Building resilience into the digital transformation process

May 04, 2021 11:43 BST

Building resilience into the digital transformation process

Worldwide spending on digital transformation technologies and services increased by as much as 10% in 2020, reaching $1.3 trillion. The pace of technology adoption continues to increase around the world, and in the words of Microsoft CEO Satya Nadella, "every company is now a software company".

For most businesses, these digital transformation projects involve the outsourcing of software; bringing the innovation, expertise, productivity, and cost benefits that often come with the use of specialist solutions. However,

the more integral to day-to-day operations these applications are, the larger the risk to the buyer's business services if there were to be any interruption to the capabilities they deliver.

Legal demand for protecting software

Assessing and advising on business continuity and the risk of supply chain disruption is one area where legal professionals can support their clients. In many cases, this can also help organisations to maintain compliance. For example, the Monetary Authority of Singapore and the UK's Prudential Regulation Authority recommend that for new software transactions, financial institutions should consider an escrow agreement to help ensure business continuity, should something have an impact on the software-as-a-service (SaaS) provider's ability to deliver.

There are a range of factors counsel should consider when supporting clients taking on software agreements, to provide them with a more resilient foundation upon which their business can transform. Firstly, there is the advice that the buyer needs to understand that a SaaS contract is not a simple outsourcing arrangement, nor will a standard software or hardware contract do. They must also remember that for all SaaS providers the business model is based on the one-to-many commoditised service offering and anything bespoke, around security requirements or escrow, is likely to be an unwelcome distraction. However, a well drafted contract can do a great deal to help manage the risks involved.

The size and age of the software provider

When reviewing SaaS agreements, it is important to consider the size and age of the provider, as this can help determine the level of risk associated with using them and their commitment to an effective escrow agreement.

Smaller, new, and growing providers are often more flexible when it comes to the safe escrow of their source code. With a limited client base, these organisations tend to run a more personal account management service, providing a forum for open discussion and negotiation around the terms of escrow agreements. However, these less well-established providers are typically more at risk of financial failure, might have 'key person' issues – such as being reliant on particular individuals for their sustainability – and

are vulnerable to take over or a deliberate sale. All these factors make it even more important to have a robust business continuity strategy in place when choosing to use them.

At the other end of the spectrum, larger, well-established providers might be more viable but are generally less flexible. Stricter licensing and standard 'short form' agreements mean that there is less wiggle room in seeking to obtain particular security or escrow requirements. The buyer is more constrained and has less power in the relationship. The business risk weighs more heavily on the buyer in this case.

In either case, the escrow agreement must be part of the risk management solutions written into any SaaS contract. In addition, counsel should suggest that their client develops an effective exit strategy, identifies alternative suppliers and rehearses what they would do should a problem occur.

Choosing an escrow provider

Agreeing to store applications in escrow as part of any software transaction can go a long way towards building operational resilience and lowering overall risks for an organisation looking to use a SaaS provider. As well as ensuring business continuity, it can also help organisations to become compliant with specific sector standards and regulations.

It is therefore crucial to choose a well-established escrow provider when working with clients on software agreements and seek businesses that are both technically capable and financially sound. When working with a larger SaaS provider, more experienced escrow providers often have existing relationships and a better understanding of the software itself. This can ensure that the escrow process is well practiced, and any verification processes are easier to maintain.

Transparency and understanding of the security of the escrow provider, and the technology used to store solutions, is also vital in ensuring that your clients' business-critical applications remain secure.

Planning for the future

For clients relying on a SaaS provider, it is also important to understand how wider obligations, such as reporting security and other issues, will be met by the supplier, particularly in highly regulated industries. Being transparent about this and ensuring that the provider is onboard from the onset is key; it will need to be an ongoing relationship between the buyer and provider, as each become part of the complex web of operational activity.

With software agreements becoming ever more ubiquitous, it is likely that regulators of the future will require organisations to have considered their exit strategy, as mentioned above, to support moving from one provider to another. Questions around how data is stored, processed, and transferred by SaaS providers will become key, and getting the answers early in the software outsourcing process ensures that any transitions will run much more smoothly later down the line.

Ultimately, with changing regulatory requirements, complex supply chains, and a shifting business landscape, building resilience into software agreements can be highly complex.

In June, we'll be hosting a webinar to provide legal professionals with more insight into how an in-depth understanding of the SaaS provider's circumstances and ensuring that the agreement includes future-proof solutions, can go a long way towards ensuring operational resilience for clients now and in the future. Come join us!

Tim Rawlins, Senior Adviser at NCC Group

Find out more and register here:https://insights.softwareresilience.nccgroup.com/legalpaneldiscussion

---

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and

innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970