Digital Intelligence
Securing the Future

Supply Chain Hardening Project - Lessons Learned

Introduction

International supply chain hardening projects can be an immense undertaking for an organisation. Through experience, observation and participation, there are key factors for success as well as the need for flexibility and appropriate resourcing on supply chain hardening. In a sense, the organisation is about to engage in an exercise which must ask tough questions. The struggle to identify accurate data - especially if it exists in remote teams and silos - can lead to a poor outcome.

Summary

- Organisations are unlikely to understand or be able to identify the full scope or scale of their supply chain.
- Internal stakeholders must support the effort for project success. This starts with executive leadership down through to the staff involved and across to the business partners within the supply chain; it may also include communications with vendors and distribution partners.
- As this endeavour can be sensitive, effective communication is essential to ensure everyone knows the meaning and intent of the project. If there is minimal understanding of the effort, key business relationships can be damaged.
- To successfully reach the goal of visibility and achieve a measure of supply chain hardening honesty, openness, patience, and accountability are absolute requirements.
- The project will require a formal charter and deliverables along with a timeline and appropriate resources, especially business analysts, procurement specialists and, when required, IT resources such as technical experts and system architects.

Case Study

The customer was a large international maritime engineering organisation based in Europe with a supply chain that extends across the globe. The company embraced a supply chain hardening project to address key business risks and gain visibility and understanding of all the “parts” which allow the business to function. The project strategy – potentially the first poor decision made - was to view the supply chain from a top-down as well as a bottom-up approach. Although this technique was not unique in this type of project, a more efficient approach would be to use an organisational risk strategy, focused on the largest supply chain risks as the organisation perceives them: to try and do everything at once can lead to nothing of any use.

The project commenced with a data dump of 2000 contract details every 12 months from the procurement team. The intent was to construct a cyber risk profile of each relationship to assess the potential impact of a data breach of that vendor, contractor, service provider or manufacturer: in short, an entire analysis of the amount and type of information that relationship collected or processed, including

the following data types: PII of the customer's personnel, intellectual property, and financial information. The format of this data gathering exercise consisted of a short assessment, which contained multiple choice answers as well as some room for additional detail. The assessment forms were then scored and given an overall Risk Profile ranging from Very Low to Very High. The relationships which were categorised as "Tier II" or "Tier B" within the supply chain by the organisation were then followed up with a Technical Assessment using NCSC's Cyber Essentials as a benchmark.

Although this data dump approach would result in a comprehensive view of the supply chain by not using a risk-based technique, a great deal of time and effort was wasted in pursuing data from relationships that would prove to be very low risk, easily replaceable with an alternative, and generic in nature as to the services provided.

Underestimating the scale of the supply chain

Unsurprisingly, the dynamic nature of the supply chain contained several third-party dependency relationships which impacted the data collection effort and demanded scrutiny of even more relationships. The project scope expanded from the initial target of 12,000 assessments of supplier relationships to 24,000 once the data had been examined: additional resources were then obviously required.

Another perhaps fatal flaw in the project was its reliance on mass email communication, which proved to be both a data management challenge and data integrity issue. in the first two months of the project, a significant number of assessments from entities the team had not contacted were received. Investigations into this data collection issue revealed that several contacts within the supply chain were forwarding these assessments - most notably the Cyber Risk Profile assessment - to other regional branches or even sister organisations with which the organisation did business. Although the visibility on these additional entities did serve a purpose to better understand the supply chain, it exponentially increased the number of relationships which needed to be assessed. This was particularly true for those based in China.

Over time, the monthly reports on completed assessments began to provide the customer with a more accurate understanding of the complexity of the supply chain servicing the organisation's business operations. The amount of the relationships and complexity of the supply chain naturally became a concern for the customer as the scope of the project changed: as it was no longer confined to assessing the security practices of their relationships, the client was now forced to consider their own internal documentation practices, policies and procedures and conduct internal due diligence, as all these new relationships and entities were discovered by the project team.

