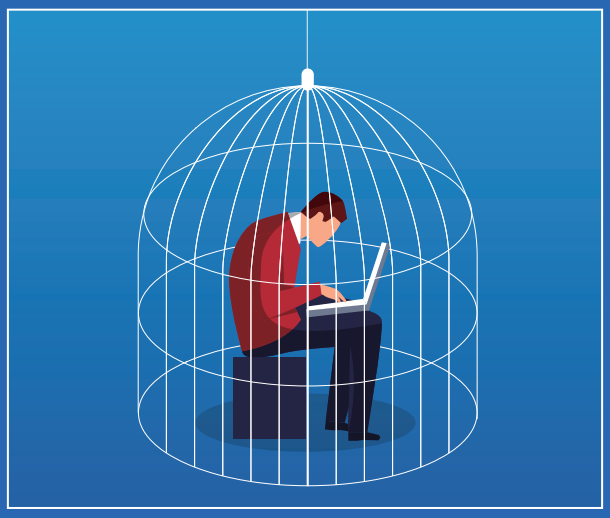

Technology Contract TRAPS AND TACTICS

Charles Nerko and **Sarah O'Brien** Barclay Damon LLP

Every organization relies on technology to power its business and store its sensitive information. Before signing a technology contract, organizations should carefully consider the following questions to minimize risks.

HAS DUE DILIGENCE ON THE SERVICE PROVIDER BEEN PERFORMED?

Before turning to the contract terms, the organization should conduct independent due diligence on the service provider. This includes analyzing the service provider's experience and abilities, financial statements, insurance policies, cybersecurity response program and test results, business contingency plans and test results, internal audits, security assessments, and litigation history.

DOES THE CONTRACT ADEQUATELY DEFINE PERFORMANCE STANDARDS?

The contract should specify the deliverables and benchmarks to hold the service provider accountable and make certain it is following through on promises. Common metrics include system uptime percentage and the deadline for service completion.

WHAT HAPPENS IF PERFORMANCE STANDARDS ARE NOT MET?

The contract should detail reporting processes, escalation procedures, and remedies for nonperformance that motivate the right behavior.

ARE IMPORTANT PROMISES MISSING FROM THE CONTRACT?

Many times, key promises related to performance standards are in RFP responses, marketing materials, or oral statements. Everything the service provider promised during negotiations or in the RFP process should be incorporated into the final contract. A contract's merger and integration clause will generally cancel out collateral representations. If the service provider refuses to incorporate a crucial performance standard into the formal contract, it is a red flag.

ARE THE FEES QUANTIFIED?

Make sure that important fees are quantified in the contract. A service provider's undefined "standard rates," "customary rates," or "rates then in effect"—particularly for services needed only when a relationship terminates—invite costly surprises when the actual fees are revealed later on.

IF THE SERVICE PROVIDER REQUIRES EXCLUSIVITY, IS IT REASONABLE?

Consider the implications when a service provider insists on exclusivity. It is reasonable to assure a service provider it will not have to reconcile a competitor's data provided in a proprietary format or maintain compatibility with a software program provided by another service provider. Some service providers, however, seek overbroad exclusivity agreements that cover an organization's entire technology needs. Exclusivity agreements should be limited to the service provider's legitimate needs while also giving the organization flexibility to use other service providers.

IS THE CONTRACT LENGTH APPROPRIATE?

Contract lengths that seem routine in non-technology contexts can be an eternity for a technology deal. Consider the lifespan of the technology itself as it relates to the hardware that will power it. A contract with a three-year term will likely lock the organization into the technology even though the hardware will likely be replaced during that time. And a lengthy contract term carries an opportunity cost of foregoing future innovations.

HOW AND WHEN DOES THE CONTRACT RENEW?

Be aware of automatic renewal language. Ensure key contract dates are appropriately calendared if the contract requires a nonrenewal notice. Ideally, contract length should be measured from a specific date rather than an undefined date tied to the "commencement of services," which may inadvertently lengthen the contract term as new services are added.

DO THE SERVICE PROVIDER'S LIABILITY LIMITS FAIRLY APPORTION RISK?

A service provider's acts and omissions can potentially inflict crushing liability on

an organization, particularly if it exposes the organization to a data breach or loss of critical data. Do your best to negotiate liability limitations to ensure a fair allocation of risk if something goes wrong, especially when the events giving rise to liability are solely within the service provider's control.

IS A REASONABLE INDEMNITY OFFERED?

