Third Party Risk Management

The Holistic Approach

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Third party cyber risk management is one of the biggest challenges faced by security teams – and certainly one of the hardest to solve. But it's also among the most important, with 61% of organizations experiencing a data breach via a supplier in the last year, and supply chain attacks up 78% in 2019.

The issue is becoming increasingly urgent, as:

1) Enterprises share critical or sensitive data with an increasing number of suppliers (on average 583 per enterprise)
2) Enterprises are raising their internal cyber bar, causing attackers to pivot towards their 'soft underbelly' – their supply chain, in order achieve their goals
3) Supply chain attacks have yielded tremendous results for attackers – with an average of 13m records being lost per third-party breach

Some of the most high profile and damaging breaches of the last few years have involved suppliers or third parties, including:

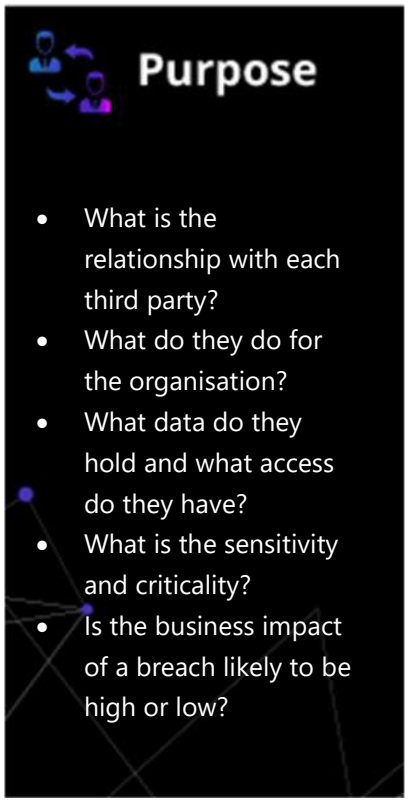
Attack	What Happened	Impact
Target Retail	Compromised through third-party managed air-conditioning system	110m consumers affected $200m+ in remediation and lawsuits
APT10 (Chinese Nation State attack)	Gained access to victim systems and data via third party managed service credentials	Unprecedented access to intellectual property and sensitive client data
NotPetya Ransomware	Infected victims through third party accounting software	Companies such as Merck and Maersk lost hundreds of millions as operations were halted. Global impact reached several billion dollars.
Quest Diagnostics	A hacker accessed over 100m patient billing records by breaching Quest's outsourced collections agency	Class action lawsuit ongoing (as of May 2020)

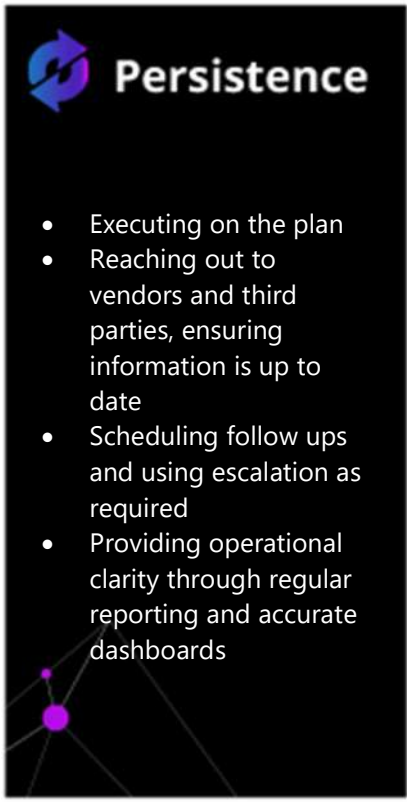
Despite the prevalence of third party breaches, organizations are yet to properly address the issue, with only 34% maintaining any kind of centralized supply chain inventory, with many of those struggling to yield positive security outcomes. Indeed, the complexity of third party relationships, combined with a lack of resources able to deliver an effective program, makes cyber risk management a seemingly impossible task.

