Managed Security
and the 3rd Party Cyber Risk Opportunity

APRIL 2021

Managed Security
< Forum :

Contents

Introduction

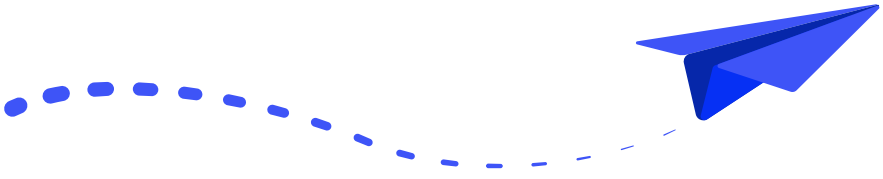
Since 2016 the Managed Security Forum (MSF) has acted as the industry group for Managed Security Service Providers (MSSPs). The group is operated by security industry veterans, working on behalf of the industry to facilitate communication and collaboration, offering a forum for MSSPs to discuss industry challenges and engage with stakeholders as a single voice. Members run the gamut of security services providers, from outsourcers to systems integrators to global and regional specialists.

Previous research by the MSF has delved into educating buyers on what to expect from managed security, the immediate impacts of the pandemic on the sector, and how MSSPs are evolving their offer to move beyond detection to the identification and elimination of cyber risk.

This issue of cyber risk has only grown in importance during the pandemic as risks have shifted and evolved. Boards are increasingly aware and informed regarding the cybersecurity threats to their companies, and many are now looking to understand and address these threats in the familiar language of risk.

Third Party Cyber Risk (TPCR), which describes the risk present among an organisation's suppliers and other partners, has become one of the most intensely discussed at the board and executive level. This focus has been growing in scale and importance for several years, and further evolved in the last year as large sections of the supply chain were confined to working from home, significantly altering the risk calculus.

This report explores how MSSPs can help customers address the increased cyber risk posed by third parties, and the commercial and technical benefits that can accrue for those MSSPs who recognise the opportunity. Data used in the report comes from interviews with several MSF members, research from BlueVoyant (an MSF member) and conversations with end users and in-house security experts.



The market for third party cyber risk

Risk is front of mind for many of us. Earlier research from the MSF highlighted how one challenge the security industry is grappling with is communicating with corporate boardrooms by bridging the gap between cyber threats and operational risk.

This predicted that cyber risk management will become a new point of differentiation for providers, and this has been taken up by influencers in security and adjacent sectors as McKinsey published a series on cyber risk[1], the NCSC published risk-based advice[2] on buying cyber insurance and a range of MSF members, such as BlueVoyant, launched extensive cyber risk offerings[3]. In fact, the MSF now predicts that cyber risk demand will continue to expand, driving a range of sub-categories, with TPCR likely to be a significant source of growth in managed security during 2021 and 2022.

Growth in TPCR is driven by demand, which in turn comes from the increasing interest of regulators, alongside the increasingly common events and breaches that demonstrate how sources of cyber risk in the security landscape are shifting. In recent years large breaches have increasingly originated from third parties, with the SolarWinds breach the most recent example to demonstrate the breadth and depth of cyber risk in the supply chain of even sophisticated cyber bodies. In the last two years the role of third parties in these events is becoming more explicit; Delta airlines lost data for hundreds of thousands of customers, leading to a class action lawsuit and a series of negative headlines. The company sued its vendor[4] [24]7.ai for causing the breach, in this case by allegedly providing access to its own third party. The biggest scandal in the history of Facebook involved mishandling of data by third party Cambridge Analytica[5], while General Electric also recently grappled with a third party breach[6] that exposed detailed employee data including drivers' licences, birth certificates and passports.

On the regulators side, the UK government has been sounding the alarm for a while and is now stepping up investment. It completed a review of the telecoms supply chain in 2019[7], initiated due to geopolitical concerns but highlighting supply chain risk as an issue in the process. This was backed up by an NCSC report into supply chain risk within the telecoms sector[8] in July 2020. The Prudential Regulatory Authority in turn issued a consultation paper on TPCR at the end of 2019 and extended this in June 2020. Google Cloud CISO and former Goldman Sachs board director Phil Venables predicts that as supply chains become inherently digital, regulatory and legislative expectations will continue to increase and "continuous evidencing of conformance to multiple standards will be expected."

