A COVID Perspective on Consultancy – Managing Onsite Consultancy When the Site No Longer Exists

22 December 2020

***By Bernard Perchman**, Team Lead, ETrading and Australian Institute of Business Alumni.*

Across the globe, the COVID pandemic has radically transformed the way that we live and work. Employees everywhere have lost their offices and found themselves working from their living rooms. The pandemic has also had a profound effect on the way that corporations practise vendor management.

To understand the effect this has had, we first need to understand the significance of vendor managed services within the Australian financial industry. These organisations are labour intensive and – particularly for information technology – have a high demand for specific types of technical experience. With a comparatively small labour pool to draw from, they typically service the balance of demand through vendors. They achieve this through various outsourcing arrangements; for simplicity, we will focus on *captive outsourcing* and *ad-hoc consultancy*. In the former, a consultancy sets up remote offices with staff who work exclusively for the client and for the latter, individuals or small groups deliver a predefined or bespoke service o the organisation. Both have seen the dramatic effects of COVID, but have experienced this in different ways.

As March ended and the pandemic events unfolded, onsite ad-hoc consultancy came to an unexpected and permanent halt. For financial institutions – some of which hosted thousands of daily vendor visits – the effect on resourcing and productivity was enormous. Project managers everywhere found their programs stalling as the workforce took stock of the situation. In workplaces, access restrictions were setting in across the globe. Overnight, onsite engagement had become an untenable option.

Vendor management offices found themselves formulating emergency strategies to find alternatives such as remote access. The technical implications of this are daunting enough – but these pale beside the security implications. In the highly regulated financial industry, the restrictions around access control are formidable. From a legal perspective, granting an individual unsupervised access to the network is tantamount to treating them as an employee of the company. This in turn triggers the obligations around credential management, background checks, and mandatory training typically imposed on permanent employees.

Given this elevated state of access privilege, many organisations further concluded that the safest approach would be to courier company laptops to these third parties. In that way, the organisation controls every segment of the communication path and can minimise the leakage of data onto external devices. However, this approach is costly and time-consuming. With most of the hardware supply chain in lockdown, many organisations face delays on hardware delivery. Then there is the cost of configuration and distribution to consider. Further, the point of supplying a laptop to a third party is to ensure that nothing is copied to or from it. Therefore, if the laptop fails to connect back due to any misconfiguration, further courier services are required to return and redistribute it.

As financial institutions prepared this new form of access, their legal teams went into overdrive to draw up the required contracts. Consulting agencies, finding their employees at home and on the bench, were naturally enthusiastic to embrace these alternatives. However, the new contractual obligations threw up complexities for consultants too. Employee data is highly confidential, and typically, an agency is prohibited from divulging this to a client organisation. In Australia, this is upheld by the *Privacy Act of 1988* which has strict guidelines around the distribution of employee data to third parties. This is particularly relevant for background checks (which extend to criminal records).

As corporations around the world adapted to this model of remote working, implementation issues began to emerge. In the data-intensive financial sector, bandwidth issues were not long in surfacing. Many financial intuitions (and indeed network providers) had designed their remote infrastructure to support a fraction of the workforce in mind, never anticipating that it would apply to the entire organisation. In response, many corporations put their teams into different time schedules in order to distribute the load more evenly throughout the day. These schedules extended to consultants, who now found themselves having to adapt their working hours accordingly.

COVID has changed the vendor engagement pattern in other ways too. In the fast-changing financial services environment, many organisations use agile methodologies to deliver software. This allows them to deliver small increments over weekly or monthly cycles. In turn, vendors will typically engage for short periods of intense interaction for the implementation, followed by ad-hoc visits for fine-tuning in later cycles. However, with remote access now in hot contention, institutions no longer have the luxury of agility. Instead, they have to draw up tight engagement schedules and hold vendors to inflexible deadlines.

This reduction in flexibility is challenging the industry at a broader level too. In Australia, many financial institutions have embraced the trend of paring back permanent workforces, then backfilling demand with short-term staff appointments from offshore service providers. A fundamental underpinning of this strategy is the service provider's ability to rapidly redeploy their talent pool to where the demand lies. This strategy, like so many others, did not consider the pervasive effects of a pandemic. In the new normal, where even the smallest engagement requires weeks of preparation, organisations simply cannot pivot the workforce at the pace at which they previously did.

In short, organisations have to rethink all aspects of interaction with their vendors, particularly with respect to information security. Financial Institutions typically lock down their systems and data on a need-to-know basis. This restriction is commonly role-based too, with privileges reducing from permanent staff to offshore partners and then to ad-hoc contractors. However, with everybody now a remote user, it is more difficult to differentiate these roles, and organisations have to account for vendors across the spectrum logging into their networks. This has a profound effect on security and confidentiality. For example, no longer does the concept of the *group only* intranet apply; publication material is now available to individuals with the most tenuous of links to the organisation.

Within information technology, we see an impact on the way that vendors support their software. Industry regulation has led to increasingly stringent requirements around confidentiality. As a result, most financial organisations prohibit despatching application log recordings to vendors for troubleshooting. As we discovered, the pre-COVID notion of inviting the consultant onsite is no longer tenable. In the initial phase of the pandemic, remote conferencing services such as Zoom experienced exponential growth as teleconferencing replaced these interactions. However, the security loopholes exposed by these types of teleconferencing tools did not take long to surface, and in short order financial institutions began to ban their usage. In any event, software support via teleconferencing is often unwieldy. At some stage, the employee needs to hand control to the consultant so that they can troubleshoot, at which point they must watch passively until the activity concludes. There is also the additional cost and jitteriness associated with viewing screens within screens.

Organisations will therefore need to reconsider arms-length software support arrangements. If they opt for remote access provision, they may need to invest in their onboarding processes, for example enlisting specialist agencies to speed up reference checks. Another alternative is to re-draft the vendor agreement to stipulate a higher degree of confidentiality, and then mandate that the vendor sponsor a dedicated line into their organisation for data exchange. At any rate, organisations have found that the COVID situation has precipitated significant contract rewriting, with both parties demanding higher levels of trust and security.

The implications for the consulting industry are profound. Many offshore call centres in India and the Philippines found themselves incapacitated by COVID because their agreements prohibited their employees from accessing the client site from home. Consulting organisations are now scrambling to re-negotiate their terms of the contract to align with changing requirements of their clients. They are also redefining the workplace conditions of migratory staff. If we consider the level of scandal that surrounds any new infection, it is understandable that a routine office visit is now perceived as a high-risk activity. Client and vendor policies do not necessarily align and even if a client site is authorised to open it does not follow that the vendor will permit their staff from entering.

Nobody can predict when COVID will end or how legislation on working environments will play out. However, COVID has affected every aspect of vendor interaction for financial institutions. They have had to redefine their expectations and relationships. The notion of scaling the workforce rapidly through the use of third parties is now facing significant challenges. In turn, this has profoundly changed the industry perception of vendor management.

Bernard Perchman

Team Lead ETrading, Commonwealth Bank

Bernard is a team lead that services the Fixed Income and Rates trading platform for Commonwealth Bank. He is responsible for all aspects of the platform including compliance, performance, security, strategic differentiation and operational processes. Bernard holds an Australian Institute of Business MBA.