CIO ACADEMYASIA

MANAGING THIRD PARTY RISKS IN THE DIGITAL-FIRST AGE

A report published by CIO Academy Asia

Produced in Partnership with adnovum

The Long Invisible Tail!

August 2021

This report is based on the insights shared by speakers and participants during a virtual workshop engaging more than 20 C-level technology leaders representing organisations from the various industries and local government agencies.

We are witnessing massive investments in digital transformation across industries. The driving force behind these investments can be attributed to new digital technologies and their disruptive potential to businesses, heralding the rise of the Digital-first age.

Rapid digitalisation has been occurring not only in technology systems; it also has had a transformative influence on the operating models, customer engagement models, and even fundamental business models of organisations. Often, these transformations are facilitated by third parties - vendors, partners, collaborators, consultants - as no organisation possesses all the capabilities and resources in-house to manage their digital transformation, while staying competitive in their respective market.

Applications Programme Interfaces, or more commonly known as APIs, have also become the de facto standard for businesses to connect their applications together and transact securely. APIs enable businesses to connect quickly with ecosystem partners and optimise business processing at scale. Gartner projects that by 2023, more than half of the world's business transactions will be completed through the use APIs. Leading software and security service provider, Adnovum, as more than 7 billion APIs under management and is expecting this number to grow rapidly.

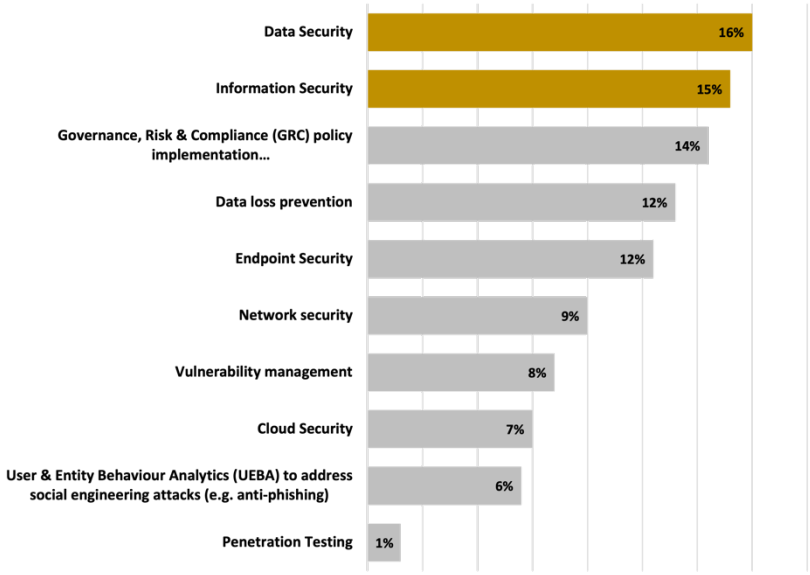
While digital transformation can help organisations capture new growth opportunities, they also introduce new risks in the process, adding complexity to their existing risk profile.

The Perfect Storm: 8 Key Trends Shaping Risks in the Digital Era

CIOAA's recent Tech Trends and Priorities 2021 Survey conducted for the Southeast Asian region highlighted the top 3 focus areas for leaders to improve their cybersecurity posture; (i) Data Security, (ii) Information Security, Governance, Risk, Compliance and (iii) Third Party Vendor Management. It was indeed very telling that most organisations are concerned about data breaches and their capability to manage third party risks.

INSIGHTS FROM OUR COMMUNITY

Your organisation's cybersecurity posture is the collective security status of your total IT. What are your areas of focus? (Select top 3)



Source: CIO Academy Asia, 2021

CIOAA's research also highlighted eight key risk-related trends which are shaping the 'perfect cyber storm'. These are: work from home, supply chain disruptions, accelerated digitalisation drive, cybersecurity skills shortage, massive third-party dependencies, shift to the cloud, budget squeeze and spikes in fake news (weaponised misinformation).

In the larger context, managing third party risks becomes crucial for organisations to protect themselves from security threats and ensure their survival in the long run. These include measures ranging from improvement in data and security postures, navigating regulatory changes (governance, risk, and compliance), managing third party vendors, and API security and management.

