ps that guarantee security of their information

Source:

The Threat

Cyber Supply Chain Incidents

- **"From December 2020 to July 2021, SolarWinds, Accellion, Microsoft and Kaseya … suffered cyberattacks so enormous that remediation and restoration efforts could take years."**
- **SolarWinds (SaaS provider)**
  - At least 18,000 of 30,000 impacted; malicious updates pushed out
  - Three class action lawsuits by shareholders against SW and Senior Executives
  - "[SW] failed to employ adequate cybersecurity safeguards and did not maintain effective monitoring systems …"

Cyber Supply Chain Incidents

- **Microsoft (Exchange email provider)**
  - At least 30,000 victims in the U.S., 100,000s globally
  - “Web shell” backdoor has given cyber criminals total access to all email
  - BACKUP ANY DATA STORED ON EXCHANGE IMMEDIATELY
- **Kaseya (IT solutions provider for MSPs)**
  - Threat actors leveraged software vuln. against MSPs and customers
  - Kaseya has 35,000 MSP customers, 800-1500 SMBs predicted ransomed, 60 deeply penetrated
  - On July 22, Kaseya announced it received the decryption key

Supply Chain Risk Definition

NIST definition:

- *Risks that arise from "an occurrence within the supply chain whereby the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits is jeopardized. A cyber supply chain incident can occur anywhere during the life cycle of the system, product or service."*

- *Source: NIST SP 800-161, Rev. 1 (2021) at Appendix E*

Law and Regulations

Blackbaud Supply Chain Litigation

- **Lawsuit Against Blackbaud and Harvard:**

"Failed to conduct proper and reasonable due diligence over Blackbaud and its security systems, practices and procedures."

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

DANIEL COHEN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

BLACKBAUD, INC., a Delaware corporation, THE PRESIDENT AND FELLOWS OF HARVARD COLLEGE, a Massachusetts not-for-profit corporation, BANK STREET COLLEGE OF EDUCATION, a New York not-for-profit corporation, and LOWER EAST SIDE TENEMENT MUSEUM, a New York not-for-profit corporation,

Defendants.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

FTC vs. Ascension (2021)

- FTC alleged that vendor, OpticsML, which Ascension hired to scan mortgage documents, had no protections to block unauthorized access
- FTC also alleged that Ascension failed to adequately vet OpticsML and other vendors, and that Ascension's contracts with vendors did not require them to safeguard information
- Ascension agreed to conduct written assessments of each vendor to determine the continued adequacy of their safeguards, and to select and retain vendors capable of safeguarding personal and sensitive information

