LOEB & LOEB LLP

Technology & Sourcing

MAY 2020

60 Seconds on Sourcing: Re-Thinking Cloud Adoption and IT Security Risks During the Pandemic

As the COVID-19 pandemic caused global office closures and sent nonessential workers home, businesses had to quickly shift to remote work environments while sustaining ongoing operations. To maintain this business continuity, many companies and their suppliers implemented new solutions—or expanded on existing solutions—on a reactionary basis, outside their normal (and time-consuming) due diligence process.

Following the initial rapid adoption of cloud solutions in response to the pandemic, companies should take a second look at these solutions, particularly to address privacy, security and compliance issues. In addition, it may be time to renew focus on existing business processes as new technologies are sourced to meet new financial, operational, personnel and other corporate demands caused by the pandemic.

Key Takeaways

- Customers should not let standard IT security due diligence practices fall by the wayside. New technologies can and should be subject to post-implementation diligence to ensure that privacy, security, and other legal and regulatory standards are being met.
- For existing relationships, customers and suppliers should maintain open lines of communication to ensure cloud solutions are implemented in accordance with contractual requirements regarding access to systems and data, among other concerns.
- Begin due diligence review now for IT projects that are a part of post-lockdown workflows.

Don't Check Your Knowledge at the Door

Organizations expend significant resources across various divisions to develop best practices in IT procurement in order to effectively manage risks. These practices should not fall by the wayside when adopting new technologies quickly on an emergency or seemingly "temporary" basis.

For companies that implemented new solutions during the early days of the pandemic, now that a "new normal" for business has emerged and resiliency has been achieved, it may be time to revisit these new technologies for additional diligence to mitigate risks. As part of this diligence exercise, customers should understand the solution being provided, including the guardrails suppliers have in place to protect the security and integrity of their data and confidential information. In turn, suppliers should understand the specific access controls and security protocols required by their customers in order to confirm they can comply with those requirements. This might require one or multiple in-depth working sessions between key stakeholders and small and medium-size

enterprises of both parties to understand what was implemented and determine whether changes are needed for a more permanent solution.

For the customer-supplier relationship to succeed, and for the use of new technologies to continue effectively, both parties will need to cooperate to accurately define key requirements, including regarding privacy, security, compliance, intellectual property and data usage rights, and develop a joint plan to implement those requirements (to the extent they have not already been implemented).

Consideration of Ongoing Contractual Requirements

In addition to reviewing newly implemented solutions, parties should continue to stress compliance with current contractual obligations. It is important to keep in place (and further enhance or reinforce as needed) lines of dialogue and governance procedures in existing sourcing relationships. Contact your existing customers and/or suppliers to understand how their work situations and IT services have changed in order to avoid pitfalls in the relationship down the road.

For existing relationships, a contractual analysis may reveal terms that are inconsistent with current work environments, such as express prohibitions against vendor personnel accessing customer data remotely or working from unapproved locations, specific IT protocols that may be impracticable or even impossible in a remote work environment, and service levels that may be unrealistic given the circumstances (e.g., unreliable internet connectivity).

These assessments are fact based, involving not just a review of contractual terms but also input from subject matter experts across an organization who are well versed in key issues such as Human Resources, risk management, IT security, regulatory and compliance. For example, where personally identifiable information (PII) and other sensitive data is being processed, it is important to understand:

- Which regulatory requirements apply to new cloud services?
- Are adequate guardrails in place to control the flow and processing of PII or other regulated data, and control who accesses such information?
- What technical controls are in place to prevent personnel from transferring regulated data off secure networks and onto local machines when connected remotely or otherwise relying on new cloud services?

Restarting the Deal Pipeline

As locations around the world begin to emerge from lockdown and other shelter orders, and as the impact of COVID-19 on the global economy reshapes how companies operate and do business, pent-up demand for new IT solutions is likely to materialize. After the initial rush to source and implement new technologies, it is important to refocus on internal processes and diligence procedures to both rethink those deals and be ready to take stock of new deals in the pipeline. Evaluating new IT projects with the same level of diligence as was used prior to the pandemic helps establish strong customer/supplier relationships, resulting in a greater likelihood of successful outcomes.

COVID-19 Resource Center

For information on the business impacts of COVID-19, please visit our COVID-19 Resource Center, which we continue to update as the situation evolves. If you have questions about COVID-19's impact on your business, please reach out to your Loeb relationship partner or email us directly at COVID19@loeb.com.

Related Professionals

For more information, please contact:

Kenneth Adler kadler@loeb.com
Alison Schwartz aschwartz@loeb.com
Benjamin Kabak bkabak@loeb.com

6330 REV1 05.13.2020