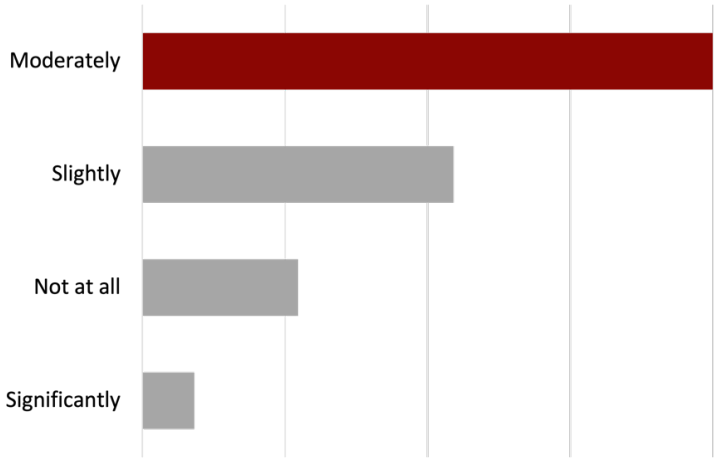
Third Party Risk Management: More than Cyber

According to **Lawrence Ang, Founder & Executive Director of Landz Consulting and a former CIO of the Monetary Authority of Singapore (MAS)**, third party risk management is more than cyber. He aptly titled his presentation as 'the long invisible tail' since it has many touchpoints and many unknowns that have no end to it. In today's context, the new norms such as work from home, budgetary constraints and attrition and outward mobility of manpower - they all pose risks to organisations.

Organisations are undoubtedly exchanging much more data with a larger network of third party supply-chain partners and third party vendors. Overtime, the sheer number of legacy APIs and data pipes create governance challenges akin to "satellite debris" that is hard to manage and leave vulnerabilities that could potentially have detrimental consequences to the organisation. **Adnovum recommends that organisations implement a single orchestration platform to gain full visibility across internet and intranet API transactions, so as to improve policy management and reign in active and inactive APIs within the organisation.**

2021 CIO SURVEY INSIGHTS

Has the recent spate of third-party related cyber-attacks and regulatory shifts impacted your cybersecurity plans?



Source: CIO Academy Asia, 2021

Third party risks span across contractual, operational and cyber-related risks, and all these have to be taken into account. Similarly, regulatory compliance is equally important. In the context of Singapore, the TRM guidelines by MAS are paramount. These guidelines provide a set of best practices for guidance on the oversight of technology risk management, practices, and controls to address technology and cyber risks. Within these, the guidelines on the management of Information Assets and management of third-party services become extremely relevant for third party risk management (due to supply chain disruptions or vendor risks).

For example, under the MAS TRM Guidelines (clause 3.3), Inventory Management (under Management of Information Assets) is critical. “It’s a pain to get it (inventory management) right but it’s a bigger pain to keep it right,” said Lawrence.
In this regard, organisations should ask themselves: do we have an inventory of inventories? These include:

1. Assets (including data)
2. Service Catalogues (or at least Applications)
3. Configuration (CMDB)
4. Users, Shadow IT and all IT personnel
5. Vendors (including Contracts)
6. IDs Inventory (especially System and Privilege IDs)
7. Activity Logs
8. Change Management
9. Backups and Restores
10. Controls & Risk Register

To manage these risks, Lawrence suggested a risk-based approach, depending on criticality and materiality (vendor database, inventories). Criticality will include confidentiality, integrity and availability of third-party services.

In the advent of large-scale remote working and increasingly hyper-connected supply-chain networks, Adnovum recommends 5 IT security practices to protect your users' digital identities and manage third party user risks:

1. Enforce requirements for users to create strong and unique passwords, if passwords are required for authentication of user identities
2. Choose two-factor or password-less authentication
3. Read permissions and settings on the personal data that users share with third party mobile and web applications
4. Encrypt internet and website connections
5. Avoid clicking on questionable links

Third Party Risk Management: The Difference Between Theory and Reality

It is true that it is easier to talk about, than to implement, controls for third-party risks. According to Lawrence, this is because of three main reasons: there is no sight (as they are third parties), no oversight and no control or influence over service levels or downstream service providers or architecture. Sometimes, we are merely price-takers when it comes to third parties! However, organisations can exert influence over third-party suppliers through the following:

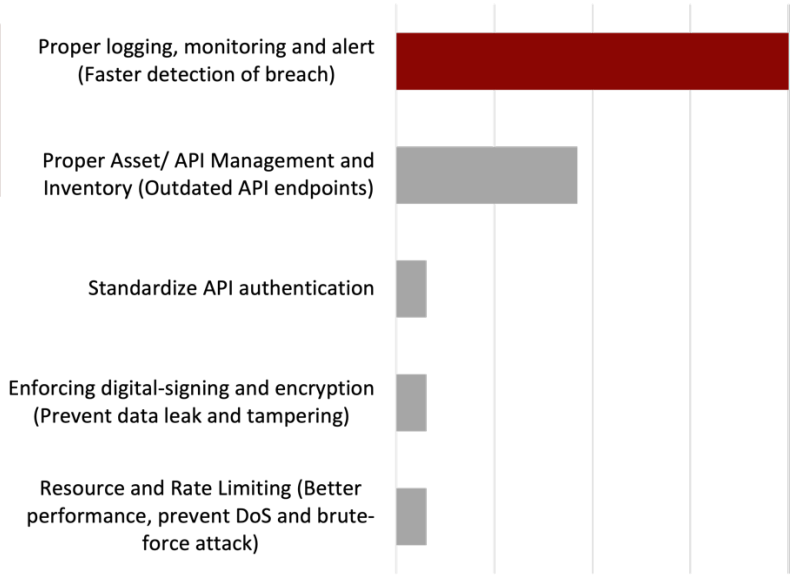
1. In pre-contract stage - through measures such as due diligence, site meet, management meet up, personal screening, terms and conditions, and even choosing the country of arbitration if things go wrong
2. Throughout the contract period: by steps such as access and activity review, personal reviews and screening, ops and services review, management meet up, site visit, etc.
3. In case residue risks are still not at acceptable levels, take "manage or mitigate" measures through technical or process controls.

API Governance: Do you have an API Strategy in place?

In a recent survey conducted by CIOAA, the results highlighted top security concerns in managing third-party risks - API management and API security, data management, cloud security, and identity and access management.

2021 CIO SURVEY INSIGHTS

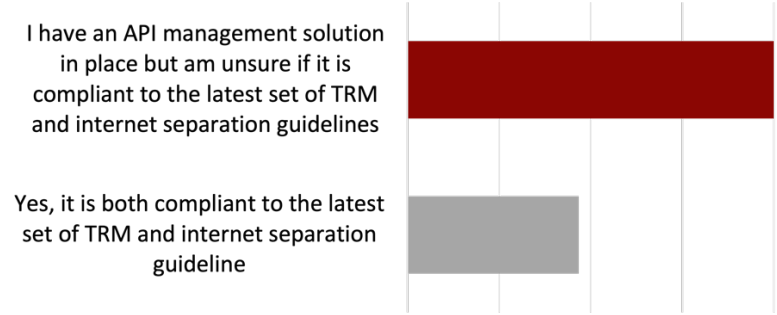
What is the most urgent priority for your 3rd party management risk management plans?



Source: CIO Academy Asia, 2021

2021 CIO SURVEY INSIGHTS

If your organisation operates an existing network of APIs, do you have an API management strategy in place?



Source: CIO Academy Asia, 2021

According to **David Chan, Managing Director of Adnovum Singapore**, API management is crucial today as we see rampant data breaches (the Solarwinds breach being the most recent critical example). Chan suggested that the Solarwinds incident may have triggered MAS's revision of TRM guidelines. Specific focus on API management could have helped in mitigating the damage done through breaches. In this respect, inherent API governance has a significant role to play in securing third party API access.

Chan suggested that organisations could turn existing businesses into a platform with APIs by leveraging existing assets such as algorithms, information, analytics, and resources. The other approach to mitigate risk could be internet separation (zero trust). With reference to figure 1, Chan highlighted that APIs are the future of B2B. According to Gartner, by 2023, more than 50% of B2B transactions will be performed through real-time APIs. Integration leaders must support both Web APIs and EDI since some B2B partners will use both. He also said that APIs provide a potential solution to B2B onboarding issues.

