

MAYER • BROWN

Contracting for Digital Services

Joe Pennell
Partner

+1 312 701 8354
jpennell@mayerbrown.com

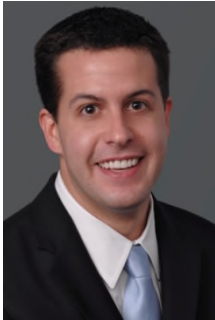
Brad Peterson
Partner

+1 312 701 8568
bpeterson@mayerbrown.com

June 7, 2016

The Age of Disruption

HOW EMERGING TECHNOLOGIES AND CYBERSECURITY ARE TRANSFORMING SOURCING



Joe Pennell

Partner

Joe Pennell is a partner in the Chicago office of Mayer Brown's Business & Technology Sourcing and Corporate & Securities practices. Joe focuses his practice on information technology and managed services transactions, including cloud computing, software licensing and implementation, and the outsourcing of finance and accounting services, IT infrastructure services and support, managed network services, and application development and maintenance. He is the Co-Chair of the ABA Section of Science and Technology Law's Cloud Computing Committee.



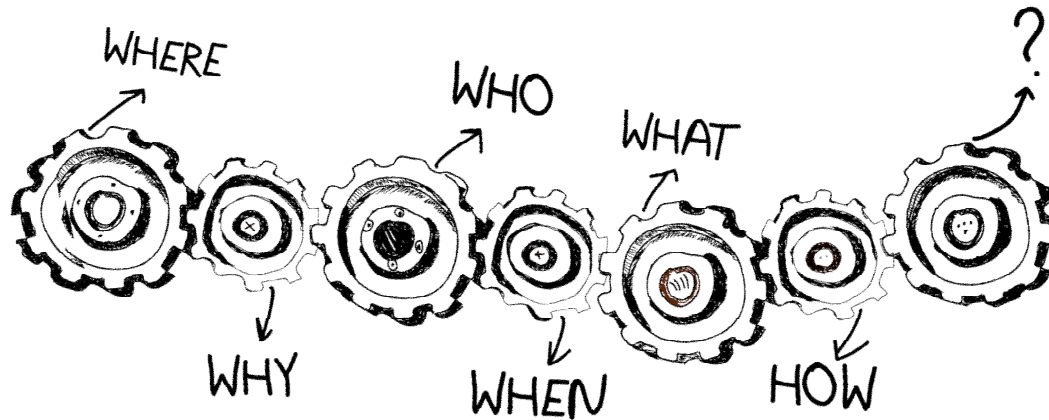
Brad L. Peterson

Partner

Brad Peterson is a partner in our Chicago office and a co-leader of our global Business & Technology Sourcing practice. He is also one of the four partners leading Mayer Brown's "Drive for Efficiency," a global, Firm-wide initiative to deliver lower and more predictable fees for our clients. Brad has extensive experience in all types of outsourcing, having completed several dozen large outsourcing deals, including many that included multi-tower business process outsourcing. Brad has over 25 years of relevant experience.

Agenda

- What's changing?
- Why does that matter for contracting?
- How can we help clients maximize value and avoid pitfalls?



The background of the slide is a solid blue color with a complex, low-poly geometric pattern. The pattern consists of numerous irregular polygons of varying sizes and shades of blue, creating a textured, crystalline effect. The colors range from a deep navy blue to a lighter, sky-blue hue, particularly towards the top right corner.

WHAT'S CHANGING?

Examples of Digital Age Technologies

- Interface Technologies

- Social media
- Mobile computing
- Internet of Things (IoT)

- Computing Technologies

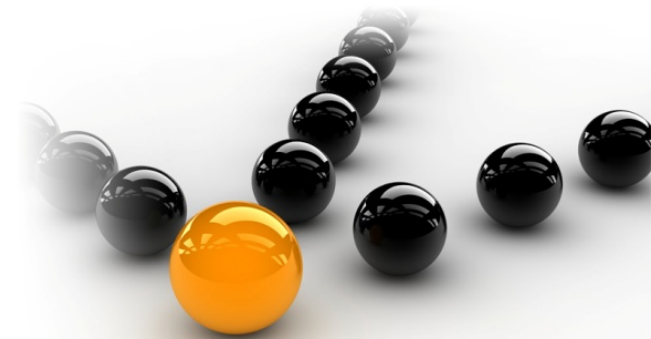
- “Big Data” analytics
- Private, public and hybrid cloud
- Software as a Service (SaaS)
- Autonomics / robotic process automation
- Cognitive computing
- X as a Service (XaaS)



These are Disruptive Technologies

“Occasionally, however, *disruptive technologies* emerge: innovations that result in *worse* product performance, at least in the near term. . . . Products based on disruptive technologies are generally cheaper, simpler, smaller and, frequently, more convenient to use.”