International trends in cyber regulation mirror this focus, as the world's biggest governments step up their efforts to regulate supply chain cyber risk and provide guidance on addressing it. In December 2020 the EU reviewed the NIS directive[9], the first EU-wide legislation on cybersecurity, and implemented NIS2[10]. This aligns regulation across the bloc and includes a specific focus on addressing supply chain risk and management accountability. The Cybersecurity Administration of China published and implemented the Cybersecurity Review Measures[11] in 2020, imposing more stringent scrutiny over the cyber supply chain of critical information infrastructure operators. The USA's Cyber and Infrastructure Security Agency published the two-year report[12] on the work of its Supply Chain Risk Management Task Force in December 2020, committing to continuing and extending its mandate.

On 7 January 2021 the Australian Cyber Security Centre issued updated guidance on Cyber Supply Chain Risk Management[13] and Identifying Cyber Supply Chain Risks[14] to provide best practice guidance on TPCR. As governments take an increased interest in the area, regulation is trending towards greater scrutiny of TPCR across vendors, partners and the broader supply chain. This significant increase in regulatory activity will inevitably become a major driver of awareness and investment, bringing the evolving security sub-sector further into the mainstream.

While TPCR has been steadily growing as a source of risk, the pandemic has brought supply chain risk into sharp consideration for many enterprises. Security teams worked flat out to make widespread remote working secure across their company, but very few have had the time or investment to apply the same scrutiny to their supply chain. Research from McKinsey[15] in July of 2020 showed large enterprises were investing in securing their networks, messaging and IAM, but not GRC. Companies who had previously relied on security reviews and periodic audits of their vendors' security suddenly found they lacked the relevant data on the same companies when the work is being performed entirely remotely. This demonstrated the blind spot in the corporate security stack.

Supply chain disruption came under scrutiny across the globe in 2020 due to COVID-19 and Brexit, but the second order effects on supply chain cyber risk are only now coming to light for many companies. Some companies have responded by bulking up existing data collection based on manual processes, but this does not scale to meet the challenge. At the larger end of the market, the number of vendors each company works with can be overwhelming; MSF member BlueVoyant found that the average large British company works with 1013 third parties. The increased demand, coupled with the scope of the challenge, highlights the need for new approaches to TPCR.

Supply chain disruption came under scrutiny across the globe in 2020 due to COVID-19 and Brexit, but the second order effects on supply chain cyber risk are only now coming to light for many companies.

Third Party Cyber Risk Lifecycle

Addressing TPCR starts with the establishment of a system to identify all vendors and third parties who have access to any company data. This mapping process involves following all data from creation and distribution to disposal, and includes identifying what procedures are in place for handling data.

Companies then implement processes that include cyber risk assessment in the procurement process, with all potential third parties scrutinised for potential cyber risk as a central consideration. Here the security team typically works hard to build a relationship with sales, legal, recruitment and other functions that frequently deal with third parties. Security teams will often have to take a hands-on role bedding in new processes early on, with the goal of automating as soon as practicable.

Addressing risk does not stop once vendors are agreed, particularly for strategic partners with access to sensitive data. Onboarding partners is an essential step in TPCR. During this stage both parties should agree processes around communication, alerting on incidents and events, metrics used to assess risk as well as the tools and technology that create these metrics. During onboarding is often an important time to communicate that the monitoring relationship is an ongoing process, and not a box to be ticked in order to get on with things.

Companies emphasise onboarding over monitoring, with Gartner reporting that 73% of efforts devoted to risk identification are allocated to due diligence and recertification efforts with only 27% of effort reserved for identifying risks over the course of the relationship. Policies around TPCR aim to create an environment where regular security updates are expected and both parties are able to acknowledge and assimilate shared data efficiently. Some will share threat intel or offer limited sight into their security stack. Best practice TPCR is based on dynamic data, as all relationships are constantly evolving, meaning flexibility and adaptability are at the heart of good TPCR partnerships.