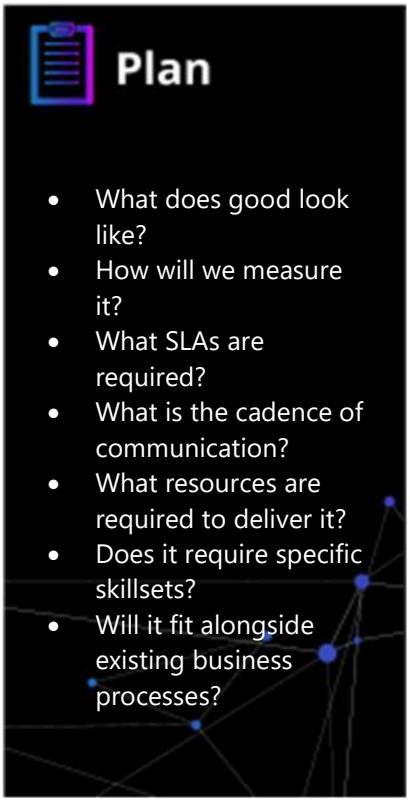
THE THREE P'S

HolistiCyber believes in three key principles that allow the implementation of an effective program. By effective, we mean a cost-effective program that reduces third party cyber risk while engaging the business and the people within it.

We refer to these principles as the three P's of third party cyber risk management:







When implemented poorly, a third-party risk management program creates unwanted overhead, repetitive workload, and poor-quality inputs leading to outputs without context. As such, the results are treated as a box-ticking exercise, and can give a false sense of control while failing to contribute to the security posture of the organization.

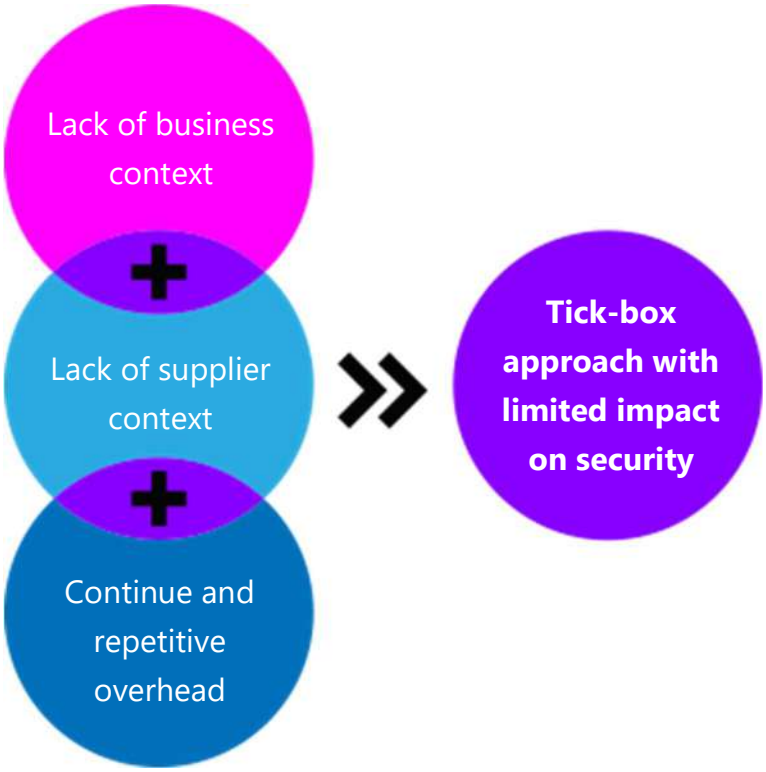
However, when implemented effectively, a third-party risk management program will help a business keep track of, manage and ultimately decrease the risks associated with compromise through the supply-chain. Given the magnitude of the problem and the cost of breaches associated with third-parties, any positive steps in this direction can be considered a clear win for the business. A healthy by-product of such a program will also be clear compliance to regulatory requirements mandating ongoing third party assessments.

Through the rest of this paper, we will detail the approach taken in delivering our fully managed service, end-to-end without any overhead on client teams – leaving them to focus on strategic and technical priorities inside their organization while still gaining clarity and governance across their third party risks.

EXISTING APPROACHES

The most common approach to centralizing third party cyber risk management is still to 'do nothing'. However, with the ever increasing cost and frequency of breaches via third parties, regulatory requirements, and the growing reliance on the supply chain to deliver all manner of essential services from cloud to office space, the do nothing approach is clearly unsustainable.

Those organizations that have implemented a third party risk program often ask their in-house security teams to select a system, or administrate the security element of an existing third party management platform or even keep spreadsheets and documents.