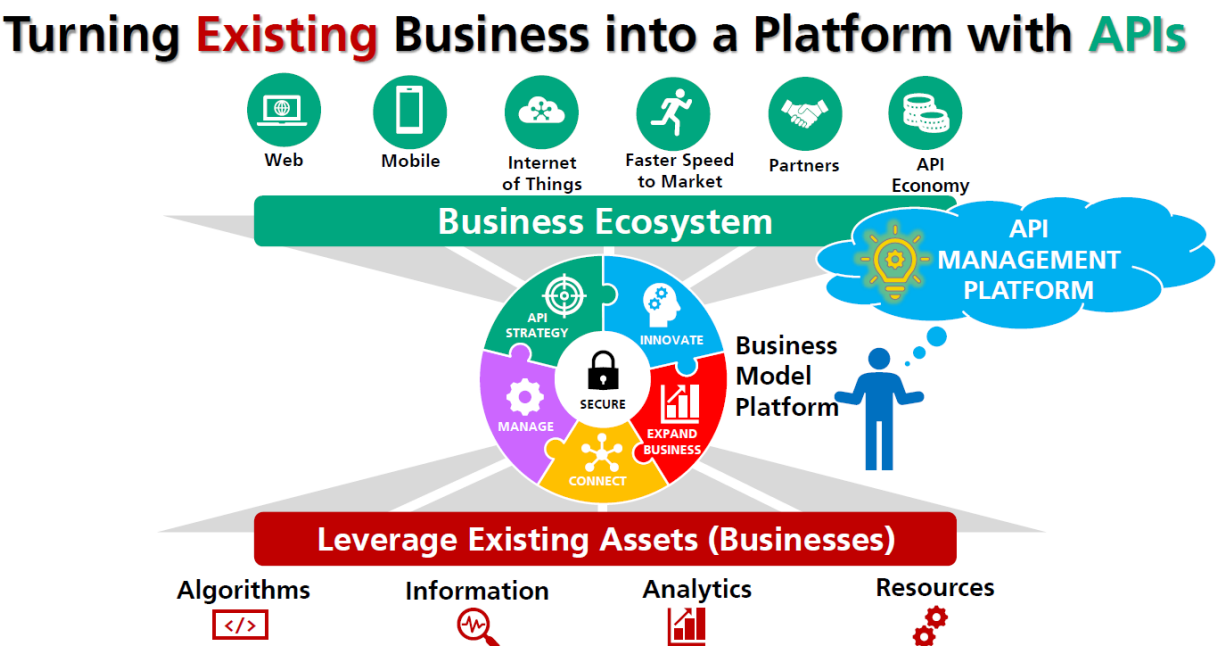


Figure 1: Source: Adnovum

Open Risk Culture: Getting it Right and Keeping It Right!

As an organisation, our challenges can come from different stakeholders. Lawrence said that they could come from audit or risk-based committees, senior management's 3 Es (Exco Emotional Emptiness and what can go wrong will go wrong!), enterprise risk management, audits and regulatory imposition (such as MAS' TRM Guidelines). Aligning of risk expectation across all these stakeholders is a prerequisite for third party risk management in the organisation.

As organisations transform to thrive in a digital environment, it is crucial that they integrate their workforce into the transformation journey. No matter how smart your API strategy is or how thorough your vendor risk management policies are, you as an organisation need to construct a digital culture thoughtfully. This culture should have elements of principles of experimentation, smart risk-taking, continuous learning, and collaboration. And you need this not only within your organisation, but you also need to transmit this culture to your contractors, vendors, and other workforce participants.

According to Lawrence, digital risk management requires the overhaul of culture beyond technology processes and the following could be helpful in its shaping and implementation:

- It's good to open up as a culture: have an open risk culture
- Work with the team collectively
- People are assets - open everything but trust nothing
- Focus on the solution
- Never blame the vendor
- Manage your auditors skilfully - don't hide anything from them and be open with them