The Innovator's Dilemma,
by Clayton M. Christianson, Harvard Business School Press, 1997



Typical Benefits and Problems of Digital Services When Compared to Established Alternatives

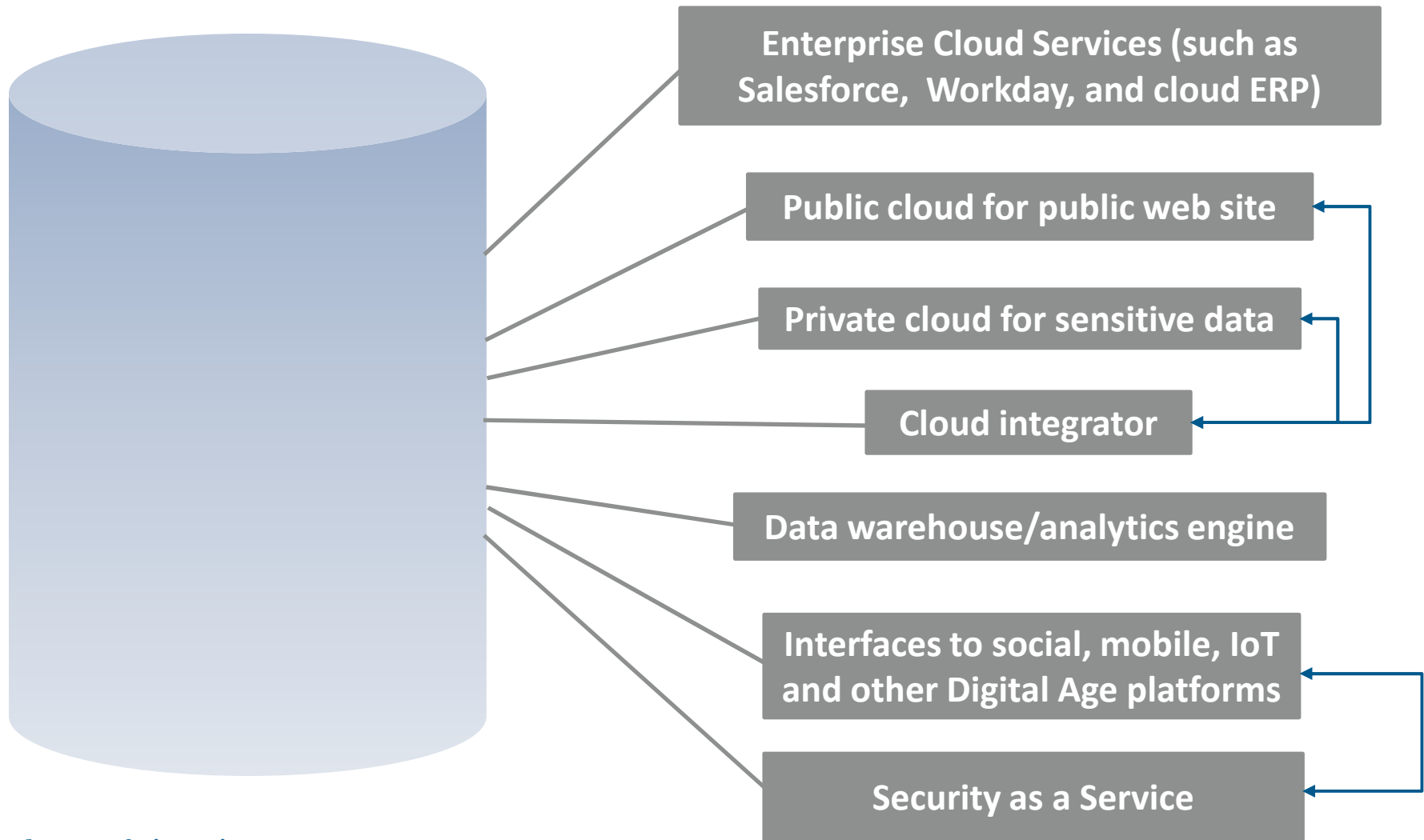
Typical Benefits

- Exciting new capabilities
- Consistent service delivery
- Scales from a single-user to enterprise use
- Point solutions
- Easy access via Internet, without installation challenges
- Low initial investment
- Ongoing cost savings