However, experience shows this approach generally results in a software-driven, box-ticking exercise that is not tailored to meet the business needs of the organization, and rarely takes into account the nature or relationship of the service being delivered by the third party. As such, the inputs and output are ineffective in understanding risk in the context of the business – something that is widely understood by all involved but are persevered with regardless. Furthermore, the program requires significant ongoing overhead from security teams to deliver, both in-house and in third parties being assessed. All of this together can quickly de-prioritize the issue, and lead to a lack of impetus in making a real change.

CREATING AN EFFECTIVE THIRD PARTY CYBER RISK PROGRAM

In the executive summary we introduced the three Ps of building an effective third-party cyber risk management program. Plan, Purpose, and Persistence. Here we will explore their meaning in more detail.

PLAN

This phase is crucial yet often overlooked by those firms seeking to upgrade an existing program, or those embarking on third party risk management for the first time. As with any security program, we need to define objectives – e.g,, "reduce our third party risk exposure by 20% each year for the next three years," or "reduce new vendor onboarding times by 30%." These should be consistently measurable, in order to demonstrate whether the program is working and maintain buy-in, or to ensure that changes can be made quickly as required.

Unless a fully managed service is selected to deliver the program, the organization will also need to consider the balance of resources required. As with any security program, the service will be comprised of people, process and technology – and the temptation is often to focus planning around 'what software will we use', rather than determining the people and skills required to deliver effectively in the context of the business. As with most facets of security, the people and the process are the most important to get right. Generally speaking, a well-oiled, capable team using spreadsheets will deliver a more effective outcome than an under-resourced program driven by software.

Regardless of this balance, the program should be governed by a series of SLAs. These may include:

- How many new third parties onboarded per month
- Time window for third parties to complete updates – and agreed escalations if missed
- Frequency of vendor renewal
- In-depth assessments carried out per month (e.g. SOC2 reports or onsite visits)

Finally, organizations need to consider their third-party risk management policies. Many tend to adopt a one-size-fits-all approach which can fail to meaningfully assess third-party cyber risk. However, once a third-party assessment tool has been implemented, the cost of tailoring policies to fit different third-party relationships can be prohibitive. Planning for this flexibility is advisable – otherwise organizations will be in a situation where they have to 'adapt to the tool', rather than have the tool adapt to their specific need.

PURPOSE

When the purpose of a third-party relationship is overlooked, third-party risk management becomes a tick-box exercise and loses its security and business benefit. It may seem obvious, but in reality this is harder than it first appears.

This is because the purpose of the relationship should drive the line of questioning, the context, and any weighting applied to responses – and it should be tailored per third-party in order to deliver an accurate representation.

To do this properly requires ongoing, human interaction, an understanding of what each third party does in business terms, and what it really means in terms of risk. The approach can be high-touch, requires experience and business nuance, and cannot easily be defaulted to a software-driven check-box exercise. However, when implemented properly, the results can be dramatic – with third parties remaining far more 'bought in' to the process, while those delivering the program internally have real belief in the output of their work. All this leads to an engaging, highly accurate program which serves as the basis of effective third-party risk reduction.

In addition, by making sure critical and sensitive parties are stringently assessed but allowing a lighter touch approach for those that are less sensitive, an organization can actually accelerate its overall third party onboarding, while removing blockages and hurdles from the business process.

For illustration, let's look at two third parties.

1) A document management system vendor that hosts the crown jewels of the business
2) An HR outsourcing service