Pay close attention to indemnity provisions to avoid situations where the organization may be liable for claims arising from incidents within the service provider's control. The service provider should provide a reasonable indemnity for issues within its control, such as covering losses from data breaches or the service provider's infringement of a third party's intellectual property. An intellectual property infringement indemnity is particularly valuable because a service provider can foist liability for patent infringement on an organization without the organization even knowing about the patent issue.

IS THERE A FAIR PROCESS FOR RESOLVING DISPUTES?

Make sure the dispute resolution clause provides a balanced method of resolving disagreements. Technology service providers tend to use dispute resolution clauses that favor their business, such as getting the "home court" advantage in litigation or arbitration. Some service providers have manifestly unfair dispute resolution protocols, such as requiring an arbitrator to be selected from the service provider's other (presumably satisfied) customers. Consider the implications of the dispute resolution procedure to ensure the process is fair, impartial, and balanced.

WHAT HAPPENS WHEN THE PARTIES SEPARATE?

It is important to "plan the breakup" at the outset of the relationship. A customer may want to invoke early termination rights when the service provider fails to meet service levels or when replacing the service provider results in cost savings or service enhancements. Terminations may also occur due to a service provider's company closure. Adequately plan the logistics for a separation at the outset of a relationship, including details such as the service provider's exit fees and obligation to facilitate a transition to a successor service provider.

WHO OWNS THE DATA AND DELIVERABLES?

Carefully review provisions addressing data and IP ownership. It is critical for your organization to retain ownership of its data and that the service provider is given access only to the data required to perform its service. A terminated service provider lacks incentives to safeguard data belonging to a former customer, so a service provider should be contractually obligated to return and destroy the organization's data when the relationship concludes. IP ownership provisions should align with the organization's expectations regarding its ownership and use of the deliverables, including after the relationship with the service provider ends.

IS THE SERVICE PROVIDER'S SECURITY ADEQUATE?

Third-party service providers are often the weak link in an organization's cybersecurity. The service provider should offer sufficient security precautions, including firewalls, encryption, and authentication. These precautions should satisfy the legal requirements of every state in which the organization does business as well as the states in which its employees and its customers are located.

ARE THERE MEANINGFUL AUDIT RIGHTS?

A service provider's performance should be monitored after a contract is signed to evaluate cost-effectiveness, benefit, service delivery, and adherence to contractual and legal requirements. A service provider should permit periodic audits by an independent third party to ensure compliance with contract terms.

WHO IS ON THE OTHER SIDE?

In the absence of an express commitment to the contrary, contracts are generally freely assignable. The organization should consider prohibiting the service provider from assigning the contract to a third party or changing its permitted subcontractors. If subcontracts are used, they should be identified, and the service provider should accept responsibility for the subcontractors' performance.

HOW WILL DISRUPTIVE EVENTS BE MANAGED?

Have proper plans to address adverse events, including a service provider's outage or disruption. For critical technology contracts, an organization should identify and prepare for significant disruptive events, including those with a low probability of occurring but a high potential impact.

HOW WILL THE SERVICE PROVIDER RESPOND TO SIGNIFICANT CHANGES?

Changes to the relationship may be necessitated by changes to laws or other regulations, changes in risk levels, changes in technology, mergers and acquisitions, and changes to the organization's business processes or priorities. Assess how the service provider will evolve and respond to changes to ensure the organization will be best served.

ARE THE BUSINESS BENEFITS WORTH THE RISKS?

Above all, an organization's relationship with a service provider should be beneficial to the business. Every contract has risk, and some service providers will simply not budge on a one-sided contract term. Management should perform a business review of the contract and its legal risks to ensure they are confident that the business benefits outweigh the legal risks associated with the relationship.

ARE EMPLOYEES TRAINED TO AVOID INADVERTENT CONTRACT FORMATION THAT MAY EVADE LEGAL REVIEW?

Employees may unknowingly bind their organization to a contract or contract amendment by purchasing from or interacting with a website with posted terms of use, paying an invoice with contract terms, emailing deal terms, or requesting upgrades from a service provider. Service providers are increasingly welcoming of large credit card payments because employees' credit card transactions typically have relaxed legal review compared to requesting payments by company check. Employees should be trained to detect things that may contractually bind the organization and flag them for appropriate legal review.

Charles Nerko is a partner and a co-leader of the Cybersecurity Team at Barclay Damon LLP. He helps businesses remain competitive, protect their confidential information, and increase their bottom line through technology contract negotiation as well as litigation against technology service providers.

Sarah O'Brien is an associate at Barclay Damon LLP and a member of its Cybersecurity Team. She concentrates her practice on state and federal commercial litigation matters involving technology and a variety of business disputes.