Key Takeaways from Practitioners

1. Technology will help in risk management but your relationships, a smart workforce, they too must be in the mix to mitigate the risks.
2. Besides smart technology, you also need intelligent people because they will do more than just checking the boxes.
3. Like KYC, have a KY3P (Know your third party). Pay attention to your vendor onboarding policies
4. Have visibility on the data exchanged with vendors. Don't just tick the compliance boxes, go beyond that!
5. A key best practice is to use tech automation tools and automate policy enforcement of access.
6. Network segmentation and internet separation minimise the risk of lateral movement should users or third-party partners suffer a breach.
7. You must pay attention to the top 3 vendors. Have a good relationship with the vendors during peacetime; if you do so, during a crisis, they will go beyond the call of duty.
8. Have a good relationship with your auditors, earn their trust: this can help you go the extra mile.
9. Vendors are not malicious. Sometimes even they have not fully evaluated all the potential risks. It's best to develop and nurture a good relationship with them.
10. Third party vendors pose uneven risk postures (as only some are matured enough); alignment then becomes an issue and they need constant education.
11. Some third-party vendors cannot be easily replaced despite difficulties in meeting risk management standards; stricter data governance and network access policies must be imposed with such vendors.
12. Shadow IT is a big problem: with restrictions placed on devices, it becomes untenable. People bring their own devices to work, adding risk. It is advisable to review archaic policies concerning use of personal devices within the organisation

Refer to Figure 2 below for a full view of Adnovum's API Management capabilities

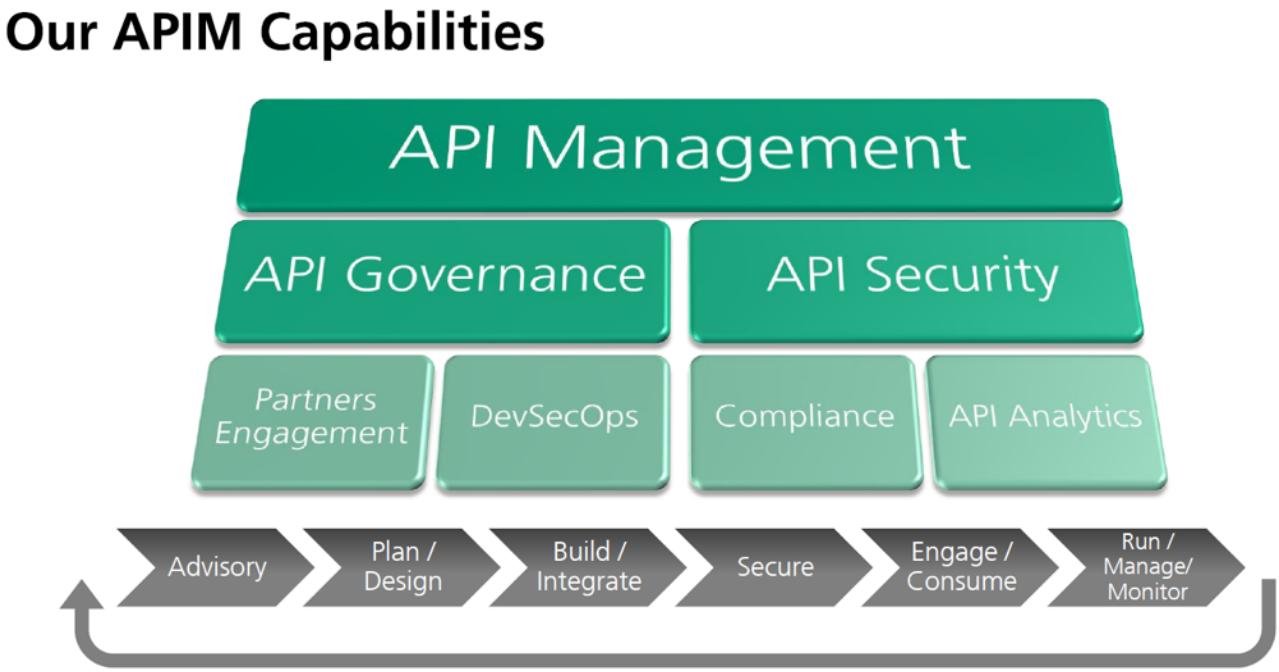


Figure 2: Source: Adnovum

Contact AdNovum for a complimentary consultation on your APIM strategy today!

CONTACT US HERE

Adnovum Singapore Pte Ltd | 3 Shenton Way, Shenton House, #23-03 S068805

+65 6536 0668 | info@adnovum.sg | www.adnovum.sg

This research primer is prepared by CIO Academy Asia in partnership with Adnovum

www.cioacademyasia.org