ANOMALIX

END TO END THIRD-PARTY RISK MANAGEMENT: ENABLED THROUGH IDENTITY AND ACCESS MANAGEMENT

WHITE PAPER

PREPARED BY: ANOMALIX

TABLE OF CONTENTS

The traditional enterprise has been through many changes in the last decade. New technology paradigms such as cloud computing, mobile devices at work, and the IoT, have created a complicated and interconnected work environment. One of the results of this technology led 'globalization' of the workplace has been an increasing dependency on third parties and an inherent trade-off between security and convenience.

A recent Gartner review of this increased "organizational complexity," found that 53% of senior leaders agree there is an increasing dependence on third parties, often extending to fourth and fifth parties. These additional parties cover a wide range of entities, from non-employees such as contractors and freelancers to business partners and third-party software and service providers. However, third parties bring increased risk.

> A Deloitte 2019, third-party governance and risk management report **found that 83% of organizations experienced at least one third-party related incident in the last three years.**

Identity and Access Management provides the backbone of a third-party ecosystem to manage this risk.

1. The Evolution of Access Management

Third-party ecosystems have always existed. However, the advent of cloud computing and Software-as-a-Service (SaaS) has changed the landscape and increased risk. Increased connectivity across disparate devices and people increases risk by adding entry points across the ecosystem.

Modern third-party risk management (TPRM) attempts to minimize the risk of third-party resource use by the process of engagement, due diligence, and monitoring of third parties. A survey from the Center for Financial Professionals (CeFPro) looked at the maturity of TPFM and identified key trends:

1. TPRM programs are increasing in sophistication but still require work to manage increasing cyber-risk.
2. *Cyber-risk is the greatest third-party concern for boards.*
3. More TPRM programs are using specialist technology to manage risk.

Current Trends in Third-party Risk Management

Risk, technology, and increasingly sophisticated TPRM programs are driving several trends in the industry:

Security vs. convenience

As businesses seek to reap the benefits of embracing outsourcing, freelancing, SaaS solutions, and other third-party options, an often-subconscious compromise is made. Especially when under pressure to act fast, security descends on the priority list while convenience rises. As a result, data secured within safe perimeters are replaced with data distributed across global cloud infrastructures. Critical tools that were once proprietary and highly protected are now rented from third parties with open access to remote workers. Privileges, once restricted to vetted full-time employees, are now shared with freelancers and contractors. In this operating environment, companies everywhere are sacrificing security for the convenient nature of third party adoption.

Weak links

Third-party ecosystems must be reliable. Any weakness in the chain can have negative effects on productivity. Cybersecurity concerns across the chain are a key trend in ecosystem reliance. Third-party members, including non-employees and software, are often targeted by cybercriminals as they are seen as the weakest link. An example of an up and coming cyber-threat is a variant on the popular scam, Business Email Compromise (BEC). Due to the perceived vulnerability in a third-party ecosystem, this social engineering scam has a new variant known as 'Vendor Email Compromise' or 'Third-Party Email Compromise' (TPEC). Instead of going after the main company, the fraudster targets an ecosystem member.

Regulation updates

Recent changes to the technology landscape, as well as consumer behavior, have resulted in regulatory updates. Many laws and directives now expect third-party organizations to be included in cybersecurity planning and security measures. A 2017 Ponemon Institute report "The Internet of Things (IoT): A New Era of Third-Party Risk" found only 31% of respondents were reviewing the landscape of third-party risk and regulation. Since the report, regulations such as the UK's IoT code of practice, expect more third-party responsibility.

Nth party risks

4th and 5th parties are often left out of the third-party equation. However, they could offer an entry point in an attack chain to move up to the main, larger enterprise parent. Visibility of 4th and 5th parties is an important trend in helping to de-risk the third-party ecosystem.

IAM for third parties (TPIAM)

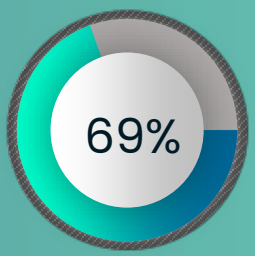
Supporting the cybersecurity efforts to protect the entire extended third-party ecosystem is identity management. Specialist tools that are designed for the complexities of identifying, onboarding, managing, and offboarding non-employees and other third parties, are essential to managing risk. These TPIAM tools provide the means to secure third-party collaboration. They are based on creating a secure, verified identity backbone and enforce robust authentication and access control on a need to know basis.

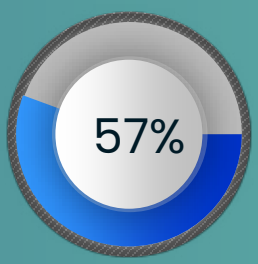
Breaches, Risk Management and the Third-Party

Organizations are going to great lengths to secure third-party ecosystems in response to growing breaches. One example is a data breach which originated at the third-party billing collections firm, American Medical Collection Agency (AMCA). The breach, which impacted 7.7 million Americans who use LabCorp, is likely to have also impacted other companies who use the third-party services of AMCA.

