Technology & Sourcing Alert
May 2020

Reacting to a Vendor's Request to Implement a Remote Working Solution as a Consequence of COVID-19

As governments throughout the world have issued quarantine orders to implement "social distancing" in the war against COVID-19, companies have been scrambling to change their operations so that their employees and personnel may work from home. This has been particularly challenging for companies that have outsourced parts of their operations to vendors that need to implement remote work solutions for their own employees. These challenges arise for various reasons, including contractual restrictions against remote service locations, difficulty (or impossibility) of maintaining required performance levels, increases in the costs of services delivery and client-required security safeguards that cannot be implemented in a work-from-home environment.

To address these and other issues, the outsourcing master services agreement (MSA) likely will need to be amended, at least temporarily, to permit the vendor to implement a remote working solution (RWS) for delivery of the services.

When drafting and negotiating the RWS terms, vendors and clients should take care to vet the overall risks and impact resulting from the move to a partial or total work-from-home environment, which should include consideration of the following questions:

- What data security protocols will apply to the RWS?
- Does implementing the RWS justify easing the vendor's data security obligations in the MSA?
- What is the plan to implement the RWS?
- Does implementing the RWS justify service level relief?
- Who is responsible for the costs of implementing the RWS?
- How long will the RWS be in place, and what are the client's rights to suspend or terminate the RWS?
- What data security protocols will apply to the RWS?

The specific security protocols that will apply to the RWS depend on a number of factors, including the services the vendor performs, the speed with which the RWS must be implemented and the sensitivity of the data, which would impact which of the vendor's employees will have access.

One of the key security issues will be whether the vendor's employees may use their personal devices or whether they must use client- or vendor-issued devices to perform services. Use of personal devices is likely to pose a greater data security risk, as the client and vendor would have limited control over, and ability to monitor, such personal devices. Therefore, requiring vendor employees to use client- or vendor-issued devices when performing services is preferred, particularly in situations where the employee will have access to sensitive data, including personal data.

Other security protocols to consider when approving a vendor's RWS include:

Attorney Advertising

- Specifying the method that employees must use to connect to the work environment. For example, will employees connect via a VPN and use a remote desktop? Will multifactor authentication be required?
- Restricting use of client-approved devices to service-related activities. This may include applying web-filtering controls to prohibit access to websites that are not approved by the client.
- Blocking the ability to print or download from devices used to perform services.
- Requiring that only secure local networks be used to access the internet from devices used to perform services. The "free" Wi-Fi available at public locations such as cafes and hotels is not secure, as traffic typically is not encrypted, and hackers can easily target these networks. If employees do not have access to a secure network, the vendor should provide them with a secure hotspot.

In addition, the RWS protocols should address nontechnical issues that may arise with employees working from home. For instance, employees should be required to work in an area where others cannot see their device's screen or, if the employees will be speaking on the phone, hear their conversation. If this is not possible for certain employees, the vendor may need to restrict the services those employees perform, or find some other arrangement for the employee. Employees also should be required to lock their screens anytime they step away from their device. Importantly, the vendor should be required to fully train employees on (and regularly remind employees of) the RWS protocols in place, to ensure all protocols are being followed.

Does implementing the RWS justify easing the vendor's data security obligations in the MSA?

Vendors likely will want to limit their liability for any data security issues arising from failure to implement specific security obligations under the MSA that are not practical (or even possible) to implement in a work-from-home environment. For example, physical access controls to an individual's home (e.g., via key cards) may not be possible.

However, implementation of the RWS does not mean that all the contract terms related to security should be superseded in their entirety for the period during which the RWS is in place. From the client's perspective, the damage resulting from a data breach caused by a vendor's employee is the same regardless of whether the breach occurred at an on-site or a remote location. Therefore, clients will want to retain all the data security obligations in the MSA to the extent possible and/or to the extent they do not directly conflict with the specific agreed-upon RWS protocols.

What is the plan to implement the RWS?

The RWS terms should include an agreed-on plan for implementing the RWS, including details such as the timeline for implementation, indication of specific vendor employees who will work remotely, duties those employees will perform while working remotely, and the infrastructure and specific protocols that must be put in place to support the RWS.

Including the plan in the agreed-on RWS terms will allow clients that are eager to restore or improve their operations to hold the vendor responsible for timely and properly implementing the RWS. Vendors, however, may want the client to acknowledge that any timeline and plan may need to be adjusted either due to the client's failure to cooperate or as a result of changes in circumstances given the fluid nature of the COVID-19 situation.

