**Privacy and Data Security Due Diligence**

**By**

**Thomas Carey, Partner**

**Sunstein LLP, Boston MA**

Privacy and data security issues can scuttle a deal or at least cost the parties a lot of money. For example, in the due diligence process involving the 2017 acquisition of Yahoo by Verizon, Yahoo disclosed two serious data breaches that compromised over a billion accounts. Yahoo had previously attempted to cover this up. The deal went ahead for nearly $4.5 billion but not before Verizon knocked $350 million off the transaction price and Yahoo paid over $100 million to settle SEC fraud charges and class action lawsuits.

Privacy and data security issues come up in two ways in the due diligence process. First, there is the question of whether the due diligence process itself is secure and adequately protective of privacy rights. Once the process has been defined, more complex question of evaluating the privacy and data security issues of the target company.

While this paper generally describes the issues as they are presented to the investing or acquiring company, the mirror image of these issues exists for the target company. A company seeking to attract investors or buyers needs to anticipate the inquiry that will be forthcoming, and should consider addressing the issues well in advance of the due diligence process so as to present the picture of a company that has its house in order.

Throughout, the term "acquirer" used to mean either an acquirer or an investor.

# I. Organizing the Process

The due diligence team should include people with expertise in privacy and data security. They may include members of the target's management responsible for IT systems and security, and for its privacy policies and practices; external IT subject matter experts (SMEs), and possibly SMEs with expertise in compliance and risk management.

The acquirer and target should agree upon a process for sharing information. The parties should agree upon whether sharing personal information (PI) is necessary for the level of due diligence being carried out. Sometimes it is enough to share only aggregated or anonymized data. Before sharing PI, the parties should confirm that any pre-closing disclosures comply with applicable legal obligations and the target's own privacy policies and other public statements.

**The Data Room.** Data sharing is often conducted by means of an electronic data room (**EDR).** Before initiating the EDR process, the parties should agree on ownership and confidentiality of the data that is uploaded. Usually it is owned by the party doing the uploading.

Many EDRs are offered by third party service providers. Before committing to one, the parties should consider the security of the EDR, with an eye to such question as:

- Strong username and password controls
- Encryption
- Access control, such as watermarking
- Lock-down procedures
- Partitioning and the availability of additional security for highly sensitive information.

**Physical Records.** Privacy laws apply to physical records as well as electronic records. Consideration should be given to the management, organization and security of physical records, whether located on-site at the Target or in a warehouse.

**Electronic Records.** In order to gather the records, it will be necessary to locate them. Ideally there is a corporate data map in the custody of a records manager. In addition, it should be useful to identify:

- All in-house servers, network attached storage systems, and data warehouses
- A schedule of all cloud storage systems used by the target
- A schedule of personal computers used by the target. For laptops, determine whether encryption is applied at the drive level.

# II. Conducting the Due Diligence

## A. An acquirer's due diligence should focus on:

- Identifying the particular types of privacy and cybersecurity risks that the target company faces given its industry, geographic reach, customer base, and the nature of its products and services
- Understanding the target's network, and system architecture and data flows
- Understanding the amount of personal information, especially customer or patient personal information, that that target gathers
- Understanding the type of proprietary third-party information to which the target has had access
- Reviewing the promises that the target has made to its customers and users regarding privacy and data security
- Recognizing whether the acquirer will need to obtain post-closing consents to use personal information that is in the hands of the target
- Learning about any prior cybersecurity incidents of the target, and its response to those incidents
- Reviewing the target's compliance with applicable regulatory and industry standards and its own policies

## B. Review of Target Policies and Contracts

In reviewing policies of the company, particularly those that are customer facing, it is important to obtain current and past versions of the policies, including the dates in which they were in effect.

Contracts should be reviewed with an eye to the allocation of risk for data breaches and privacy violations (often in warranties, disclaimers and indemnity provisions). In addition, the acquirer should look for damages limitation clauses, provisions dealing with ownership of data, and that address control over reporting data breaches.

The acquirer should review privacy policies of the target and compare the policies to actual practices.

Data governance policies should address document retention (including on backup tapes and disaster backup sites), access control and the handling of litigation holds.

The acquirer should look for the existence of a formal policy that classifies data in accordance with its level of sensitivity and the compliance of the policy with any industry standards or governmental requirements applicable to the target. See, e.g., NIST's "Standards for Security Categorization of Federal Information and Information Systems", https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf .

Here is a checklist of the types of documents to obtain and review:

- The company's privacy policies, both internal and external
- The terms of use of its website
- Telemarketing and email marketing policies
- Results of any security audits, vulnerability scans and penetration tests
- Privacy impact assessment processes and reports
- Certifications (ISO 27001/2, PCS DSS, SOC)
- Business-to-business customer, vendor and supplier contracts
    - This can be particularly important if the target operates in, or has customers that operate in, regulated industries such as finance, health care, energy or telecommunications
- Incident response plans and playbooks
- Privacy and information security training materials
- A description of the target's internal privacy and security training programs and records of how often conducted and how broadly the training has been disseminated
- Employee background investigation policies (credit checks, drug test or other screening procedures employed) and onboarding process
- Organizational and reporting structure relating to the security function
- GDPR and CCPA compliance policies and materials, if applicable
- Cyber insurance policies (including claims history)
- Internal controls to guard against fraudulent requests for money

## C. Review of Target's Policies and Procedures

In reviewing the Target's policies and procedures, the acquirer should consider:

- Does the company's cybersecurity program mitigate security risks through controls that are
    - Administrative
    - Operational, and
    - Technical
- Does the Target have:
    - a written information security policy (WISP)
    - An employee-facing acceptable use policy?
    - A data classification and handling policy?
    - A data map and a data classification system?
    - An inventory of physical IT assets and privately held assets (such as cellphones) that have aces to the target's data?

    - A policy governing "self-help" cloud computing services such as Google Sheets, Google Drive, Dropbox, Evernote?
    - A policy governing the use of USB or other portable drives?
- Does the Target conduct regular risk assessments and vulnerability and penetration tests? If so, with what frequency?
- Does the Target have dedicated privacy and security personnel?
- Does that Target have an incident response plan that it tests?
- How does the Target manage vendor risks?
- Does the Target have a business continuity plan, a disaster recovery plan and back-up protocols?
- How does the company protect the physical security of its facilities and assets?
- Does the company use anti-virus software, encryption, access controls, network monitoring, authentication and asset management?
- Does the target have an insider threat program to detect potential theft of proprietary information or intellectual property?
- Does the Target conduct privacy impact assessments when implementing new systems or processes?

## D. Review of Past Breaches

If the Target has had prior data breaches, the due diligence inquiry should examine:

- How were the incidents detected?
- What period of time elapsed between the intrusion and its detection?
- Was data exfiltrated?
- Did the Target notify its cyberinsurance carrier?
- Did the Target consult with company counsel or outside counsel about its legal obligations?
- Was a third-party forensic consultant engaged to investigate the incident? If so, what was in the report provided?
- Did the Target file data breach notifications with governmental authorities?
- Has the Target experience a theft of intellectual property, including trade secrets?
    - Has it sent demand letters, cease and desist letters or threatened lawsuits against former employees on account of such possible theft?
- Has the Target been defrauded or extorted as a result of an email compromise?

## E. Compliance with Laws and Standards

The first task in this regard is to identify the privacy and data protection laws that apply to the Target. In addition to conducting its own review, an acquirer should ask the Target which laws, regulations and industry standards it seek to comply with.

Here's a list of laws, regulations and industry standards to consider:

### 1. Laws of General Applicability

- **Federal Children's Online Privacy Protection Act (COPPA)** – applies to the collection of information about children under the age of 13
- **Telephone Consumer Protection Act (TCPA)** – applies to robocalls and unsolicited transmission of faxes and text messages

- **EU General Data Protection Regulation (GDPR)** – Applies to collection of data pertaining to residents of the European Economic Area
- **Federal Trade Commission (FTC)** – While the FTC has not promulgated a general privacy regulation, it pursues enforcement actions against companies that it views as having unreasonably poor information security standard or that act in a manner contrary to their stated privacy policies
- **Controlling the Assault of Non-Solicited Pornography and Marketing Act (Can-Spam)–** regulates unsolicited email.
- **Sarbanes Oxley Act (SOX)** SOX imposes stringent requirements on financial reporting and intel controls, including data security measures, to prevent corporate fraud.
- **State Data Breach Notification Laws –** generally require reporting of data breaches to a governmental agency and to affected consumers
- **State Privacy Laws –** The grand daddy is the California Consumer Privacy Protection Act (CCPA), but don't overlook the California Shine the Light Act. Many other states have general privacy laws in effect or soon to be phased in. As of September 13, 2023, those states include:

| State | Effective Date | Statute |
|---|---|---|
| California | 1/1/20 | California Consumer Privacy Act |
| Colorado | 7/1/23 | Colorado Privacy Act |
| Connecticut | 7/1/23 | Connecticut Personal Data Privacy and Online Monitoring Act |
| Delaware | 1/1/25 | Delaware Personal Data Privacy Act |
| Indiana | 1/1/26 | Indiana Consumer Data Protection Act |
| Iowa | 1/1/25 | Iowa Consumer Data Protection Act |
| Montana | 10/1/24 | Montana Consumer Data Privacy Act |
| Nevada | 10/1/19 | Security And Privacy Of Personal Information |
| Oregon | 7/1/24 | Oregon Consumer Privacy Act |
| Tennessee | 7/1/25 | Tennessee Information Protection Act |
| Texas | 7/1/24 | Texas Data Privacy and Security Act |
| Utah | 12/31/23 | Utah Consumer Privacy Act |
| Virginia | 1/1/23 | Virginia Consumer Data Protection Act |

### 2. Financial Services Industry

Some of these laws impose requirements on financial institutions that extend to their vendors. Key laws applicable to the financial services sector include:

- **Graham Leach Bliley Act –** protects customer financial records
- **The Fair Crdit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA)** regulate the privacy consumer report information, including credit information.
- **New York Department of Financial Services Cybersecurity Rules** - These rules impose specific security requirements, including technical controls and reporting obligations.

