NTT Security

Whitepaper

Managing the risk of IT Multi-Sourcing

Two decades ago, a decision to outsource IT was an all-or-nothing choice. A company either chose to run its own IT department, or selected an outsourcing partner to do it for them.

As outsourcing has matured, much has changed. Some organizations may be on their third or fourth iteration of IT outsourcing and rather than just selecting a single provider, most now favor a blend of in-house and external capability, often across multiple providers. Today, many companies would not think of their IT infrastructure as outsourced – rather, selectively multi-sourced.

Industry analyst Gartner defines multi-sourcing as "the disciplined provisioning of business and IT services from the optimal set of internal and external providers in the pursuit of business goals". This definition indicates the strategic decision making that underpins a successful multi-sourcing strategy. Multi-sourcing is not just accidently finding that you have a disparate set of providers to manage.

Done well, multi-sourcing gives an organization access to the innovations offered by different best-of-breed providers, or the value of 'as-a-service' solutions, within a tightly connected and integrated IT model. This approach can help organizations move faster to deliver strategic and operational goals. But, this interdependency is forcing organizations to think carefully about how to capitalize on the resources of multiple (and sometimes fiercely competitive) providers within their ecosystem – all while managing the risk to the integrity and availability of business services that they provide. And particularly as cloud becomes a significant component of organizations' digital strategy. Organizations understand that their IT service providers can introduce risks into their carefully structured environments that can impact infrastructure stability.

Applying security discipline to multi-sourcing

In our experience, organizations that are building a multi-sourcing governance framework – either to operate themselves or through a primary contractor – tend to focus on commercial and contractual aspects of service delivery. Evaluating providers exclusively through Service Level Agreements (SLAs) will not highlight security risks such as access to and control of sensitive data as it moves across multiple platforms, compliance regimes and jurisdictions. Organizations may have exhaustively tested a potential partner's skills in their specific area of expertise as part of contractual due diligence, but fail to apply the same rigor to challenging the provider's security capabilities and processes. Asking the right, rigorous questions about a provider's security and understanding how they will fit into an organization's enterprise security architecture and operations is key to managing risk. And building risk management into contractual agreements requires experience of how to delegate responsibility for security controls and metrics while retaining single accountability. NTT Security has worked with its clients at various points in evaluating and engaging multi-sourcing providers – from helping an organization to understand where providers fit within its overall risk profile, to crafting and enforcing written agreements.

By 2020

90% OF EXPENDITURE ON TECH WILL HAPPEN OUTSIDE THE CORPORATE IT BUDGET [1]

Today's reality is that IT has not always been allowed to apply discipline to every technology decision within the organization. Powerful and easy to acquire tools and technologies, such as Dropbox™ – for quickly sharing a file with a colleague or partner – to Amazon Web Services™ – for spinning up development environments fast – have ushered in an era of business self-sufficiency. Tech-savvy users now increasingly purchase, control and provision their own services and solutions. And this Shadow IT shift is gathering pace, with Gartner predicting that by 2020, 90 percent of expenditure on IT will happen outside the corporate IT budget. As part of this trend, users have taken out contracts directly with third-party providers and are managing these and the agreed SLAs themselves without due consideration of the potential pitfalls of inconsistent support for end-users and security risks for the entire organization.

1. Press release: Gartner Says Every Budget is Becoming an IT Budget

No organization will be in full control of its security risk without complete visibility to all the technology being used that may be bypassing established controls and layers of security.

The question of accountability

Bringing disparate third parties within a multi-sourcing governance framework provides an opportunity for organizations to regain full control of the IT supply chain by design; transitioning, operating and supporting these user-commissioned services to ensure that they are fully aligned to both business and security requirements. Failure to take control can have significant impact not only on an organization's risk profile, but also on its bottom line and reputation.

The legislative requirements organizations face in highly-regulated sectors such as finance, pharmaceutical and healthcare, still apply whether they choose to multi-source or not. The regulated entity remains responsible for regulatory compliance and cannot pass its obligations to third-party suppliers. Many high profile data breaches can be traced back to failures within third-party providers. Reacting to a fine on a UK business due to inadequate controls within an IT provider, the director of enforcement and market oversight at the UK's Financial Conduct Authority, Mark Steward, said: "Other firms with similar outsourcing arrangements should take this as a warning that there is no excuse for not having robust controls and oversight systems in place."

This paper considers some of the steps organizations can take to create and manage a trusted collaborative ecosystem by establishing a common framework to ensure the governance of security and risk processes across multiple providers. In essence, establishing a win-win scenario for clients, technology partners and suppliers.

40%

OF ORGANIZATIONS THAT DON'T USE OR PLAN TO USE THIRD-PARTY SERVICES HAD CONCERNS AROUND DATA SHARING [2]

Developing and applying risk management to multi-sourcing

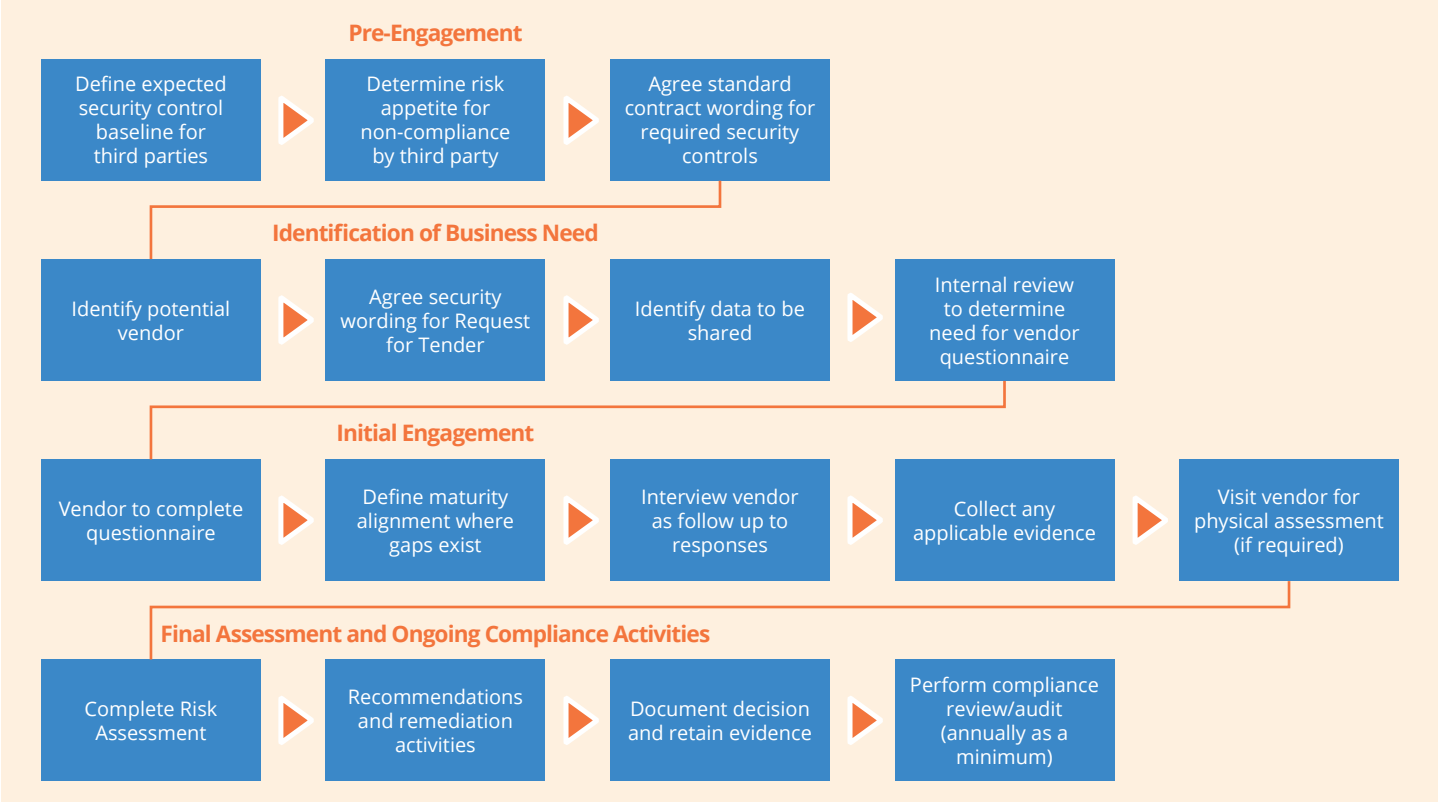
As with most applications of security in today's fast moving digital world, it is much more difficult to retrofit risk management than to build it in from the start. This means that there is work to do before entering into contracts with providers to achieve seamless end-to-end security control across a multi-sourced environment. But in our experience, it is common for organizations to already be reliant on an ecosystem of over 20 very different services when they seek support with multi-sourcing risk management. These providers may span many different business areas, such as workforce management, network management, wireless services, collaboration solutions and mobile device management, and are often not only already established, but in some cases mission critical.

1. Assessing the risks

The first step many organizations take is to perform a third-party risk assessment across all these services in line with the organization's own risk profile and compliance landscape, as part of their multi-sourcing program governance model. Only by performing this type of in-depth analysis can an organization understand what it needs to fix and how quickly – particularly in areas such as data protection, enforced by the General Data Protection Regulation (GDPR), and associated Identity and Access Management (IAM) controls. NTT Security's global Risk:Value research shows that 40 percent of organizations that don't use or plan to use third-party services had concerns around data sharing.

Not all of your suppliers will be focused on security, but to trust their services going forward, multi-sourcing governance has to be established. So, what does this involve?

Figure 1 : The process steps described below are recommended activities to include in a Third Party Assessment



2. Making trust an ongoing component of the third-party provider engagement process

For a multi-sourcing approach to succeed, organizations need to implement the right partner model – a model which allows your business units to benefit from the vast range of expertize and services available without introducing unwanted risk. To maintain trusted relationships, cybersecurity must be a component of every purchasing decision. As we have established, organizations cannot escape ultimate accountability for the security of their data and systems. The objective of a risk assessment is to highlight high-risk providers that may already be on board. And once an organization has clear visibility to the security risks of each provider, they can make informed decisions about how to embed security into the engagement, or whether there is an alternative provider that better meets their defined security criteria. Carrying out a third-party risk assessment gives you the choice of protecting what matters to you as an organization and how to establish and maintain trust in your providers, both old and new.

57%

OF DECISION MAKERS BELIEVE A DATA BREACH IS INEVITABLE AT SOME POINT [3]

3. Establishing and maintaining clear visibility of security risks with each IT provider

Having the right conversation about cybersecurity must be part of onboarding any new provider of IT services. This means including other functions such as vendor management, quality assurance and, most vitally, procurement in the development and maintenance of the third-party risk assessment methodology. They need to understand the organization's security requirements and ensure that providers are asked the right questions at the right time during any purchasing or due diligence processes.

This may mean reviewing contracts to ensure that:

- An organization maintains the right to audit providers' services for security practices throughout the period of the contract. This may mean securing agreement to monitor aspects such as IAM controls, network and endpoint activity, and log analysis. In many cases organizations are concerned about the additional burden of monitoring both their own and the third parties' ecosystems. One solution is to separate internal and external monitoring by partnering with a managed security services provider. There is little point in establishing a third-party governance framework if there is a visibility gap between what has been agreed and what is actually happening in a real-time business relationship.
- Compliance requirements are agreed – such as PCI DSS and GDPR. In our experience, organizations have had to increase the scope of their own audits if suppliers do not hold the relevant certifications, adding to the cost and complexity of compliance efforts.

4. Preparing for incidents amongst multiple providers

It's often said that complexity is the enemy of security, and even best practice multi-sourcing governance models are highly sophisticated. It is impossible to eliminate risk in business and according to NTT Security research, 57 percent of decision makers believe a data breach is inevitable at some point. Fortunately, growing awareness of cyber attacks is encouraging more companies to not only put incident response plans in place, but also to test them as part of ongoing business continuity.

But one area some organizations that have adopted multi-sourcing have yet to consider is the impact on their businesses of a security incident at one of their providers. Too many organizations would be unable to answer questions such as:

- How would this impact your productivity, system availability and integrity?
- How would this impact compliance – for example, with a 72-hour reporting window for data breach notification required under the GDPR?
- How would you detect whether an issue is within your own or third-party systems?

Our advice to organizations that take a multi-sourcing approach is to ensure that they have a comprehensive breach readiness and communications plan for if the worst happens. A strong incident response plan won't stop the breach happening – but a timely response might mean the difference between quietly dealing with the problem in partnership with your suppliers, versus the breach becoming headline news.

5. Terminating a contract

Organizations must be prepared for the termination of the outsourcing arrangement. Appropriate provisions should be made to ensure the ongoing security of information and systems in the event that a contract is terminated or transferred to another provider. This work may primarily be carried out by the procurement and legal departments, but security leaders will need to ensure they are aware of the termination procedures and the elements that could have a direct security impact on the organization. These could include returning the information as appropriate, maintaining confidentiality by the vendor, handover of services from one vendor to another, or from a vendor back to the organization itself. Security should be included in the comprehensive terms and conditions, but it is important to assess how the vendor would return the organization's information assets or fixed assets upon the termination of the third-party relationship.

2 & 3. NTT Security Risk:Value Report 2017

NTT Security recommendations for managing the risk of multi-sourcing

- It is much easier to build in agreed security controls as part of a contractual agreement than to retrofit these once a contract is rolling and a vendor is firmly outside a multi-sourcing governance model. Organizations need to eliminate the 'buy first – security later' approach by asking the right questions at the right time with support from everyone involved in the purchasing process.
- For organizations that already have contractual agreements in place with multiple vendors, security needs to be integrated seamlessly so as not to inhibit existing contractor governance and processes. This requires a holistic approach, aligned to the business objectives.
- Third-party assurance must be as high on the business agenda as the benefits that new and innovative systems and approaches deliver. IT security professionals can add significant value in evaluating and advising on the best suppliers that balance opportunity and risk once a multi-sourcing governance model is established and agreed.
- Many of our clients find that it is more efficient and cost effective to partner with security specialists to assess their third-party risk exposure and develop a sustainable security program. This may require additional, specialized resource with an awareness of multi-source provider risk – not only to plan and execute risk assessments, but to consistently monitor the organization's infrastructure for targeted threats.

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **http://www.ntt.co.jp/index_e.html** to learn more about NTT Group.