Does implementing the RWS justify service level relief?

Given the challenges of quickly implementing an RWS, vendors may want clients to temporarily waive service levels (or at least service level credits) while the RWS is in place. For example, if the RWS will allow only limited services to be performed or a portion of vendor personnel to perform services remotely, or if the vendor's employees experience reduced internet connectivity at home, it may be difficult or impossible for the vendor to meet the service levels that were contemplated with the services performed on-site by a larger number of employees.

Clients, on the other hand, likely will want to continue to hold the vendor accountable for performance, especially given that the RWS may need to be in place for an extended period of time. In an effort to balance the conflicting goals, the parties may agree to either (a) new service levels that apply only while the RWS is in place, and/or (b) a waiver of only a subset of service levels that are likely to be impacted as a direct result of working remotely (e.g., waiver of service levels

measuring productivity, but maintaining service levels measuring accuracy). In addition, the parties may agree to continuous improvement targets for the service levels to allow the vendor to ramp up performance throughout the duration of the RWS terms. In any event, the vendor should continue to use good faith efforts to perform, notwithstanding the challenges faced when performing under the RWS.

Who is responsible for the costs of implementing the RWS?

Where the vendor is expected to incur significant costs to implement the RWS, the vendor may want to pass on at least a portion of these costs to its clients. For instance, the vendor may need to purchase new devices for those employees performing services remotely for the client, install additional servers and software to run the infrastructure, and provide internet access for employees who do not have internet at home. These costs will add up quickly, and they most likely were not included in the vendor's cost model that is reflected in the prices under the MSA.

Clients, however, will want the vendor to bear the costs of the RWS, as the clients are already incurring costs to move their own employees into a remote-work environment due to the unexpected COVID-19 disruption. Indeed, as the BCP/DR recovery terms in the MSA may already address responsibility for costs to restore services after a disruption caused by COVID-19, the parties should first look to the MSA to determine financial responsibility. If the MSA does not directly address financial responsibility for implementing the RWS (and even if it does), the parties may agree to a shared-cost model.

How long will the RWS be in place, and what are the client's rights to suspend or terminate the RWS?

Given the uncertainty and ever-changing nature of the COVID-19 pandemic, it will be difficult to determine a period of time in which the RWS may be used. Therefore, instead of specifying a period of time, the RWS likely will need to stay in place until the vendor is able to return to "business as usual" and perform the services on-site.

However, clients also may want to have the option to suspend or terminate the RWS in cases where the RWS is not working as anticipated, the client believes that its data is at risk or there is a breach of the RWS terms. For the greatest flexibility, clients may even seek to have the right to suspend or terminate the RWS for convenience to avoid having to show cause for the suspension or termination. Note, however, any suspension or termination of the RWS before it is possible for the vendor to return to business as usual likely will impact the vendor's ability to perform under the MSA (particularly where government-mandated stay-at-home orders preclude employees from working on-site). Therefore, in the event of a termination or suspension of the RWS terms, the client and the vendor should agree to work together in good faith to find and implement an alternate solution, as necessary, to maintain the continuity of the client's operations.

In some cases, the vendor also may seek to have a right to suspend or terminate the RWS under certain limited circumstances. However, clients should be cautious in granting this right and consider the disruptions that may result from the vendor unilaterally pulling the plug on the RWS (even to return to pre-RWS operations).

Conclusion

Migrating an outsourcing vendor to an RWS poses several challenges and likely will require amending the MSA. When negotiating the RWS terms, clients and vendors should consider the data security protocols that should be put in place for the RWS, how the RWS impacts the data security obligations in the MSA, how long the RWS may be used and rights to suspend or terminate the RWS, the implementation plan for the RWS, appropriate service levels that should apply to the RWS, and who should be responsible for the costs of moving to the RWS. Further, if the client permitted the RWS proposed by the vendor to be implemented quickly at the onset of the pandemic, without fully vetting the situation and/or agreeing in writing to favorable terms governing the RWS, now is the time for them to revisit the particulars surrounding the RWS and appropriately negotiate and document its details in order to ensure a meeting of the minds and avoid disputes down the road.

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

Akiba Stern . . . . . astern@loeb.com
Alison Pollock Schwartz . . . . . aschwartz@loeb.com
John Monterubio Jr. . . . . jmonterubio@loeb.com

6346 REV1 05-26-2020