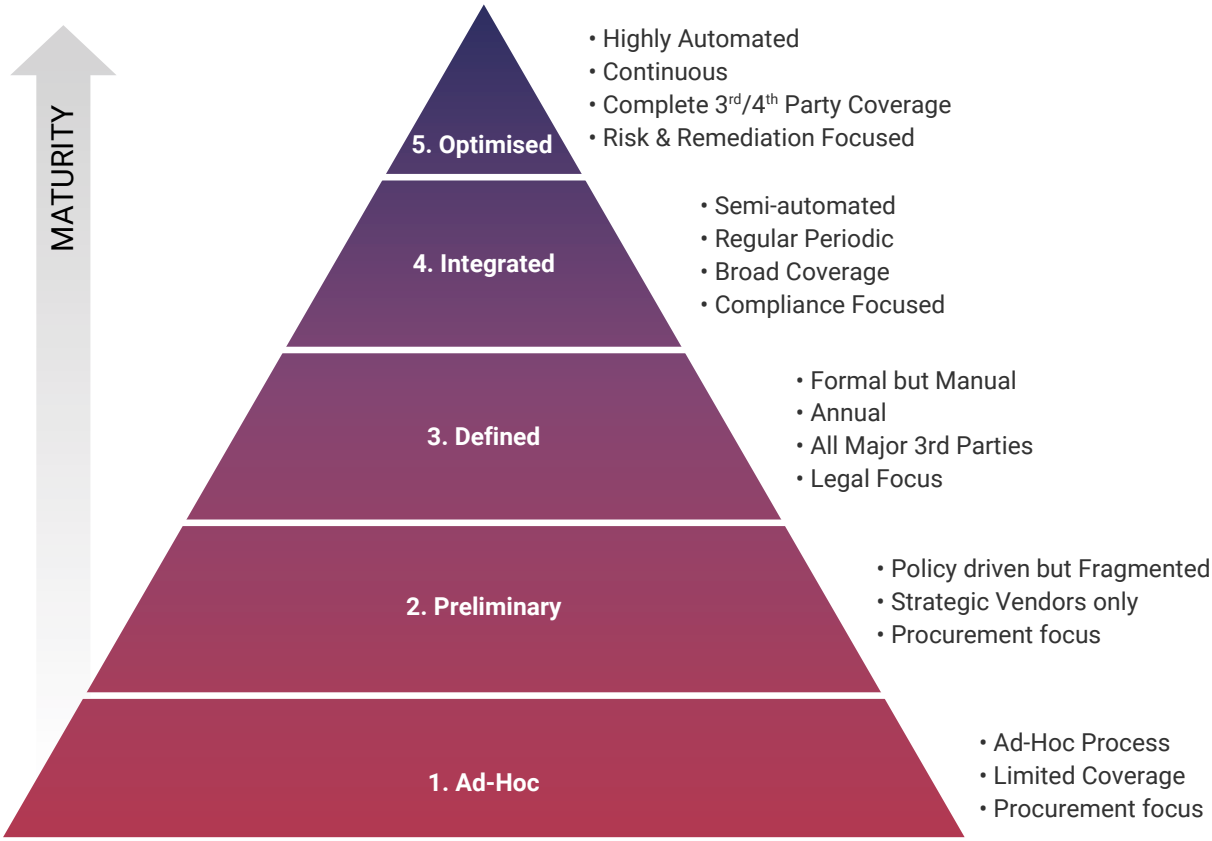
Finally, companies typically ensure that their vendor contracts and processes include detailed provisions for handling data in the case of termination. This is where lawyers will often add value by including clauses that require partners to hand over or destroy sensitive data, as well as revoke access to physical and digital systems. Improperly terminated relationships can create shadow IT that in turn creates cyber risk.

THIRD PARTY CYBER RISK LIFECYCLE

Third Party Cyber Risk Maturity Model

In recent years TPCR has grown organically, as first movers in security and risk built bespoke models and processes to capture the increasing share of risk involved in sharing data with third parties across the supply chain. As more breaches emerged this philosophy spread, creating demand for technological solutions that could standardise and automate the process of identifying risk. Clearly the direction of travel here is one way, as companies are sharing more data with an ever-growing number of third parties and more high-profile breaches are shown to originate with vendors and suppliers. This is especially pertinent when the relationship with third parties changes over time.

The below diagram lays out the distinct maturity phases that are evident in what is evolving from an organically grown function to a central cog in corporate risk. This diagram was based on detailed interviews with a range of MSF members, who described the varying degree of maturity that they currently see across the various customer bases.