Typical Problems

- Missing critical capabilities
- Limited ability to customize
- Supplier may change or terminate services at will
- “AS IS” (consumer) terms
- Built as standalone solutions, without APIs or connections
- Cybersecurity risk
- Displacing people

Customers Thus Are Adding Digital Services to Established Environments



The background is a solid blue color with a complex, low-poly geometric pattern of various shades of blue. A horizontal band of a slightly lighter blue shade runs across the middle of the image.

WHY SOURCING MUST CHANGE FOR DIGITAL SERVICES

Traditional Approaches to Supplier Selection Do Not Fit Digital Services

- Traditional RFP models assume that supplier can customize its services.
- Traditional, customer-standard contract terms assume that suppliers are confident in their capabilities and plans.
- Sourcing process is assumed to start with a sourcing event, not online subscriptions by end users on the web with BU budgets.
- Focus on “apples-to-apples” comparisons that limit ability to pick genuinely novel selections or assess innovation capability.

Traditional Approaches to Contract Terms Do Not Fit Digital Services

Traditional Services	Digital Services
Suppliers provide services that meet customer needs	Customers buy what supplier is selling
Humans using tools	Tools programmed and maintained by humans (“digital labor”)
Pricing metered on cost-driving inputs (such as FTEs)	Pricing based on access to a fixed-cost infrastructure
Value primarily in performing needed activities	Value primarily in data generated by services and insights from data analysis
Long-term commitments for services anticipated to be lasting parts of core	Short-term commitments for services likely to be transitional

Traditional Approaches to Service Integration Do Not Fit Digital Services

- Each new inflexible platform requires multiple integrations.
- Digital Age providers often lack capabilities in integration.
- New integrations require custom work because service levels and service support models vary greatly.
- New integration points = new potential points of service and security failures.
- New potential points of failure increase the need for operational risk mitigation strategies (e.g., parallel cloud platforms with different providers).



Traditional Approaches to Supplier Governance Do Not Fit Digital Services

- Change management will be increasingly complex across the multi-supplier ecosystem (e.g., a change in an operating system creates the need for changes in APIs, user apps and database organization).
- Incident management with multiple integrated Digital Age solutions becomes challenging (e.g., is the problem in the mobile app, the SaaS to which it connects, the platform or the API, when all are from different providers?).



Traditional Approaches to Supplier Governance Do Not Fit Digital Services

- Standardized service platforms may not allow for customized supplier relationship management.
 - Designated governance teams and committees are generally not within the cost model for Digital Services.
 - Inter-supplier operating level agreements are only available for the most bespoke interrelated outsourcing arrangements.
 - Robotically automated processes cannot speak for themselves.
- Business users may have little connection with suppliers.
- Customer governance teams are not currently staffed to be educating the business about supplier services and choices and otherwise replacing the supplier's engagement team.

What Goes Wrong for Customers Who Use Traditional Sourcing Approaches for Digital Services

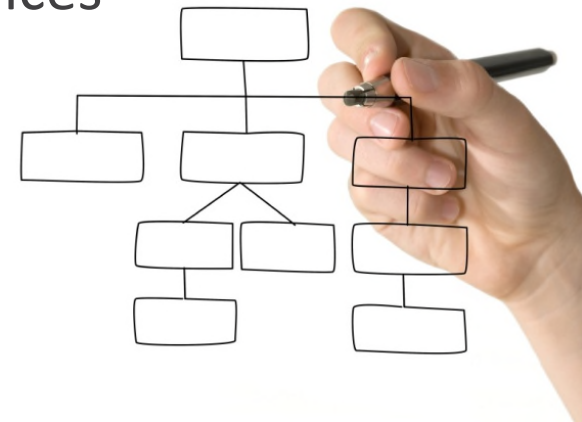
- Suffering over the long term by initially agreeing to one-sided supplier forms for services that will become mission critical
- Investing in the wrong Digital Services due to inadequate due diligence, inadequate processes or rogue contracting
- Undermining existing sourcing relationships with new “cloud terms” as established providers expand to offer Digital Services
- Failing to identify, understand and mitigate risks
- Surprise costs and operational problems from failure to understand “hidden” costs of integration and filling in service gaps
- Vendor management organizations and supplier governance functions overwhelmed with increased volume, leading to little-to-no actual supplier monitoring and management