The new visibility of the supply chain from the data collection effort could have been seen as a benefit, revealing internal weaknesses in process, procedures, and due diligence. Unfortunately, the organisation became overwhelmed and viewed the discoveries unfavourably. The data revealed gaps in execution of due diligence on these newly discovered relationships and supply chain entities. The view from team leaders was that these factors and the diligence requirement constituted a "distraction" to daily

operations and staff productivity. These were unintended consequences – and perhaps a failure of the project to plan for "unknown supply chain partners". What was apparent was that the procurement team and contract management were weak and perhaps embarrassed the organisation: they had no idea of who they were truly dependent on. Eventually, the customer informed us that their supply chain consisted of more than 150,000 business relationships.

Stakeholder buy-in

Another list in the unintended consequences of the supply chain hardening project data collection was the mounting internal resistance to the project. This was especially true after the revelation that the organisation was potentially unaware of the complexity and entities in their own supply chain and did not hold a central or accurate database of their supply chain contacts.

The resistance to the project's revelations came mostly from individuals in executive and departmental leadership positions. However, their attitudes and lack of enthusiasm may have had an impact on the contract managers and members of staff the project team relied upon for the information required. Several of them were openly hostile to being involved in the project, viewing it as outside their job description or area of expertise. The project team would seek engagement with these individuals and managers when the security team encountered difficulties. In most cases, the cybersecurity team was able to resolve miscommunication or misunderstandings.

There were persistent challenges with some members of staff. Eventually, to try and reduce the potential of conflict, the project team created packages of information about the exercise, including a presentation, case studies of supply chain attacks and a decision matrix framework. This, in hindsight, was perhaps another fatal flaw: had materials been prepared in advance the project could have synchronised with the day-to-day operations of the resources required to execute the data collection effort. Unfortunately, this new clarity did not completely address the previous relationships and residue of conflict.

All projects require stakeholder buy-in for them to be effective. This extends from the highest levels of executive leadership down to the department heads, team leaders and finally members of staff involved. The project's revelations made the organisation feel uncomfortable and the subtext of the data gathered could be interpreted as "poor performance" on the part of the managers and teams. This situation quickly descended into acrimony, delays and accusations of the project being "a waste of time and money".

Miscommunication

As noted previously, several of the setbacks and challenges of the supply chain hardening project related to poor planning and lack of communications from the project team.

Interestingly, one of the first attempts to efficiently gather assessment data into a manageable format was thwarted by the supply chain entities themselves for valid or semi-valid reasons. Although the project team had selected a SaaS platform to manage the assessment effort – which the organisation had internally vetted and deemed secure for processing the cyber risk profiles - some suppliers with different regulations, levels of risk, or internal policy requirements were not comfortable putting sensitive and potentially sensitive data into a third-party tool they had little knowledge of. The result was the data would now be entered into Excel spread sheets, abandoning any hope of automation and efficiency of the data-gathering effort.

Externally, the aims of the project were thwarted by the supply chain entities themselves. As the team sent out more assessments to the contacts, the information they received from the procurement teams and contract managers – without prior communication about the data-gathering – resulted in the customers unsurprisingly acting against them. Many of the team's assessments were reported as Spam or Phishing attempts by supply chain partners.

The organisation had not effectively communicated the project's goals to their own supply chain entities. This outcome was exacerbated by the fact that details held by the contract managers and procurement team may have been incomplete and/or inaccurate. Although in subsequent communications this was clarified, initially the supply chain hardening project may have had a negative impact on the organisation, as following this first effort emails were struggling to hit supply chain partners, and due to security controls in those entities' environments, the organisation's business communications were now being blocked or directed into spam folders

Over time, this spam issue appeared to ease, but it never fully went away. Additionally, because of the lack of communication and full understanding of the required information, the project team had unintentionally ended up contacting supply chain entities with which the organisation was in financial or legal disputes or had otherwise ceased to conduct business with. Other organisations were unhappy to be hit with "spam" with no forewarning.

It is worth noting, however, that each email the project team sent also included a document, an "attachment", making the initial communication even more suspect. The document did explain the project, the recipient's involvement, and expectations of them. In addition, the Director of the Cybersecurity Department for the organisation issued email notices on several occasions to emphasise the importance of the project.

In some cases, this was not enough. With the initial communication botched by the project team, this now placed an onus on contract managers and procurement team members to personally communicate "no this is real and we need your help" to successfully obtain completed assessments. On several occasions, the project team was given licence by the organisation to indicate that a failure to comply with the assessments may have an impact on future contracts and continued business - a message far outside scope, generally threatening and detrimental to a cordial business relationship. If such communications

were needed, it would have been far better to have an executive of the organisation make such requirements known.

