Debevoise & Plimpton

Debevoise Update D&P

Tips for Creating a Sensible Cybersecurity and AI Risk Framework for Critical Vendors

February 16, 2021

Companies face increasing cybersecurity and AI risk from third-party vendors. Cybersecurity risks arise when companies share sensitive personal data or company information with their vendors or when their vendors have direct access to the company's information systems. Companies using AI technology that is developed by a vendor can also face risk if the AI behaves unexpectedly, and that results in negative impacts including on critical business operations. In recognition of these kinds of third-party data risks, on October 30, 2020, federal banking agencies—including the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency ("OCC") and the Federal Deposit Insurance Corporation ("FDIC")—released a joint paper (the "Joint Paper") outlining sound practices designed to help banks increase operational resilience.

The Joint Paper's recommendations regarding third-party risk management include:

- Prioritizing third-party dependencies that are most significant to the firm, and setting appropriate risk tolerances;
- Understanding, managing and mitigating those risks;
- Verifying that third parties have sound risk management practices and controls in place that serve to identify and mitigate hazards to operations and are consistent with the company's tolerance for disruption; and
- Addressing key third-party concerns to the extent that these concerns affect the company's operational resilience though due diligence, contract negotiations, ongoing monitoring and termination of contracts.

To address the cybersecurity and AI risk posed by vendors, companies have adopted vendor risk-management frameworks that often include one or more of the following elements:

- Creating a list of **High-Risk Factors**, to help guide which vendors are high risk and whether measures should be considered to reduce risk;

- Conducting a **Preliminary Risk Assessment** based on the high-risk factors to preliminarily categorize vendors as low or high risk;

- A **Vendor Questionnaire** to be completed by the vendor, if appropriate; and

- A list of **Risk-Mitigation Options** for consideration to reduce the risk of vendor relationships that are preliminarily determined to be high risk, which may include **Contractual Provisions**.

In this post we provide some examples of each of these elements.

HIGH-RISK FACTORS

Examples of Possible Cybersecurity High-Risk Factors

For vendors that receive sensitive personal or company information or that have direct access to parts of the company's information systems that contain confidential data, these are some examples of possible high-risk factors to consider:

- The vendor has access to a large volume of the company's sensitive personal information such as credit cards, bank account numbers, tax returns, social security numbers or medical information.

- The vendor has access to the company's trade secrets, information on material pending transactions or other sensitive business or financial data.

- The vendor has a poor score from a third-party cyber-risk rater such as SecurityScoreCard or Bitsight.

Examples of Possible AI High-Risk Factors

The Joint Paper underscores that any vendor AI system that is critical to the company's core business functions—where the failure of the system would result in a material loss of revenue, profit and franchise value—may be seen as higher risk by federal banking regulators.

For these vendors, as well as vendors that provide AI technology that will likely result in adverse impacts on individuals (e.g., the denial of insurance coverage, increased premiums, denial of a loan or benefits, or loss of an employment opportunity), here are some examples of possible high-risk factors to consider:

- The AI system will make decisions with little or no human involvement, and those decisions had previously been made by humans;
- The AI system will perform important operations including with respect to key infrastructures or is critical to a core business function;
- The failure of the AI system would endanger the company's key business lines or threaten the stability of financial markets;
- The AI system will involve the use of large volumes of sensitive personal information;
- The AI system is novel or untested and will be deployed quickly on a large scale; and
- Individuals who may be potentially impacted by a decision made by the AI system will not be aware of the role of the AI system in the decision that affected them and will not have any ability to appeal that decision to a human.

PRELIMINARY RISK ASSESSMENT

By applying the relevant high-risk factors to particular vendors, the company can assign a preliminary risk rating of either low or high. For low-risk vendors, the company may decide that little more needs to be done, if anything. For vendors that are preliminarily assessed as high risk, the company may decide to pursue additional due diligence through a tailored vendor questionnaire.

VENDOR QUESTIONNAIRE

For vendors that are preliminarily assessed as having a high risk, these are some examples of information that may be requested.