Furthermore, research by Risk Based Security has shown a 35% increase, over two years, in incidents where companies handled sensitive data on behalf of business partners and other clients. This data illustrates a growing picture of third-party exposure to cyber threats. However, Experian's "Seventh Annual Data Breach Preparedness Study" shows that third-party risk security awareness is not at a complete loss:

69% of respondents conduct background checks on new full-time employees and vendors.





57% of respondents reported regularly conducted third-party cybersecurity assessments in 2019.

Similarly, the Accenture "Third Annual State of Cyber Resilience 2020 " *report states: "Our latest research shows that most organizations are getting better at preventing direct cyberattacks. But in the shape-shifting world of cybersecurity, attackers have already moved on to indirect targets, such as vendors and other third parties in the supply chain."*

To improve the situation further and take TPRM into a new era, businesses must understand the challenges and how they can be overcome.

2. Key Challenges Organizations Face in Navigating Third-Party Risk Management

Each part of the third-party risk management lifecycle contains challenges. These need to be met by balancing security against convenience and usability. Security must be upheld without impacting the relationships and productivity of the third-party.

Lifecycle point	Challenges
Evaluate and perform due diligence	Risk assessment doesn't always occur. For example, companies who value convenience over security may skip evaluations which can leave security gaps.
Onboard	The definition of third-party spans of a variety of types and identity management needs to be specialized to cover all parties. Without enough diligence in onboarding, security gaps can appear if all parties are not considered: • Management • Fluid permission control without usability compromise • Wide-scope governance and visibility • Data and IT access control • Control of work apps, such as Zoom • Remote onboarding • Consistent onboarding across parties • Handle large numbers of third-party - management of IDs and access permissions • Provide general governance of a large web-like ecosystem of nth degree connections • Provide the tools to use a Zero Trust security approach (never trust, always verify applied to people, apps, and devices)
Monitor and audit	Throughout the relationship between enterprise and third-party/non-employee companies may find it challenging to continually reassess and change permissions, keep track of third-party updates that change the risk profile, and keep track of data access across third parties.
Offboard	Offboarding requires swift removal of permissions for adequate security and maintenance of trustworthy data. Without the right expertise and tools, this can prove to be a challenge for companies.

3. Managing the Full Third-Party Risk Management Lifecycle with IAM Top of Mind

Third-party ecosystems are the epitome of hybrid work environments. Building trusted ecosystems will need a unified identity backbone that can be controlled centrally and provide a mechanism for global governance. Hybrid often means dealing with heterogeneous identity systems. In a third-party ecosystem, this can result in security gaps where enterprises are unable to properly control access permissions. Third-party IDs must be in sync to meet the needs of modern TPRM. Synced and unified IAM helps to streamline data access and build trust. An enterprise can then meet the challenges of the entire TPRM lifecycle. A unified digital identity ensures a single, trustworthy identity record, for every individual third-party/non-employee.

Life Cycle of Trusted Third-Party ID

Building trust across the third-party lifecycle involves identity management in three key areas:

Pre-relationship management

Onboarding is the fundamental step in creating a unified third-party identity (TPIAM). The issues inherent in heterogeneous identity systems can be overcome by using identity unification.Due diligence, risk profiling, and verification of third parties provide trusted TPIAM to control access permissions and set privileges.

Management during relationship

Continuous monitoring of access measures to ensure that 'need to know' permissions are persistently controlled is paramount. Standardized ID and central control provide a mechanism to adjust these permissions during the monitoring stage.

Post-relationship management

Offboarding is a crucial stage at which security can fall through the gap. A survey by Osterman Research shows 89% of workers continue to have access to sensitive corporate data after they are no longer employed. This exposes the enterprise to considerable risks of insider threats, data leaks, and non-compliance to data-privacy regulations.

4. How Anomalix Can Help

Third-party ecosystems are a target for cybercriminals. However, a single authoritative identity source increases trust and visibility. A single unified identity scheme provides the basis for a trustworthy security approach. The principles of “never trust, always verify” are at the heart of third-party risk management. Relationships are built over time and using due diligence. Applying a fully synced identity system to TPRM gives an enterprise the tools to manage the entities that make up its extended third-party and non-employee ecosystem. A complex third party ecosystem needs the specialist identity services of reputable solution providers, like Anomalix, to achieve this level of control and visibility across the chain.

5. Conclusion

The modern and connected enterprise is at risk because of the nature of the extended business models needed to compete in global markets. Identity management, in the form of specialized third-party IAM (TPIAM), provides the backbone for effective third-party risk management. The flexible nature of TPIAM systems that unify third-party and non-employee identity is the key to managing access control across the ecosystem and throughout the lifecycle. The importance of using fit-for-purpose TPIAM cannot be understated. In a world where cybercriminals look for the easiest way into an organization, managing all potential entry points is a vital security strategy.

info@anomalix.com

Anomalix, Inc
405 W Superior St
STE 404
Chicago, IL 60654