Protections

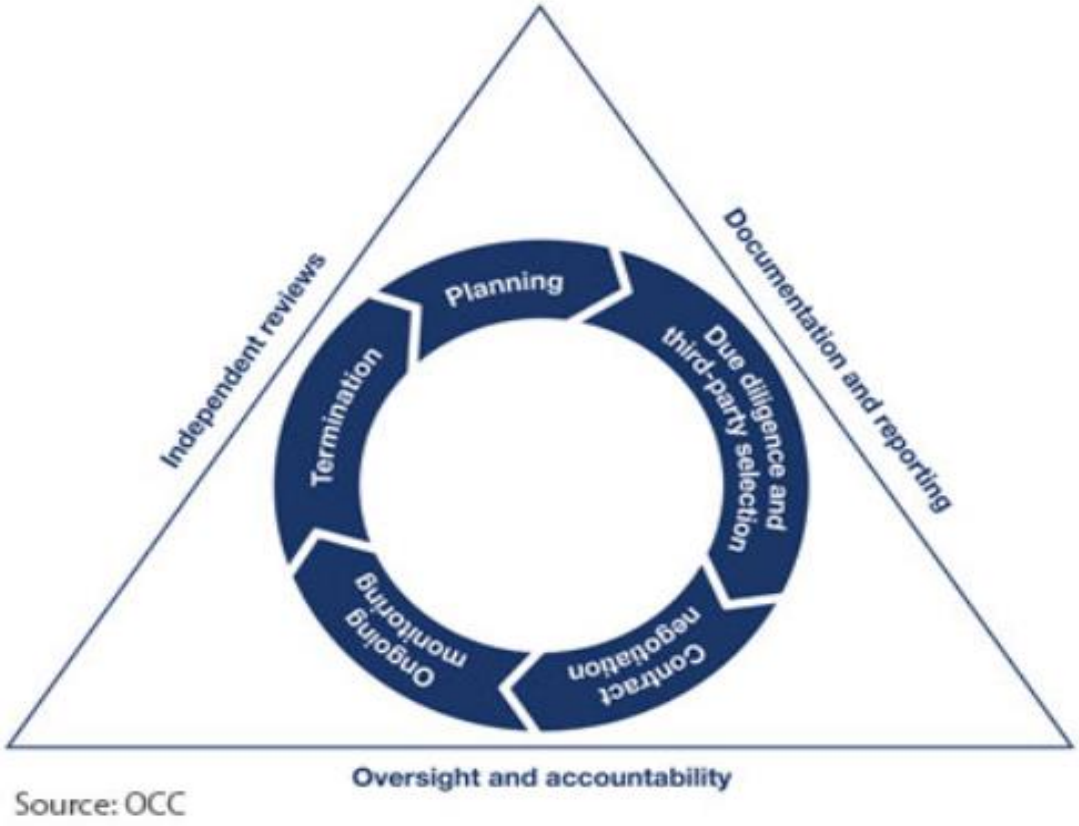
You Should Implement

Federal Reserve, FDIC and OCC Guidance

- Recently published guidance on how banks should manage third-party risks (yet to be finalized)
- Intended to cover risk management practices for all stages in the life cycle of third-party relationships
- The guidance defines a third-party relationship as “any business arrangement between a banking organization and another entity, by contract or otherwise”

Risk Management Life Cycle

(Planning, Due Diligence, Contract Negotiating, Monitoring, Termination)



Source: OCC

Planning

- Understand potential information security implications including access to the organization's systems and to its confidential information.
- Describe how the organization will select, assess and oversee the third party, including monitoring the third party's compliance with contractual provisions.
- Outline the banking organization's contingency plan in the event the banking organization needs to transition the activity to another third party or bring it in-house.

Due Diligence

- Evaluate the third party's ownership structure and its legal and regulatory compliance capabilities.
- Assess the third party's financial condition, including review of the third party's audited financial statements, annual reports, and other available information.
- Assess the third party's degree of and its history of managing customer complaints or litigation.
- Determine how long the third party has been in business and whether there have been significant changes in the activities offered or in its business model.

Contract Negotiation/DPAs

- Data protection agreements (DPAs) are the best way to ensure vendors protect your data.
- The negotiation process affords an opportunity to vet a vendor's data security and privacy programs.
- The DPA fosters compliance with privacy and security laws as well as business requirements for privacy and security assurance.
- The DPA also allows parties to explicitly address privacy and security issues of concern to their business, such as rights to data, procedures in the event of a security incident, and responsibilities for data subject and regulator requests.
- Red flags include low liability limits for security incidents, a lack of transparency, or vagueness in the commitments to security and privacy.

DPA Best Practices

- Address cross-jurisdictional transfers of personal data.
- Cover all your data – not just personal data.
- Use a super-cap for security incident liability limits.
- Embed a standards-based security questionnaire to learn more about the vendor's security program.
- Address costs and timeframes in situations where cooperation will be required.
- Use straight-forward language so that business and technical professionals on both sides of the deal can understand their obligations.

DPA – Other Diligence

- For most vendors handling data, have a program to regularly review vendors' compliance with their DPA obligations.
- For some vendors, this may mean reviewing their audit reports.
- For others, it may mean asking them to complete a questionnaire.
- Consider also asking for audits or questionnaires if a question about the vendor's compliance arises.

Ongoing Monitoring

- Approve, or delegate to, an appropriate committee reporting to the board, and approval of contracts with third parties that involve critical activities.
- Review the results of management's ongoing monitoring of third-party relationships involving critical activities.
- Confirm that management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring.

