Debevoise & Plimpton

May 2018

TMT INSIGHTS
From the Debevoise Technology, Media & Telecommunications Practice

A Checklist for Cybersecurity and Data Privacy Diligence in TMT Transactions

Companies in the technology, media and telecommunications ("TMT") sectors typically are online-dependent and collect a great detail of valuable information from and about their customers. For these and other reasons, TMT companies are among the most attractive targets for all sorts of cyber breaches, including denial of service attacks, viruses, ransomware and other forms of malware. When considering the acquisition of a business in the TMT sector, diligence requires paying close attention to these cybersecurity, data protection and privacy issues.

Acquirers should explore four key areas, using tools including document review, interviews with the target's personnel, and questionnaires:

- When and to what extent the target collects, stores, processes and transfers personal information
- The target's information security resources, practices and procedures
- The target's data security and privacy compliance history
- Where applicable, particular sector-specific requirements

Collection, Storage, Processing and Transfer of Personal Information

A checklist of issues should include the following:

- ☐ *The categories of personal data collected.* Virtually every business has employee-related data. TMT companies that are retail-oriented or consumer-facing are also likely to collect and store vast amounts of personal information from website visitors and customers.
- ☐ *Whether any data is subject to specialized regimes.* If, for example, the target collects or stores card data or health information, it may be subject to the Payment Card Industry Data Security Standard or the Health Insurance Portability and Accountability Act, respectively.

- *From whom is data collected.* Data collected from persons outside the United States may be subject to national or transnational laws. The European Union's General Data Protection Regulation ("GDPR"), which goes into effect on May 25, has been the subject of significant publicity. Focusing on compliance with EU data protection law, including the GDPR, may be a given but many countries outside the EU also regulate the collection and use of data from their citizens.
- *Where data is stored.* Knowing where the target stores its data–on premises or in data centers, in the U.S. or elsewhere–and whether it maintains a data inventory is important in understanding the target's compliance with data protection laws (including those relating to data localization) and assessing potential vulnerabilities.
- *Use of third-party software and service providers.* Third-party systems can be both potential points of vulnerability and vectors for attacks on the target itself. If the target uses third parties to collect or store significant amounts of data, it is important to understand how it vets and selects those vendors and ensures their continuing compliance with data security best practices and applicable law.
- *Downstream data practices.* If the target is itself a service provider that stores or processes data on behalf of other organizations, diligence should include those entities' own data collection practices and compliance with law and best practices, as well as the target's contractual obligations to those entities.
- *Transfer of personal data.* The European Union's 1995 Data Protection Directive regulates the transfer to the U.S. of personal data about EU residents. This regime is not materially changed by the GDPR. If the target does collect information from EU residents and transfer that data outside the EEA, diligence should include ensuring that it does so for authorized purposes and in accordance with appropriate legal mechanisms, such as model contractual clauses, binding corporate rules or (for transfers to the U.S.), the Privacy Shield.

Information Security Resources, Practices and Procedures

- *Data Security Resources.* Understand the target's data security function, including the experience, resources and reporting lines of its leaders, who may include a chief information security officer and/or chief privacy officer, and their role and reporting responsibilities in the organization. If the target has adequate personnel, that will go a long way towards getting comfortable with its level of data security awareness and preparedness. If the target is being carved out of a larger organization and the data security functions and resources are at the seller level, a potential acquirer should review the target's internal resources and reach agreement with the seller as to which, if any, of the responsible personnel will transfer as part of an acquisition.
- *Training.* Periodic training of personnel on data security and privacy issues is critical to minimizing the risk of breaches caused by careless or intentional acts of employees or contractors.