Cybersecurity

- Do you have a written information security and business continuity policy?
- Do you voluntarily comply with any cybersecurity standards such as ISO 27001, PCI-DSS or NIST-CSF?

- Do you have a full-time Chief Information Security Officer?
- Do you have cybersecurity training for new employees and annual cybersecurity training for all employees?
- Do you conduct periodic phishing testing for employees?
- Do you conduct annual penetration testing?
- Do you encrypt Company's nonpublic data?
- Do you require multi-factor authentication for remote access to your computer system?
- Do you enforce data access controls to limit users' access to Company's data based on business needs, and do you periodically review access privileges?
- Do you monitor activity of authorized users and detect unauthorized access?
- Do you participate in any cybersecurity threat-sharing group?
- Do you have a written incident response plan? When was it last updated?
- Have you conducted a cybersecurity tabletop exercise in the last 12 months?
- Do you have insurance that would cover cybersecurity incidents?

AI

- Describe any training, testing or benchmarking of the AI system.
- Are there ways to detect when the AI system has drifted significantly from its anticipated results?
- Are you able to explain the factors or data inputs that are most significant in the decisions of the AI system?
- Will any errors, vulnerabilities or flaws that you discover or are reported to you by other customers be reported to the company?
- Describe any efforts to ensure that the company has the rights to use the data used to train or operate the AI system for these purposes.

- Is any data associated with the AI system being shared with anyone other than the company?
- What measures are in place to protect the security, integrity and availability of the AI system and the associated data?
- Has the AI system been stress tested to determine if it can withstand unexpected inputs or disruptions?

RISK MITIGATION OPTIONS

If, after analyzing the responses to the vendor questionnaire, the company concludes that the vendor is indeed a high risk, it should consider measures that may reduce those risks. For vendors assessed to be a high risk, these are some examples of mitigation measures that may be implemented through contractual provisions or otherwise:

Cybersecurity

- Require the vendor to make specific improvement to its data security program.
- Restrict the vendor's access to company data or only provide the data in a form that reduces risk (e.g., password-protected, anonymized, etc.)
- Require the vendor to conduct periodic cybersecurity assessments and alert the company to any significant negative findings.
- Require the vendor to provide prompt notification and cooperation in the event of a data incident.
- Require the vendor to indemnify the company for any losses the company suffers as the result of certain cyber incidents originating on the vendor's systems.
- Require the vendor to have a certain level of cyber insurance.

AI

- Require details of any training and/or testing procedures and results.
- Conduct testing on the AI system for biases or unjust impacts on participants.
- Implement training for relevant personnel on the detection and mitigation of AI bias, model drift and other performance issues.

- Phase in the AI system in stages and in parallel to the existing process so that any unexpected performance issues or impacts can be identified and mitigated at an early stage.

- Continually monitor the performance of vendor AI systems against relevant performance benchmarks and requirements.

- Develop a contingency plan in case the model degrades or can no longer be used for performance-related reasons.

- Require the vendor to notify the company of any material risks, performance issues or vulnerabilities in the systems (or similar systems) that become known to it.

- Conduct disaster recovery, business continuity and stress testing for AI systems associated with critical operations and core business lines and assess the ability of the vendor to continue delivering services during disruptions.

CONCLUSION

Regulators are focused on companies' cybersecurity and AI risks and increasingly, on the significant portion of that risk that comes from their vendors. In order to reduce operational, regulatory and reputational risk, companies should consider adopting a sensible vendor data risk framework that (1) identifies vendors that pose a high data risk and (2) provides practical options for reducing those risks.

* * *

To subscribe to the Data Blog, please click here.

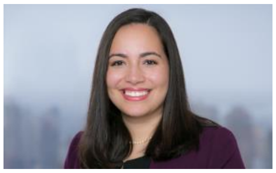
The authors would like to thank Debevoise Summer Associate Alexandra Jimenez for her contribution to this article

NEW YORK

Avi Gesser
agesser@debevoise.com

Michael Bloom
mjbloom@debevoise.com

Anna R. Gressel
argressel@debevoise.com



Zila Reyes Acosta-Grimes
zracostagrimes@debevoise.com