Termination

- Assess changes to the third party's business strategy, legal risk and its agreements
- Evaluate the third party's financial condition and changes
- Review the adequacy of the third party's insurance coverage
- Review relevant audits and other reports from the third party
- Monitor for compliance with applicable legal and regulatory requirements

Responses

You Should Have Ready

Incident Response Plan

- **What Should an IRP include?**
  - An Incident Response Team (IRT):
    - Individuals with *clearly defined roles and responsibilities*
  - Roles that:
    - provide timely, organized, and effective response;
    - avoid loss of or damage to IT systems, network, data;
    - minimize economic, reputational, or other harms; and
    - manage litigation, enforcement and other risks.

Why RA?

- **Risk assessments**
  - Lead to policies, then standards, then procedures – all of which come together to comprehensively outline objectives and administrative, technical and physical controls.
- **Risk assessments should**
  - Should assess at least once every 12 months, internal and external risks to the security, confidentiality, or integrity of personal or sensitive information and systems.

Key WISP Elements

- **Examples of Technical Controls**
  - Information Protection and Control
  - Vulnerability Assessments
  - Penetration Testing and Quarterly Scanning
  - Identity and Access Management
  - Detective Measures
  - Security Patches
  - Asset Management
  - Mobile Device Management
  - Email Management
  - Vendor Management

About Armstrong Teasdale

Overview of Armstrong Teasdale – Firm Information

For 120 years, Armstrong Teasdale has forged long-term relationships with clients large and small around the globe.

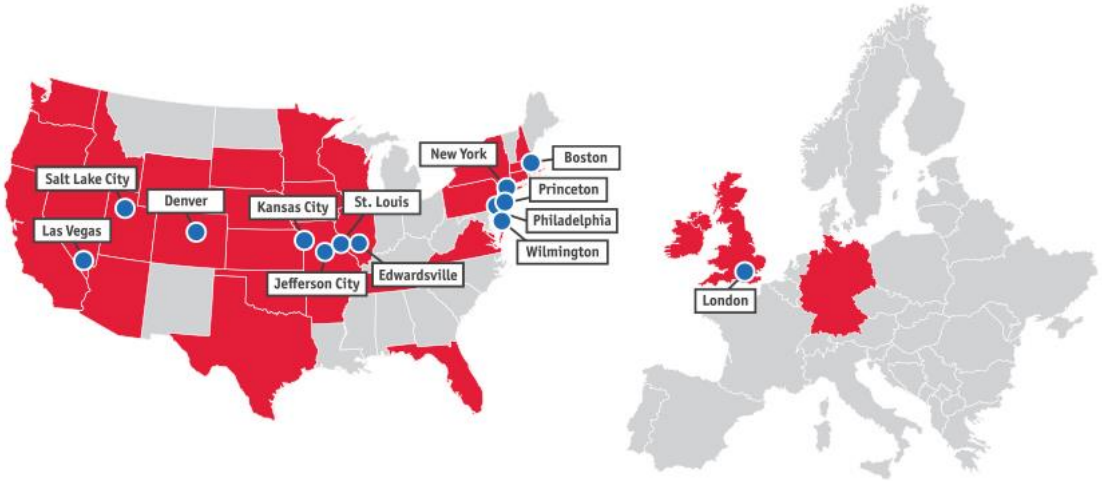
350+
— LAWYERS —

300+
— STAFF —

— SERVING OVER —
125+
FORTUNE 500 COMPANIES

— AM LAW —
200

With 13 offices across the U.S. and in London, our lawyers are licensed to practice in 30 states plus Washington, D.C., as well as in the U.K., Germany and Ireland.



**As of Oct. 2021*

Jeffrey Schultz
St. Louis
jschultz@atllp.com
314.259.4732

Scott Galt
St. Louis
sgalt@atllp.com
314.259.4709

Romaine Marshall
Salt Lake City
rmarshall@atllp.com
801.401.1604

Dustin Berger
Denver
dberger@atllp.com
720.722.7197