REIMAGINING SOURCING FOR THE DIGITAL AGE

Understand the Challenge for Your Company

- Learn the emerging technologies and the new issues/risks
- Understand your company's IT roadmaps
 - What is your strategy for the Digital Age?
 - Which Digital Services are transitional? Which are your future core?
 - Who are the stakeholders?
- Understand key sources of risk for Digital Services for your company
 - How are your regulators approaching key issues?
 - What risks might increase in connection with your data, products, operations and so forth?



Examples: New Sources of Risk–Legal

- Inadvertent disclosure of confidential information or trade secrets by permitting use of customer data in “big data” analysis
- Cybersecurity and privacy law compliance
- Failure to comply with records retention requirements
- Inability to comply with litigation holds and e-discovery requirements
- Export law violations in global clouds



Build a Digital Age Sourcing Team



Digital Age Sourcing Evaluation Process

- Use requirements documents to facilitate assessment of standardized Digital Age provider offering to business needs. Importantly, customer does this assessment
- Prepare gap analysis and review with Digital Age sourcing team and determine if service gaps can be filled with other provider solutions, or not
- Determine impact on financial case for use of Digital Age provider solution. Sometimes what is left out of a solution will drastically affect the business case (e.g., hidden costs of service integration, compliance like e-discovery and litigation holds, costs to manage incidents, etc.)
- Establish requirements for due diligence and risk analysis even prior to “proof of concept” use

Develop Digital Age Risk Assessment Tools

- Using the gap analysis prepared in the previous step, transfer the gaps into a risk chart that identifies the risk
- State potential risk mitigation factors from the provider, and potential risk mitigation solutions from the customer
- Assess the nature of the risk based on the selected mitigation steps



Example: Risk Assessment Tool

Risk	Provider Mitigation	Customer Mitigation	Level of Risk after Mitigation	Comments
Provider services are not yet certified to standards typically followed by customer.	Provider is working on certification, which could be available in 12-24 months.	Customer will limit use to less sensitive data until certification completed. Also will monitor status of Provider certification and assess each 12-month period.	Medium	Customer may consider encryption of data as an added protection but must evaluate whether that will cause usage or service integration issues.

Develop Risk-Based Contracting Tools for Digital Services

- Create template for legal gap analysis to measure supplier offerings against customer minimum requirements for key contract terms
- Invest in new policies, such as a Cloud Computing Policy, to simplify and govern basic decisions on risks
- Create checklist (and integrate into sourcing evaluation process) of hidden legal and compliance costs of solutions and other risks
- Perform legal gap analysis and transfer results into a risk assessment tool

Example: Risk-Based Contracting Tool

Risk	Provider Mitigation	Customer Mitigation	Level of Risk after Mitigation	Comments and Considerations
Provider (cloud platform provider) reserves right to discontinue services on 30 days notice to Customer.	Provider will agree to extend notice to 90 days.	Customer will (a) maintain back-up platform arrangements with other providers, (b) confirm that all data and apps may be extracted within a 90-day period, and (c) develop migration plan now that assesses how Customer will migrate out in 90 days without business interruption, including leveraging a “SWAT” team to work on APIs and integration issues during 90-day migration-out period .	Medium	Customer will continuously assess Provider status to determine if this risk changes in level based on Provider performance, financial health and direction in market.

Develop Positions and Contract Language for Digital Service Contracts

- To move at a Digital Age pace, have templates for Digital Services.
- To win the “battle of the forms,” create templates in simple, reasonable and plain English similar to those used by Digital Service suppliers.
- To get deals done, know what is (or is not) possible within the Digital Service model.
- To mitigate risk, avoid agreeing to “cloud terms” even if they are “market” in consumer contracts, or your company has accepted them in low-risk applications and no-leverage negotiations.
- To prepare for integrated Digital Services, amend existing contracts with current outsourcing service providers to include cloud provisions.