MANAGED SECURITY FORUM – THIRD PARTY CYBER RISK MATURITY MODEL

The most basic implementation of TPCR that MSF members described, is a system based on Ad-Hoc processes that are not well-defined or embedded. Risk identification is limited to clauses in vendor agreements that use boilerplate language related to data protection or similar regulation. While it is possible that risk can be identified and mitigated in these systems, this only works if a highly capable security team goes above and beyond their stated roles with an extremely hands-on approach. In the rare cases where this can exist in practice, it is neither scalable nor sustainable.

At the next level of maturity companies have a Preliminary framework in place for identifying risk, but one that is not universally applied. Here a company identifies what it considers to be strategically important vendors and inserts some interventions at routine points in the engagement. The focus is normally on initial procurement, particularly onboarding, and manual solutions are the most prevalent.

Next, we see a Defined process brought in that covers the majority of third parties but stops shy of full coverage. At this stage, a company will typically issue questionnaires to suppliers to ensure they meet necessary regulation. These are distributed, collated, and reviewed manually, which can lead to delays in rectifying any risk that is identified. While reviews are regular, they are normally annual, which removes the ability to rapidly identify risk and respond. Questionnaires for this stage are legalistic, focusing on avoiding liability and reducing recourse to legal action. This level of maturity can also include annual audits and penetration tests, again delivered manually.

This stage of maturity was fit for purpose in an analogue age but has been rendered obsolete. As processes became digitised and the number of vendors that make up a typical supply chain has skyrocketed, manual solutions to track and record static risk cannot keep up. Data shows that this began as widespread digital transformations took hold from about 2014 and accelerates to this day.

THIRD PARTY CYBER RISK – SCALABILITY CHALLENGES

Integrated TPCR makes up the next level of maturity. Here the company has introduced some automation and moved beyond annual reviews and onboarding as the sources for assessing risk. Audits and pentests are undertaken more regularly and based on subjective considerations. Monitoring includes regulatory requirements such as modern slavery, anti-bribery, and minimum wage compliance, while supplementing the compliance data collected with some real time cyber indicators.

Level four is where companies incorporate security ratings technology as standard, solutions that provide useful data points for assessing risk. These provide an outside-in assessment of third parties and offer useful data points to enhance security. The security industry seems to be reaching a consensus that they are a useful signal and improving in effectiveness. A bad rating is seen as evidence of likely risk, where a good one is more indeterminate. They played a central role in establishing integrated TPCR as best practice, provided they are deployed in an environment where more data means more value.

But the pace of digitisation, accelerated by the global pandemic and overhaul of work practices, has created a new frontier in cyber risk management. While security ratings have enhanced the visibility into TPCR, they are increasingly seen as moving the problem further along the spectrum. Identifying risk is a useful first step, but it is only useful as a means to remediate issues and reduce the risk. Companies at level four maturity will identify risk across their supply chains but will not always have the capacity to address it. Getting this right means having sufficient talent and resources in place, which often means working with a third party that can implement the ratings while providing a full service.

The final level of maturity is when the above model is taken and automated across all parties. At this Optimised stage of maturity, a company proactively remediates problems and mitigates risk based on live data. Experienced professionals use open-source data, security scores, scanning and proprietary tools to identify weaknesses in third party security and compliance, with the authority to engage with and actively help third parties remediate issue and reduce risk. Rather than focusing on legal liability or compliance, companies at this level consider risk across every touchpoint. The weighting of risk is based on the quantity and sensitivity of data shared with each third party, and the mixture of automation and human input that is applied varies accordingly.

The security industry seems to be reaching a consensus that they are a useful signal and improving in effectiveness.

Problems faced by customers

While customers' demand for third party cyber risk solutions has increased in recent years, driven by increased risk and focus from regulators, the methods in many cases have not met the needs.

Integrated TPCR was the gold standard of handling third party cyber risk until recently. This approach introduced technological solutions into what had been seen as an analogue problem, where it was addressed at all. Companies with the aspiration to identify risk across every partner relationship approached the problem with more of a technological bent, adding breadth and rigour to a process that addressed the growth in data touchpoints across the supply chain. Getting to level four maturity allowed companies to get a handle on their expanding supply change and proactively respond to certain breaches among their partners.

Level four companies will often incorporate self-assessments, but there are concerns that these do not always comply with regulation, particularly in sectors like financial services and life sciences. The use of security ratings tools to identify TPCR has improved the visibility into such risks but has created the problem of operationalising this knowledge. Identifying risk is useful but it often amounts to handing a company a different sort of problem, the need for remediation.