- **Payment Card Industry Data Security Standard (PCI DSS) –** This is historically a contractual requirement of credit card issuers and acquiring banks, but states are adopting it as a regulatory requirement. Validation of compliance is performed annually or quarterly. In March 20223, it was updated to implement multi-factor authentication (MFA) and targeted risk analyses to establish risk exposure operation and management.
- **Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) Regulations**: Financial institutions are subject to BSA and AML regulations that require them to establish and maintain comprehensive AML programs to detect and prevent money laundering and fraud.

### 3. Health Care Industry

- **Health Insurance Portability and Accountability Act (HIPAA):** HIPAA sets the standards for the protection of patient health information (PHI) and governs how healthcare providers, health plans, and healthcare clearinghouses handle and disclose PHI. HIPAA includes privacy, security, and breach notification rules. Healthcare organizations often need to adhere to specific data security standards, such as the **HIPAA Security Rule**, which outlines technical safeguards, physical safeguards, and administrative safeguards for securing electronic protected health information (ePHI).
- **Health Information Technology for Economic and Clinical Health (HITECH) Act:** HITECH, part of the American Recovery and Reinvestment Act (ARRA), reinforced and expanded upon HIPAA requirements. It introduced stricter penalties for HIPAA violations and encouraged the adoption of electronic health records (EHRs) and health information technology.

### 4. Government Contractors

- **Federal Information Security Management Act (FISMA):** FISMA sets forth requirements for federal agencies and their contractors to establish and maintain information security programs. It mandates the development of security policies, periodic risk assessments, and compliance reporting.
- **Defense Federal Acquisition Regulation Supplement (DFARS):** DFARS is a supplement to the Federal Acquisition Regulation (FAR) that imposes cybersecurity requirements on government contractors, especially those in the defense sector. Contractors must comply with the **NIST Special Publication 800-171 standards,** which focus on protecting Controlled Unclassified Information (CUI).
- **National Institute of Standards and Technology (NIST) Standards:** NIST has developed a series of cybersecurity standards and guidelines that are widely used by government agencies and their contractors. NIST's cybersecurity framework, Special Publication 800-53, and Special Publication 800-171 are particularly relevant for government contractors.
- **International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR):** These regulations govern the export of defense-related articles and services. Government contractors working on projects involving ITAR or EAR-controlled items must comply with strict data security and export control requirements.
- **Classified Information Security Requirements:** Government contractors working on classified projects must adhere to specific security requirements outlined in the National Industrial Security Program Operating Manual (NISPOM) for the protection of classified information.

- **The Privacy Act of 1974:** governs the collection, use, and disclosure of personal information by federal agencies and contractors that maintain systems of records containing personal information.
- **Cybersecurity Maturity Model Certification (CMMC):** CMMC is a new framework designed to enhance the cybersecurity posture of defense contractors. It requires contractors to meet specific cybersecurity maturity levels, which are assessed by third-party organizations.

#### 5. The Energy Sector

- **Critical Infrastructure Protection (CIP) Standards**: the Federal Energy Regulatory Commission (FERC) enforces the North American Electric Reliability Corporation (NERC) CIP standards. These standards mandate cybersecurity requirements for the bulk power system, including controls for electronic access, physical security, and incident response.
- **Energy Policy Act of 2005 (EPAct 2005):** EPAct 2005 includes provisions related to the protection of critical energy infrastructure and requires the development of cybersecurity standards and best practices for the energy sector.
- **Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2):** Developed by the Department of Energy (DOE), the ES-C2M2 provides a framework for assessing and improving the cybersecurity posture of energy organizations.
- **Energy Information Sharing and Analysis Center (E-ISAC):** E-ISAC facilitates information sharing and collaboration among energy sector entities to enhance cybersecurity readiness and response.

### F. Other Pre-Acquisition Due Diligence

If the target company operates in a highly regulated or sensitive industry, it may be necessary to engage in due diligence activities that are more invasive than usual. For example, it may be necessary to engage a specialist to run vulnerability scans or penetration tests on critical assets and applications; or to scan systems for current or past artifacts of current or past compromises.

The acquirer should also consider conducting interviews with target employees regarding how data is actually collected, stored and used. When possible, these interviews should be conducted with the target's IT, HR, and CISO officers.

## III. Further Considerations

During the process of collecting the data, new information may come to light that requires another round of due diligence requests. Once the acquirer has enough information to assess the risks associated with the potential transaction, it may decide to beef up the representations and warranties of the target; or set aside additional escrow funds to cover the risks discovered; or reprice the deal; or cancel it entirely. In addition, the information gleaned from the process may result in a change in plans as to the level of operational integration that the acquirer may hope to accomplish in the short term after the acquisition. The purpose of the process is to properly assess risk and the challenges associated with the proposed transaction. A thorough process should help reduce the number and severity of the bumps down the road.