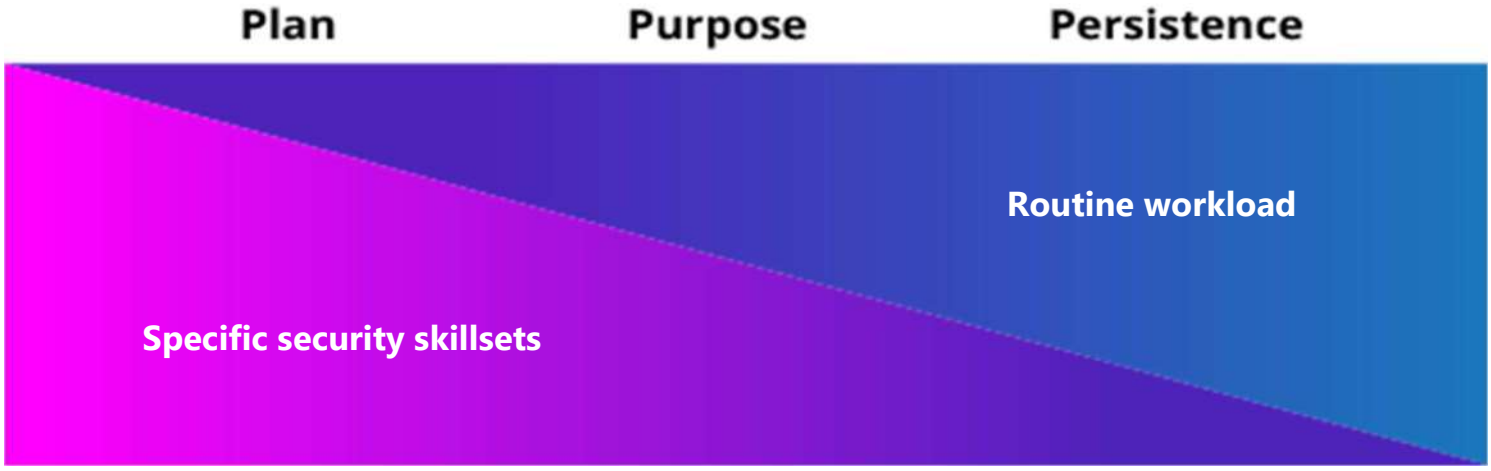
These two companies are likely both of high importance to the organization – but have different sensitivities and criticalities that mean the information we need to gather regarding security is very different.

For the document management system vendor, we would want to understand the SDLC process and employee training programs from a secure code perspective – to reduce the risk of vulnerabilities acting as a backdoor into the organization.

Conversely, the HR service handles a different type of data, and so poses a different risk to the organization. This may be mainly driven by PII and sensitive recruitment processes – and so the third party assessment needs to address this risk. However, if the HR service also provides a system to manage its workflow, then this again changes the third risk profile, and should tailor the risk assessment accordingly.

PERSISTENCE

Once the initial setup is complete, it is time to execute the plan – an operational move that carries a very different resource profile and mindset to that needed in planning and understanding the security implications of business purpose.



The ongoing delivery of a third-party risk management program is a significant operational overhead which can be extremely expensive to deliver. All too often we hear about security teams swamped with day-to-day third-party compliance, which can be demoralizing while also causing the organization to miss out on security progress elsewhere.

However it should be noted that security team input continues to be beneficial in assessing the purpose of a third party relationship. This allows the correct context to be applied in order to drive relevant information gathering. Furthermore, security team input is advisable in interpreting the reporting and dashboards presented by the third party management program, in order to gain a picture of the complete attack surface.

For a program to deliver long-term value for money, organizations should be alert to ensuring processes are continually organized, clear, followed and are persistently executed on-time. To achieve this, organizations should ensure an appropriate level of management overhead and ongoing governance.

THE HOLISTICYBER MANAGED SERVICE

HolistiCyber delivers a fully-managed service in order to address the challenges presented by third-party risk management.

The service follows the principle of the 3Ps – plan, purpose, and persistence, and covers all phases of the third party risk program. From setup, tailoring, and onboarding, right through to following-up with your third parties in accordance with pre-defined playbooks, HolistiCyber will deliver the end-to-end service while providing dashboards and reporting.

Unlike many other outsourced services – and those delivered by a software-based approach, HolistiCyber believes that truly understanding the business and its third party relationships is critical, as this informs the most appropriate data collection and contextual interpretation. Our approach ensures the program is always tied to business risk, and that third parties and in-house teams alike are not swamped with data they know to be irrelevant. We know that investment in any third-party cyber risk management program can be substantial – and as such we are geared to deliver rapid measurable impact and substantive business benefit.

Furthermore, your security team will be freed up to focus on additional complex cyber challenges faced by the business.

The service is priced on a 'per third party' basis and is scalable across all sizes of business, from those with ten third-parties to those with several thousand.

In addition, in-depth reviews are included where required – ranging from SOC2 assessments through to on-site visits on your behalf.

New York

Anthony Carpinelli
VP Revenue
+16465685357
anthony.carpinelli@holisticyber.com

London

Peter Cohen
Managing Director EMEA
+442038075355
peter.cohen@holisticyber.com

Tel Aviv

Ran Shahor
CEO
+16465685357
ran.shahor@holisticyber.com