- *Written information security plan.* Both law and best practice may require the development, maintenance and periodic review of a written information security plan. Certification of information security practices or conformity with an industry-standard framework (e.g., the Cybersecurity Framework of the National Institute of Standards and Technology), can signal the target's commitment toward data security.
- *Data loss protection.* Measures a target takes to prevent data loss may address the risk of potential exfiltration by a departing employee of valuable or commercially sensitive data.
- *Audits and other data security assessments.* Obtain and review any periodic data security assessments or audits of the target. The extent of the target's periodic testing of network and application vulnerabilities can assist in assessing the risk of an attack being successful. Evaluate material weaknesses, the cost of remediating them and who is responsible for remediation.
- *Business continuity and disaster recovery plans.* If these plans are in written form, they should be reviewed to understand when and how the target backs up data and how the target would continue operations under various adverse scenarios affecting data security.

Data Security and Privacy Compliance History

- *Data security breaches.* Examine data security breaches occurring during a reasonable look-back period (such as the past two or three years) that had—or could have had—a material effect on the target's businesses. Understand the circumstances, nature and extent of each breach and review any forensic analysis and incident reports. If personal data was accessed and disclosed, review the notifications made to affected persons and government authorities. Assess the consequences of the breach (i.e., leakage, actual use of disclosed information by bad actors), any litigation and regulatory inquiries and the steps taken to remediate security gaps that may have facilitated or contributed to the breach.
- *Complaints.* Examine any meaningful (and material amounts of) complaints made regarding the target's privacy practices during the look-back period, as well as any governmental inquiries into the target's data security or privacy practices.
- *Privacy policies.* Consumer-facing TMT businesses that collect information on their websites should have comprehensive and accurate privacy policies. Inasmuch as privacy policies frequently change over time, review whether the target's actual practices regarding the collection and use of personal data conformed with its stated policies in effect at the time.

Sector-Specific Issues

Specific types of TMT businesses may warrant additional diligence:

- *Telecommunications*

  - *Data Security Practices*. U.S. telecommunications companies are subject to regulation by the FCC. Under the Communications Act of 1934, the FCC requires carriers to maintain "just and reasonable" data security practices, which includes their taking "every reasonable precaution" to protect customer data; the failure to maintain appropriate security practices can be considered be an unjust and unreasonable practice.
  - *Customer Proprietary Network Information*. The Communications Act also restricts carriers' use and disclosure of customer proprietary network information. The FCC has adopted regulations that obligate those companies to provide notice to consumers regarding uses of their data and report breaches both to the FCC and affected consumers. Failure to comply with the FCC's regulations can result in significant civil penalties.

- *Software*

  - *Access to Codebase*. Targets may employ a range of software on a variety of platforms, from on-premises installations to software-as-a-service (SaaS). Assess the data security measures that a SaaS or other software vendor takes to restrict access to its codebase and development platforms. Diligence should encompass review of the vendor's relationship with third-party developers or others who may have access to those platforms, ensuring that they are required to adhere to appropriately stringent data security obligations.
  - *Security Updates*. Targets that are software dependent should regularly update software to address known or potential security vulnerabilities. An outside audit of the codebase may identify such vulnerabilities, including the use of older software or the failure to update the software with security patches.

Contributors

Jeffrey P. Cunard
Partner – Washington, D.C.
jpcunard@debevoise.com
+1 202 383 8043

Michael A. Diz
Partner – New York
madiz@debevoise.com
+1 212 909 6926

Jonathan E. Levitsky
Partner – New York
jelevitsky@debevoise.com
+1 212 909 6423

Jim Pastore
Partner – New York
jjpastore@debevoise.com
+1 212 909 6793

Michael Schaper
Partner – New York
mschaper@debevoise.com
+1 212 909 6737

About Our Practice

Debevoise's far-reaching TMT practice is a top choice for clients seeking trusted advisors for complex deals or high-stakes cases. Highly ranked in a variety of categories in the technology, media and telecommunications space, Debevoise has what *Chambers Global* describes as a TMT practice that is "full-service and creative, and has a global presence." For more information please visit our Technology, Media and Telecommunications practice page.