Several MSF members share anecdotes of companies that had previously used manual methods of data collection progressing through the maturity stages, along with those that did not have full coverage across their vendors. A new baseline seems to be emerging around fourth party risk; assessing a company's partners' partners. Systems that do not have full coverage across every touchpoint where data can be accessed are becoming obsolete, as well as those without the means to process all data and address risk. Organisations without the technical resources and well-defined processes to address newly identified third party cyber risk could find themselves no better off from a risk reduction perspective, and potentially even worse off due to explicit knowledge of risks that cannot be remediated.

These challenges are defining the Optimised maturity level for organisations, the new benchmark for best practice in TPCR. Here security data is captured across the supply chain in real time, analysed by trained specialists and converted to risks, which are remediated and reported. Inputs are automated, with the option of additional data gathering from GitHub, social media or the dark web.

Fully optimised TPCR solutions require buy-in from board level, a risk framework that acknowledges and accounts for the company's compliance and subjective needs, and a tech-driven stack that incorporates automation and provides dynamic data as an output. All of this contributes to TPCR remaining a prominent security issue into the medium-term. Solutions and services that can track the flow of data until it stops and monitor all potential liability are in demand.

Scaling Third Party Cyber Risk

Market-driven demand for automation and technical expertise in supply chain risk has created a significant opportunity for MSSPs.

In particular, Optimised TPCR allows MSSPs to be a point of integration that provides third party cyber risk management services, from identification of risk through to remediation. This relies on continuous monitoring, while using this data to enhance the other security services provided to customers.

Some companies remain at level three maturity, where they recognise the need for granular assessment and advanced onboarding of strategic vendors but do not cover every vendor or incorporate automation. Others at level four implement technological solutions and widespread coverage of vendors, but with a one-size-fits-all model that does not deliver remediation and ultimately reduce risk.

Delivering a service that offers level five maturity to customers requires a mix of mostly automated monitoring with complex remediation, done at scale. Where MSSPs can add value is by supporting on remediation throughout the TPCR lifecycle. This includes establishing and modifying the TPCR system in place, assessing potential vendors using scanning and ratings data, onboarding vendors by establishing contractual SLAs regarding data security, remediating any risks that arise by notifying the client and working with the third party to resolve it, and ensuring best practice data hygiene is observed when terminating partnerships.

There are no silver bullet tech products that can facilitate this service in isolation; different tools have different pros and cons. While automation is critical, there is always going to be a human component to getting TPCR right if Risk Reduction is the desired outcome. Context and analysis are important when evaluating the relationships with third parties and the resultant effect on cyber risk.

The primacy of organisational context has led to many companies handling TPCR in-house, struggling to build a specialist function that can monitor and manage hundreds and even thousands of vendors. This is typical of the maturity process seen in other sections of the cyber security industry, where customers will attempt to develop their own capability before the market matures to a point at which vendors can provide more complete solutions and services.

Even those few companies that have the budgets and capabilities to develop a full Optimised TPCR monitoring capability and to act on this new knowledge, find that building and maintaining these functions is complex and expensive. The investment needed to address TPCR across a complex modern supply chain is too much to keep up with the scale of the threat for many companies. By working with an MSSP, companies can access industry-leading talent and technology, with services that incorporate their internal data and scale to their need.

The MSSP advantage

For companies seeking to progress from either Defined (L3) to Integrated (L4), or from Integrated (L4) to Optimised (L5) TPCR maturity, MSSPs can add real value. Managed security providers have a long history of integrating the latest automated solutions, setting and maintaining security standards in line with SLAs and compliance, monitoring security, and responding to and mitigating risks.

Most will have the technical talent to operate TPCR tools, the legal and managerial experience to set and maintain security SLAs for vendors, and the forensic capabilities to investigate risk and take steps to reduce or avoid it.

Where customers are seeking to advance from Integrated to Optimised, MSSPs offer additional resource in processing data such as security ratings. Managed security providers are comfortable with integrating a wide variety of data inputs, as well as working with large volumes. This allows them to more accurately incorporate ratings and other data points when assessing risk.

Even for customers who are already at the Optimised level of maturity MSSPs can add value, by scaling capacity up or down. This can add resources during strategically important onboarding or acquisitions, or simply free up internal resources for more strategic work.

