Cyber and Data Due Diligence in the 3rd party supply chain

We have heard so many stories recently from companies who have received questionnaires, running to many pages, from their clients and or prospective clients, asking about the Cyber Security and Data Protection safeguards that they have in place.
This is a response to the fact that so many cyber attacks and data breaches originate in the 3rd party supply chain.

In **May 2021, President Biden** issued a cybersecurity executive order aimed at protecting federal government networks and modernizing the nation's overall cybersecurity. This executive order had 7 main elements:

1. Enhancing threat information sharing
2. Modernizing the federal government's cybersecurity
3. Enhancing software supply-chain security
4. Cyber Safety Review Board
5. Standardizing federal playbooks
6. Improving detection on federal networks
7. Improving investigative and remediation capabilities

In March 2022, President Biden issued a further statement relating to Cyber Security (see full statement below: clink on link below) which clearly put the responsibility for security at all our doors:
https://www.thetrustbridge.co.uk/post/statement-by-president-biden-on-cybersecurity-march-21-2022

"This is a critical moment to accelerate our work to improve domestic cybersecurity and bolster our national resilience…From day one, my Administration has worked to strengthen our national cyber defenses, mandating extensive cybersecurity measures for the Federal Government and those critical infrastructure sectors where we have authority to do so, and creating innovative public-private partnerships and initiatives to enhance cybersecurity across all our critical infrastructure… But the Federal Government can't defend against this threat alone.

Most of America's critical infrastructure is owned and operated by the private sector and critical infrastructure owners and operators must accelerate efforts to lock their digital doors. *…I urge our private sector partners to* ***harden your cyber defenses immediately*** *by implementing the best practices…You have the power, the capacity, and the responsibility to strengthen the cybersecurity and resilience of the critical services and technologies on which Americans rely. We need everyone to do their part to meet one of the defining threats of our time — your vigilance and urgency today can prevent or mitigate attacks tomorrow."*

Despite the call for these measures, in a pilot program undertaken by the U.S Defense Department launched in April 2021 and designed to root out digital vulnerabilities among contractors, identified hundreds of flaws over the course of one year in a report issued on May 2nd 2022.

From the sample of 14 participating companies and 141 publicly accessible assets , the cybersecurity researchers discovered some 400 issues across these companies during the Program. This pilot was intended to identify whether similar critical and high-severity vulnerabilities existed for small-to-medium-cleared and non-cleared defense-industrial base companies with potential risks for critical infrastructure and the U.S. supply chain.

This highlights the need for all companies / organisations to check that any supplier / client/ 3rd party alliance has good cyber and data security measures and practices in place.

The Trust Bridge has developed an audit process (accredited and approved by the UK regulatory authority) with a report which will enable all participating companies to re-assure their partners, clients and suppliers that they have implemented best practice measures:

Client companies :
The key considerations when dealing with all suppliers:

- Accepting that your supplier has good security practices, good data hygiene and that no breaches have occurred, is not enough.
- No organisation can afford to take on trust that any supplier has full control of their data and that they are compliant with existing and emerging regulations.
- Clients and customers should see proof of security practices and controls, policies and actual processes from all organisations with whom they are or intend to conduct business
- All organisations should perform extensive technical due diligence to ensure their investment is wise
- Target organizations should be prepared or risk a reduction in valuation or cancellation of investment.

In line with the UK Data Protection Act 2018 and the provisions under UK and EU GDPR (General Data Protection Regulation), all organisations must ensure any data assets they hold are fully compliant with existing and emerging regulations. Most other countries and states are introducing regulations that are very similar to GDPR: **CCPA / GDPR (and UK) / NDPR / DIFC / LGPD**

This is not an issue which is going away and cyber / data privacy and protection is now seen as critical to all organisations.

If you are a supplier company, you may very well have received stringent and extensive questionnaires from your clients and potential clients.

It is now more important than ever for client companies to be re assured that the data that they are transferring to you (as a supplier) is being is held securely, who can access the data and how the data is processed and used, and that it is being transferred securely. They cannot afford to suffer a cyber incident /data breach as a result of dealing with any suppliers who are not diligent with their data protection policies and processes. Over 45 % of all cyber incidents occur within the 3rd party supply chain.

- your competitive advantage will be through increased client trust.

The regulatory and commercial importance of data privacy and security has been increasing rapidly in parallel with the growth in the information economy. In general, data are the most critical assets of a company.

The Data Due Diligence process should ensure that the supplier organisation conforms to data regulations, and if not; has demonstrable plans in place to become fully compliant.

More importantly, the client company must establish whether a supplier is aware of:

- what data assets it has
- where they are
- the level of accuracy and importance of any asset
- access permissions to data
- what physical and cyber security protocols are in place
- Is the data "portable"

This due diligence must include review of continuing processes to cope with the inevitable data security problems that will arise, such that any disruption caused will be ameliorated, especially where user data is involved.

This is not a one-off fix for any organisation.

Excellent data asset management is key to business performance and it is not an exaggeration to say it will be key to survival.

Although the current regulations of concern deal with personal data – the data assets of a company cover much more information and knowledge. In general, it behoves any company to understand data at a strategic level and not assume that, just because the company is regulatory compliant at a given time, all is well with the organisation's data policies and procedures.

The "How" of Data Due Diligence

Supplier companies are receiving more and more questionnaires from their existing and potential clients: Be Prepared
By having your Cyber and Data Protection policies and procedures documented, and accredited if necessary, in place and available for examination by outside organisations, you can shortcut many of these lengthy questionnaires and due diligence exercises.

The TrustBridge understands the data protection regulations and their practical implications, is aware of new regulations which are emerging and has the legal and technical expertise and resources to assess risk and fix what is non-compliant or should be improved.

The Trust Bridge has joined forces with a couple of global law firms and a number of expert cyber companies, combining their expertise to guide organisations through a data due diligence process fully examining the data protection landscape of any 3rd party company. We can help client companies prepare the data due diligence questions they should be asking their suppliers, and prepare supplier companies to submit the answers, guiding them through the process.

In this new data economy, data is an invaluable asset. However, the greater value is in the protection and treatment of that data. The greater value in any organisation is in its data protection polices and processes.

The TrustBridge Report can be used as an independently accredited document to send to your clients and prospective clients together with any proposal or pitch you may be undertaking. It pre-empts any supplier due diligence questionnaire that they may require to be completed.

The TrustBridge Report can also be used as a questionnaire in itself- for all organisations to use as a standard for their own suppliers to meet. TTB can review upon completion and rate the supplier organisation for alignment and best practice.