Examples – Changes in Contract Provisions

Managed Services Provision	Digital Services Provision
Services will conform to Customer's past practices, policies and standards in addition to the Services description in the contract.	Services will conform to specifications.
Customer owns all intellectual property developed by Supplier as part of the Services.	Customer owns the intellectual property developed by Customer using the Services. Supplier owns all changes to its systems.
Supplier shall use trained, acceptable, verified, qualified personnel and keep its software at n-1 currency.	Commitments based more on outcomes or outputs and less on the people or machines.
Supplier shall comply with Customer's security standards and policies.	Supplier shall comply with express agreements and remain certified under industry standards (such as ISO 270XX).
Supplier will change Services to remain current and meet changing customer requirements.	Supplier will not promise to improve Services, but will provide any improvements made to the platform at no additional charge with adequate notice.

- Map the data flows through the Digital Service
- Identify data created as a result of the Digital Service
- Identify possible other uses for data accessible to provider
- Gain data rights at least to data that you collect or provide and, if possible, to data created as result of the Services or of processing your data
- Limit uses of your data where possible
- Obtain rights to “big data” insights resulting from use of your data
- Watch out for providers asking for rights to use “anonymized” or “aggregated” data or data “to improve our Services”

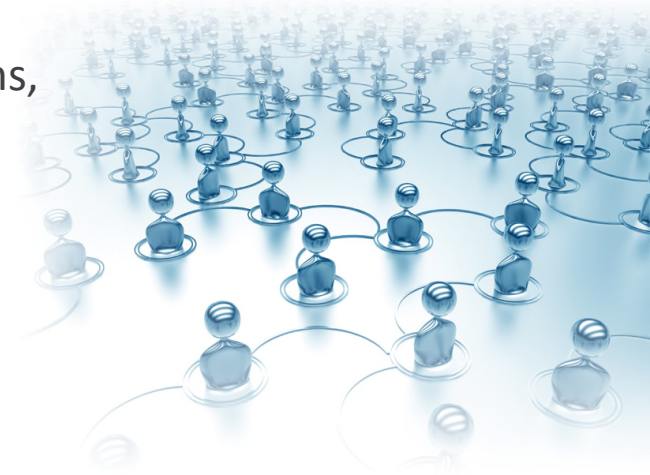
Prepare for Integration with Digital Age Suppliers

- Integration is a key responsibility to allocate in the contracts.
- Integration works best if the integration approach is selected before new suppliers are added and thus becomes part of the process.
- Current experience points to customer as best integrator, but this may change as multi-supplier ecosystems expand.
 - Customer remains ultimately responsible
 - Greater control over incentives
- Suppliers can serve an integrator role *with the right contract*.
 - Prime supplier with subcontractors and managed third parties
 - Supplier providing oversight and assistance in managing other suppliers
- Traditional integrators bring great expertise.

Prepare for Governance and Ecosystem Management for Digital Services

- Invest in a new governance model and new skills for this new category of service supplier
- Identify and adopt a governance approach for Digital Age suppliers who are not allocating personnel to work with you, perhaps based on your software vendor strategy and the individual characteristics of each Digital Age provider
- Implement master agreements for panel providers to supersede click-wrap terms and achieve adequate scale for governance efforts
- Reexamine existing sourcing arrangements and renegotiate, retrofit or resource to require existing suppliers to work with inflexible Digital Service providers
- Build personal connections via sales channels and user groups

- The move to Digital Services is now inevitable even for large enterprises with established IT systems.
- Yesterday's services sourcing will not meet Digital Age needs.
- The solution is to update your contracting approaches for the Digital Age, by:
 - Preparing yourself
 - Updating your strategies and policies,
 - Developing new templates and contracting positions,
 - Creating an integration plan, and
 - Adapting your governance approach.



QUESTIONS

Joe Pennell, Partner

Mayer Brown, Chicago

+1 312 701 8354

jpennell@mayerbrown.com

Brad Peterson, Partner

Mayer Brown, Chicago

+1 312 701 8568

bpeterson@mayerbrown.com