The rapidly expanding number of vendors in the modern supply chain, coupled with the emerging risks in a remote-first world, makes optimised TPCR better suited to delivery as a service at scale. Companies dealing with over a thousand vendors quickly see the benefit of outsourcing risk remediation rather than trying to significantly expand their security team in a market where talent is hard to find.

As companies follow best practice and treat cyber security as a risk rather than a subset of IT, it is easier to articulate how TPCR risk in the supply chain bleeds into other areas of risk. Security ratings, scanning, questionnaires and other TPCR inputs will have a significant impact on other challenges and considerations within the security function. Decisions about architecture, for example implementing zero trust, or more tactical decisions around how controls such as DLP are implemented, should be taken with a full understanding of how data is shared with partners and what risk is created as a result. Where MSSPs are involved in providing these services they can see considerable synergies by incorporating level five TPCR data.

Customers increasingly want to pay for remediation and problem solving, rather than more data and inputs for internal security teams that are already operating at close to full capacity. Having the service delivered by an MSSP offers the buyer solutions rather than more problems.

Third party cyber risk as business development

When MSSPs offer TPCR they have an opportunity to broaden the buyers that they sell to within companies, while getting exposed to potential future customers through remediation. A well-run remediation service can be a pipeline of new business, providing MSSPs a distinct advantage by giving them a more detailed understanding of the challenges faced by their customers' partners and also presents the opportunity for MSSPs to demonstrate their capability first-hand as a means to win new customers.

It also provides access to the MSSPs customers' executive teams. Most MSSPs sell to the CISO and very often to the Security Operations team, but TPCR offers the opportunity for MSSPs to build relationships with a range of different executives, unlocking new budget pots and enabling new services to be delivered.

Chief Risk Officer

As cyber security continues to evolve into being treated as a business risk, corporate CROs are finding a lot more of their budget and time spent on cyber risk. MSF members we spoke to report that CROs often own TPCR, working in collaboration with procurement to monitor supply chain risk. These executives want to address security and require everything to be defined in terms of risk identification, mitigation and cost.

Chief Information Officer

This function often wants to digitise and automate wherever possible, so working with the CIO is a chance to understand strategic technology direction. Because TPCR is inherently cross-function and digital, many CIOs are in favour of the process, and will approach it from the perspective of integrating the service and its output across the organisation. MSSPs working with CIOs should demonstrate how TPCR data supports additional security services across the organisation.

Chief Financial Officer

In many companies the CFO will be responsible for a portion of company risk, and in every company, they will be sensitive to the reputational cost of a breach and the potential fines that can accompany it. For listed companies in particular, CFOs will be conscious of the risk associated with market-sensitive data. This risk can often be a useful starting point for discussing the potential application of TPCR services with a CFO.

Vendor Spotlight

BlueVoyant, an expert-driven cybersecurity services company, has recently launched a managed third party cyber risk service that includes continuous, risk focused monitoring and remediation to cover the entire supply chain. The company aims to provide a service that offers the same breadth of service across a clients 3rd parties as a good MSSP offers into the internal client environment.

Below are three real life case studies involving companies that found that the scale of their supplier ecosystem and the personnel needed to handle vendor remediation was unsustainable, despite their sophisticated cyber teams.

These case studies illustrate the need for continuous monitoring, scalability to cover the entire supply chain, automation and the resources needed to achieve that scale. They underline the personnel and expertise required to ensure issues are successfully managed through remediation. All three of these case studies involve companies which are highly sophisticated with impressive cyber teams, but even they found that the sheer scale of the supplier ecosystem and the amount of data involved in external monitoring, along with the personnel that would be needed to get vendors to fix problems, is unsustainable internally. Outsourcing to an end-to-end managed third party risk service allowed these busy cyber teams to focus their skills on top priorities, while retaining visibility of the whole supply chain.

i. Zero tolerance for ransomware. A major US automotive manufacturer retained the Managed Risk Service to reduce exposure to ransomware in its extensive supply chain, monitoring more than 1,000 companies in real time. This allowed analysts to discover previously unknown signatures associated with the Trickbot module known as 'Anchor', which infected host companies across the supply chain. By contacting the critical priority supplier during the initial stages of the AnchorDNS infection, staff put a proactive mitigation plan in place, ensuring the manufacturer's vehicle production schedules were unaffected.