Reliance on honesty for accuracy

With nearly no third-party way to verify any of the cybersecurity information received from the supply chain entities, the data collection effort may have been doomed from the start. The major concern was the degree of honesty with which the supply chain organisations would fill out the assessments. Most of the criteria were "self-assessment" in the form. The project team had no real way of telling if answers given were inaccurate except if something seemed ambiguous with the assessment form itself, or if the responses that came back were vague and/or conflicted with previous answers.

The assessments themselves were sent to contacts within the supply chain from the contract managers and procurement team's database. These individuals would most likely not have had much insight into the cybersecurity practices, policies, and procedures the project team wanted to gather information about, although it was requested they pass the form on to a relevant party who had either the knowledge and/or the authority to provide the requested answers. In some cases, the recipients would respond after communicating with the relevant party. Sometimes the assessment would reach the hands of IT or cybersecurity departments; in a few cases a member of the board would sign off on the assessment. At any stage in this process an individual may accidently provide misinformation because of misunderstanding or accidentally give inaccurate or "aspirational" information to obscure potential lapses in cyber hygiene and a lack of security best practices from their own internal stakeholders, as well as their own supply chain.

It was evident - as far as the project team could tell – that honesty was not so much the issue; rather the focus was on competence and understanding of what had been asked in the assessment. This was especially true when it came to the technical security assessments. Some businesses within the supply chain, such as small mechanical manufacturing companies, had no understanding of what was being asked of them, such as the implementation of a requirement of whitelisting applications and sandboxing capabilities of anti-virus solutions. At other times, language barriers caused issues with the data collection.

Surprisingly, this language or culture barrier resulted in an erroneous data collection result. A handful of assessments had evidently been tailored to seem as though the company responding posed a higher risk to the organisation than they did. A few of them had gone so far as to open the assessment backend, remove the scoring formula and manually rate themselves a "Very High Risk". The project team determined these actions may have been taken to make the supply chain partner seem more important to the organisation than they were.

Effort and risks

Supply chain hardening projects are a huge challenge, especially for global organisations with thousands or tens of thousands of suppliers. Poor practices in data management can make such an exercise nearly impossible, taint any data gathered and cause distress internally and externally with supply chain partners. A critical enabler is to take a risk-based approach and focus on those partners who enable operations. Large organisations must ensure they hold an accurate and centralised contact database.

Communication before – both internally and externally - and during the project is essential for the data gathering effort. The project must be explained prior to the launch with lead time to allow the supply chain entities to understand what is expected of them, as well as to allow them to field any concerns they may have with the customer or the project team. A clear path of escalation with reluctant internal resources or external supply chain partners must be established to handle those relationships if there are concerns or resistance. Supply chain hardening projects rely heavily on the cooperation of the supply chain entities. Their honesty, understanding and competence to accurately complete surveys and assessments is key.

Projects such as these can collapse for a verity of reasons, ranging from project scope creep through to the politically sensitive nature of the data. Careful communication is needed to ensure that the data does not make internal stakeholders and their teams embarrassed and defensive about their potential failings at record-keeping.

More efforts are required for proactive communication and contingency planning to enable project success. Face-to-face ideally, or Teams/Zoom calls to address concerns of challenges are vital to address internal stakeholder concerns or supply chain entity challenges in gathering accurate data. Although the project was carried out with the best intentions, this case study illustrates the difficulties which can be encountered in a supply chain hardening business effort. *

Jake Kelly,
Cyjax Intelligence Analyst

** Please note this case study does not refer to any current or past customer of Cyjax Ltd. Should you have any inquires please reach out to sales@cyjax.com*

About Cyjax

Cyjax was formed in 2012. Working closely with the financial sector, we developed technologies and methodologies to help stem the advance of digital threats impacting banks and consumers around the world. We quickly established ourselves as a leading provider of cyber threat intelligence capabilities across all industry verticals, a journey we continue today. Cyjax is built on its own growth and remains wholly owned by its founding members in the UK.

Cyjax Limited
The Old Chapel, Union Way
Witney
Oxon OX28 6HD

info@cyjax.com
+44 (0)20 7096 0668
www.cyjax.com