Supply Chain Risk

Trust in your suppliers

Supply chains are becoming increasingly digitalised at all levels, which, of course, leaves them vulnerable to cyberattacks. How can we mitigate risk and ensure more secure and resilient supply chains?

Supply Chain Risk

Supply chains continue to be a source of high-profile breaches and are an area of great focus. A lot of audit and assurance activities are based around those contracts with the highest commercial value which tend to be with large, well-established organisations and are frequently for commodity services. Nine23 can support you in understanding what Cyber Risks apply to your organisation and how best to understand these risks and how to mitigate them.

Commercial Reality

The majority of organisations have suppliers that are important to the delivery of day-to-day business operations. And those suppliers have suppliers of their own underpinning aspects of their services to you. You can go quite far down that particular rabbit-hole and one of the key questions to consider for any organisation is when to stop looking and rely on assurances and contractual measures with the partner to address the remainder of concerns.

As compromises have impacted enterprises through these suppliers increasing focus has been placed on providing scrutiny and assurances around supplier activity in the conduct of their duties. For IT suppliers this is typically done via log inspection, technologies like Privileged Access Management (PAM) and an array of audit activities. Highly regulated organisations have extended these audit activities out to major Cloud and SaaS providers (such as Microsoft, Amazon etc.) who now regularly conduct supplier audit activities with their enterprise clients.

Assurance Approach

The majority of audits consist of a checklist, with providers responding to templated questions on how they conduct activities in relation to the account. These are self-assessed by the providers and are often subject to limited validation. Critical providers can be subject to inspection of their activities or detailed follow-up audits and this is especially common in highly regulated sectors (Critical National Infrastructure, financial services, defence etc.).

Challenges & Considerations

Supply chains are typically too extensive for this detailed audit activity to occur consistently across the breadth of providers, so organisations typically only do so for their most critical providers or strategic partners, using the self-assessed model for the remainder.

The most nuanced and important assessment at this stage is what makes a provider critical or strategic. In many organisations this starts with commercial value of the agreement. These tend to be held with large, established firms with their own mature audit and compliance regimes, well suited to engage with these types of audit activity. These agreements are also often for broadly commodity services (software licenses, cloud service provision, property etc) which often pose more limited direct risk to the organisation, but could well be the subject of invoice fraud attacks or similar.

Breaking the Chain

As a number of breaches have shown, the weakest link in the chain has frequently been those providers who don't necessarily have large value agreements and who have links to the client environment but aren't technology firms in and of themselves – Heating, Ventilation and Air Conditioning (HVAC) suppliers featured in several high profile breaches, as an example.

Other high impact compromises have been to small, specialist providers of business process outsourcing arrangements such as forensic services, construction and Professional and Business Services (PBS). The impact of these compromises was disproportionate to the value of the work undertaken for three main reasons:

Criticality of the duties undertaken by these firms was not understood in terms of wider business process
Activities were specialised enough that alternative providers are not common and work often cannot be undertaken in-house
Firms providing these services were small enough that they did not have large security teams or budgets with which to counter such threats
So when reviewing your assurance regime you should be able to clearly articulate the criticality of any outsourced service provision and have a business continuity plan for the event of that provision being unavailable. You could also consider an 'audit the auditor' role where a 3rd party conducts supplier assurance activities on your behalf and your team focuses on auditing that provider. This is common in Service Integrator models and for companies with limited internal team capacity.

How Nine23 can help?

Organisational supply chains can be complex and extensive. The level of risk increases proportionately with this complexity and many high-profile breaches have come from the difficulty in managing this complexity.

Nine23 understand the importance of having trust in your suppliers and this can only come through an effective supply chain audit and assurance regime.

Working with your cyber security, service management and commercial teams we will help map your supply chain and evaluate the criticality and risk potentially posed through this relationship. We will propose and implement business processes and technologies, where appropriate, to enable the monitoring and management of this risk. We can also act in an "audit the auditor" model where we conduct supply chain audits on your behalf and your auditing effort is focused on your activities.

We will work closely with you and your partners to identify and mitigate supply chain risks to both parties.

We are a UK Sovereign, cyber security solutions company that designs, builds and supports end-users to use technology, securely. We are passionate about delivering the best possible front line experience and believe you should expect the same technology innovations in your work as you benefit from in your personal life. We deliver ecosystems accreditable to OFFICIAL-SENSITIVE to SECRET as part of our secure UK data sovereign private cloud, Platform FLEX.

Contact
+44 (0)2382 020300
www.nine23.co.uk
2 Venture Road, Chilworth,
Southampton, SO16 7NP