ii. Preventing attack through poor IT hygiene. A Singapore-based global engineering company onboarded a new data services supplier, when the service quickly identified three RDP ports open in this supplier's network. Further investigation revealed that one of the IP addresses also had an FTP server openly accessible to the internet via anonymous login (no password required). The entire file system was accessible, leaving the company open to potential legal action and potentially exposing third and fourth parties to infection. Instead, the service offered a remediation plan to the supplier to address the issue and take preventive measures for exposed files.

iii. Proactive risk reduction. Following the recent release of four critical vulnerabilities in Microsoft Exchange that are known to be leveraged by state-sponsored actors, a global financial services organisation needed to know its exposure across its 30,000-company ecosystem. Within 90 minutes the service identified all observed Exchange servers, including versions and IP addresses involved. This identified 5,700 that were then triaged and prioritised, allowing urgent remediation advice to be sent.

An effective Managed Risk Service (MRS) assesses, prioritises against risk thresholds, and delivers a specific remediation plan directly to the vendor. It then confirms to the client that actions have been carried out.

A fully managed 3rd party cyber risk service does more than assess the risk or bury the customer in data from which it cannot extract value. An effective Managed Risk Service (MRS) assesses, prioritises against risk thresholds, and delivers a specific remediation plan directly to the vendor. It then confirms to the client that actions have been carried out. Just as a good MSS provides companies with total visibility of their own environment, and remediation, an MRS aims to do the same for the supply chain. This external visibility, with appropriate escalation, covers every point in the vendor lifecycle, from the point of onboarding forward. Instead of logs feeding into an internal SOC, external metadata and advanced analytics feed a ROC (Risk Operations Centre). The principles of reactive and proactive defence apply in the same way. For existing and legacy supply chains, a sophisticated service can be as proactive as an internal SOC is for company networks: it can take a wide range of proactive threats or CVE alerts and map them instantly across the supply chain, isolating and closing off possible threat vectors before they are exploited.

Conclusion

The shift towards cyber risk management in the security sector has been well-documented over several years, by the MSF and elsewhere. But the identification of Third Party Cyber Risk as a central component to this risk outlook has been more of a slow burner, only thrust into the spotlight following prominent breaches or pandemic-driven changes to working. In the last year, a consensus has begun to form around the need to secure the supply chain, driven by stakeholders such as regulators, product vendors and multinationals. This consensus will continue to be driven by breaches and regulatory pressure.

At the same time, managed security providers have faced downward pressure on margins even as their sector sees increasing overall investment. Services are being automated and commoditised as providers are forced to offer more mature and sophisticated services in order to remain profitable and competitive. While there is clearly a role for MSSPs within the security ecosystem, that role continues to evolve and MSSPs must evolve with the market.

The MSF belief is that these two factors can come together, and the managed security industry can play a leading role in shaping and informing the consensus around third party cyber risk. This capability will grow to become a more central part of the security stack and a greater source of security data, allowing MSSPs that offer it as a service to cross-sell and build a more strategic relationship with customers. In some cases this may hasten the demise of providers, but it will also provide opportunities for new business models built around a strategic relationship with more senior executive relationship at client level.

To learn more about the MSF visit:
https://www.prevalent.ai/managed-security-forum/

Or email:
MSF@prevalent.ai

References

1. https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-in-a-digital-era
2. https://www.ncsc.gov.uk/news/experts-first-advice-on-cyber-insurance
3. https://www.bluevoyant.com/bluevoyant-crx-press-release-sept-2020
4. https://www.databreaches.net/delta-airlines-sues-247-ai-over-2017-data-breach/
5. https://www.standard.co.uk/news/world/record-facebook-fine-will-spark-change-in-handling-of-personal-data-a4198376.html
6. https://www.tripwire.com/state-of-security/featured/ge-data-breach-third-party/
7. https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference
8. https://www.ncsc.gov.uk/information/5g-and-us-sanctions-round-up
9. https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive
10. https://www.lexology.com/library/detail.aspx?g=dbf9f9ad-04cd-4c7f-83dd-86eb9fd63e78
11. https://www.lexology.com/library/detail.aspx?g=5d777758-4f5a-41fb-8b2a-a305a6a093a0
12. https://www.cisa.gov/publication/ict-scrm-task-force-year-two-report
13. https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management
14. https://www.cyber.gov.au/acsc/view-all-content/publications/identifying-cyber-supply-chain-risks
15. https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets