ENTHEC

WHITEPAPER

Third-Party Risk

HOW TO GAIN ACCURACY IN THE ASSESSMENT

INDEX

INTRODUCTION

The digitalization of organizations has made interconnectivity of systems and reliance on third parties in business common in today’s business environment, gaining agility and efficiency. However, this interconnection also leads to greater exposure to cyber risk, forcing organizations to be more aware of the importance of third-party risk management.

Suppliers, partners, and other third parties that have access to an organization’s sensitive systems and data pose a significant risk to the organization’s cybersecurity. Cybercriminals can exploit third-party weaknesses to circumvent an organization’s cybersecurity strategy and access sensitive information, steal data, and disrupt business operations, among other things. For this reason, it is crucial for organizations to effectively and accurately assess and manage their third-party cyber risk throughout the duration of their business relationship to ensure security and business continuity in an increasingly interconnected environment.

In this whitepaper we will discuss the importance of third-party cyber risk assessment within an organization, the common methods of assessing that risk, its shortcomings, and the benefits of introducing a continuous cyber surveillance approach into third-party risk assessment as a complement and reinforcement. In addition, we will present some Use Cases to illustrate how organizations can improve their third-party risk management.

HIDDEN INFORMATION AND NTH PARTIES

Organizations often focus on securing their own network and systems, but neglect the security of the third-party systems and data they work with. Suppliers, partners, and other third parties may have access to sensitive information, making them a potential risk to the organization's security. As Gartner notes in its Third-Party Risk Assessment Model report, organizational leaders recognize that connecting their systems to third parties is a critical part of an organization's operations, and the risks continue to grow due to varying third-party cyber protection maturity, increased involvement of those third parties with corporate assets, and increasing connections of those third parties to their own third parties. This essential connection to third parties leads to two extreme difficulties when assessing risk: hidden information and scope.

HIDDEN INFORMATION

One of the main challenges in managing third-party cyber risks is the lack of transparency. Many vendors and contractors are unwilling to provide full information about their security practices, either because they do not have the resources to implement adequate security measures or because they do not want to reveal confidential details about their processes.

Furthermore, it is important to note that in many cases, third parties may also not be fully transparent about cybersecurity incidents, so as not to jeopardize the continuity of agreements or their reputation. This may include concealing security breaches, failing to update software, or failing to report these security incidents, further increasing the risk to the organization.

Organizations may also be unaware that certain vendors and contractors are outsourcing critical services to other third parties without proper notification. This can lead to a lack of control over who has access to the organization's systems and data, increasing the risk of cyberattacks.

NTH PARTIES

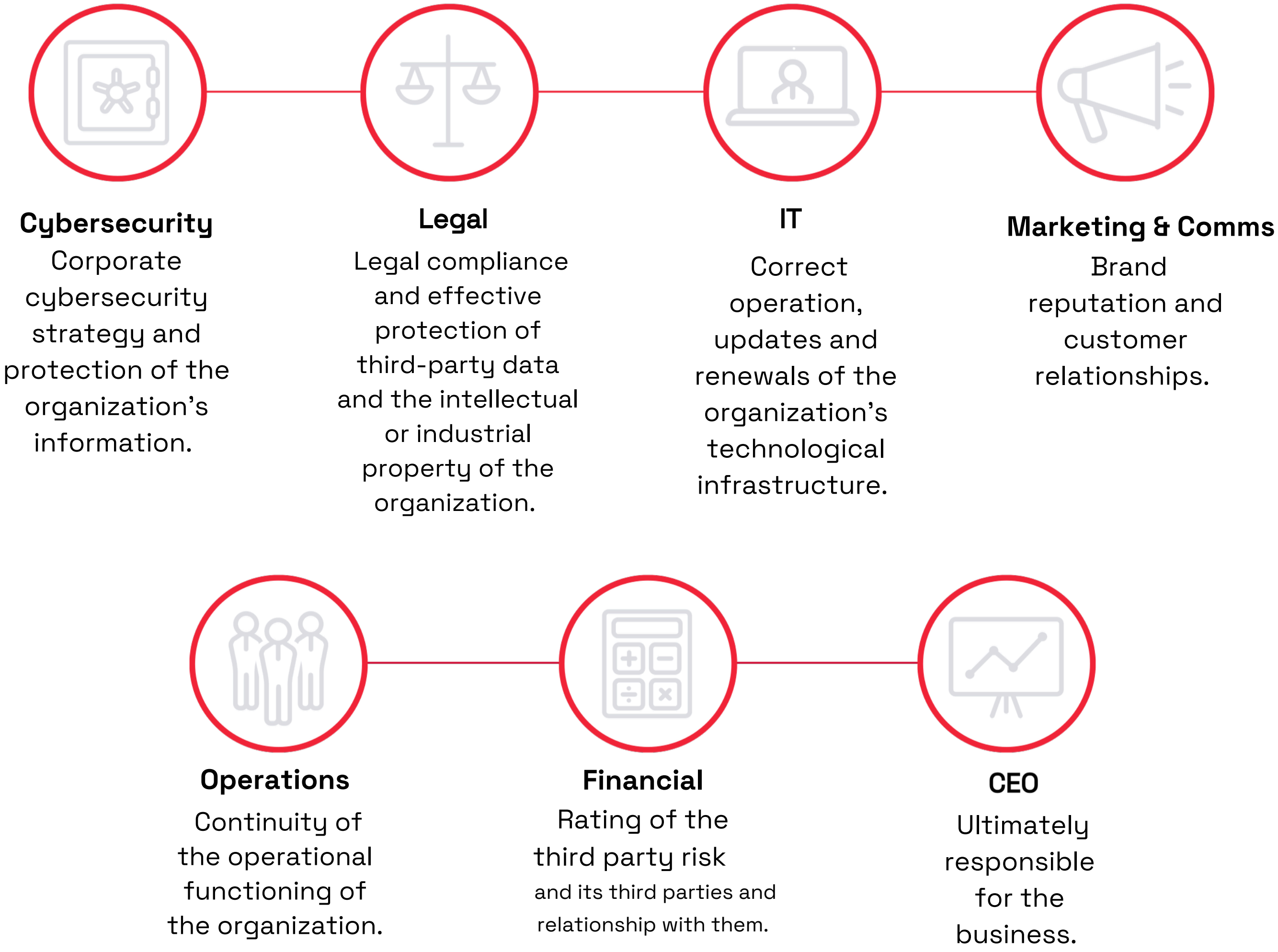
Third-party risk management often overlooks an important aspect: the risk associated with third-party third parties, also known as "nth parties."

Nth parties are the third parties of the original organization, those who have access to the systems and data of the original organization's suppliers and contractors. This complex system of dependency adds difficulty to the identification and management of third-party risks. In addition, Nth parties have their own third parties and suppliers, which further extends the supply chain and complicates the assessment of risks. The original organization has no direct control over Nth parties, which increases the risk of security vulnerabilities occurring in the supply chain. In addition, Nth parties may be less transparent than direct third parties, which complicates the assessment of associated risks.

Within the third-party risk assessment, the risk associated with the nth parts is beginning to be considered by those responsible for cybersecurity as critical for organizations due to its apparent impossibility not only of controlling it, but simply of assessing it.

THE ORGANIZATION FACING THIRD PARTY RISKS

Typically, in all organizations, third-party risks are the responsibility of the information security department and the legal department. However, both the scope of protection and the consequences of third-party risks go beyond these two departments.



Cybersecurity
Corporate cybersecurity strategy and protection of the organization's information.

Legal
Legal compliance and effective protection of third-party data and the intellectual or industrial property of the organization.

IT
Correct operation, updates and renewals of the organization's technological infrastructure.

Marketing & Comms
Brand reputation and customer relationships.

Operations
Continuity of the operational functioning of the organization.

Financial
Rating of the third party risk and its third parties and relationship with them.

CEO
Ultimately responsible for the business.

For an accurate third-party risk assessment to exist, all of these departments within an organization must manage responsibilities for protecting risks from third parties and must be involved in the assessment itself, within the parameters that involve their area, led by the CISO and the information security department.

NEED TO ACCURATELY ASSESS THIRD PARTY RISKS

An accurate third-party risk assessment is essential to protecting the security of your organization. Cyberattacks targeting suppliers, partners, contractors and other third parties can be very effective in gaining unauthorized access to your organization's systems and data. Therefore, any corporate cybersecurity strategy must consider an effective third-party risk assessment.

Assessing third-party risk involves evaluating your ability to protect your organization's systems and data. It requires examining security processes and policies, security measures in place and their actual effectiveness, regulatory compliance, and other critical factors that may impact your organization's security.

As a starting point, it is necessary to identify and classify the business risks associated with the organization's interdependence with third parties, since this interdependence implies that their vulnerabilities can have a significant impact on the organization's operations and reputation.

Assessing third-party risks as accurately as possible helps organizations prioritize risk management and take appropriate preventative measures against the shockwave of a cyberattack on a third party.

The third-party vulnerability was the fourth attack vector in 2022 data breaches in the Spanish financial and banking sector

Europa Press

73% of organizations say their third parties have more access to data assets than three years ago

Gartner

Organizations recognize dedicating only 27% of resources to identify risks of third parties in the course of the relationship

Gartner

Accurate third-party risk assessment enables organizations to:

Information

Prior to initiating a relationship with a third party, make more informed decisions about selecting suppliers and contractors. By carefully evaluating suppliers and contractors in terms of their ability to protect the organization's security, organizations can make more informed decisions about sourcing and managing their supply chain. This can help reduce the risk of cyberattacks and protect the organization's reputation.

Compression

Understand the full scope of cybersecurity risks associated with your supply chain and therefore take appropriate preventative measures to protect yourself. By carefully assessing suppliers and contractors, organizations can identify vulnerabilities and weak points in their supply chain and take steps to mitigate the risks.

Compliance

Comply with security regulations and standards. Security regulations, such as various data protection laws, require organizations to implement appropriate security measures to protect the organization's and its customers' data and systems. By carefully evaluating vendors and contractors, organizations can ensure that they comply with these regulations and standards.

Focus

Focus on vendors and contractors that pose the greatest cybersecurity risk. By prioritizing vendors and contractors based on their cybersecurity risk, organizations can focus their resources on the most critical areas and reduce the costs and time associated with risk management.

THE COMPLEXITY OF THIRD PARTY RISK ASSESSMENT

Third-party risk assessment begins before the contractual relationship is established and should continue until the collaboration ends and the interdependence is extinguished. Common assessment methods are:

Previous relationship

Due Diligence

This involves a comprehensive security assessment of suppliers and contractors that have access to the organization's systems and data, including assessing the maturity of the supplier's security program, identifying security vulnerabilities in the systems, and evaluating the supplier's ability to respond to security incidents. It is typically conducted through questionnaires developed by the organization itself.

During relationship

Audits and Offensive Security

It involves the review of security audit reports and risk assessments carried out by the provider, as well as the performance and verification of the results of Offensive Security tests (pent testing, Red Team, etc.) carried out by the third party.

DEFICITS

- Manual and non-objective methods based on questionnaires and tests.
- Mandatory authorization for carrying out intrusive tests.
- High costs of carrying out tests (pentests and similar).
- Impossibility of verifying the accuracy of the information provided and the absence of hidden information.
- Risk assessment at a given point in time, without continuous monitoring of the risk throughout the relationship, including changes in the relationship.
- Information becomes outdated in just a few days. Risk cannot be assessed to the nth degree.

Added to these problems is another one that is a major problem and represents a critical risk: the limitation of the assessment of third-party risk to the internal perimeter of your company. The protection of the external attack surface is an increasingly bigger problem in companies, since until now it has been impossible to control the risk level of the extended IT perimeter that includes suppliers, clients, partners and other third parties. It has been proven that these are a widely used attack vector and, therefore, any vulnerability that exists in your cybersecurity system can automatically become an entry point for the companies with which you interact.

This complexity generally means that traditional assessment of third-party risk is inaccurate and unreliable and therefore not useful for designing an effective protection strategy against third-party risks.

CYBERSURVEILLANCE APPROACH: CONTROL BEYOND THE INTERNAL PERIMETER

One of the main reasons why successful cyberattacks on companies continue to occur is that cybercriminals use leaked information exposed on the Internet, the Deep Web and the Dark Web to bypass the defense systems in which companies invest huge amounts of resources. Information leaks are a key that unlocks any defense.

This reality is what has given rise to the birth of a new approach within the cybersecurity strategy of organizations: cyber surveillance for Continuous Threat Exposure Management (CTEM)

Cyber surveillance is a cybersecurity strategy based on continuous and automated monitoring and analysis of the Web, Deep Web and Dark Web to detect in real time the organization's exposure to ongoing threats and detect exposed vulnerabilities. In this way, an organization can know in real time what corporate information is available to any cybercriminal in order to control and neutralize their attack capacity.

A defense is effective only when all threats, own and third-party generated, are accurately known and when internal and external vulnerabilities are controlled.

CTEM CYBERSURVEILLANCE FOR THIRD PARTY RISK ASSESSMENT

One of the main capabilities of CTEM cyber surveillance is that it can be used as a Security Rating Services (SRS) tool: the independent assessment of own and third-party risks for a broad view of the cybersecurity maturity of any organization using an external approach.

The tool collects data from the Web, Deep Web and Dark Web through non-intrusive means, analyses it and assesses the third party's security posture using a specific scoring methodology. This information provided by continuous and automated cyber surveillance serves to expand, complete and weigh the information obtained by traditional third-party risk assessment methods, such as Due Diligence or Offensive Security, also allowing for continuous and real-time assessment of said risks for the duration of the collaboration between the organization and the third party.

ADVANTAGES OF CTEM MONITORING IN THIRD PARTY RISK ASSESSMENT

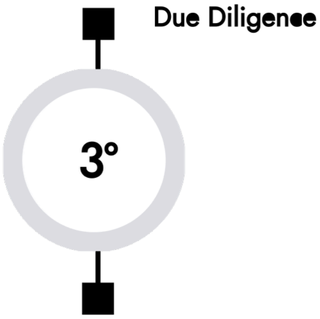
- Objective valuation method that does not require human intervention.
- Non-intrusive method that does not require third party authorization.
- Accurate data on the leak and exposure of third-party information, as well as the security breaches that caused the leak.
- Continuous and real-time monitoring and analysis of third-party risk throughout the duration of the business relationship.
- Control of hidden information.
- Ability to assess risks to the nth degree.

APPLICATIONS

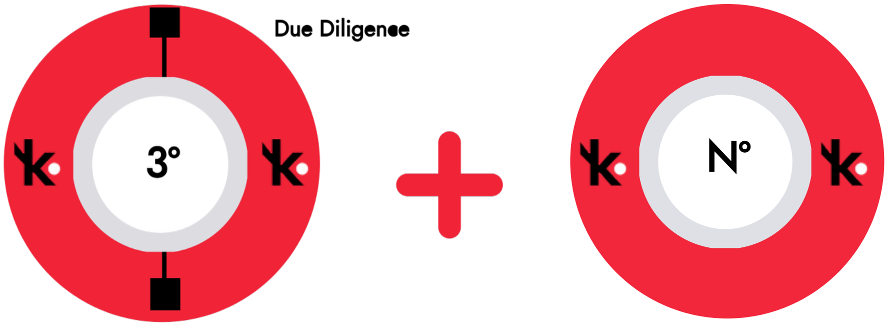
The Continuous Threat Risk Management approach can be used to assess third-party and nth-party risks both in a one-off transaction (acquisitions, mergers, cyber policies, etc.) and in a long-term business relationship, providing the precision and reliability that is lacking in the most common assessment methods.

SPOTLIGHT ASSESSMENT OF THIRD PARTY RISK

WITHOUT
KARTOS THIRD PARTIES



WITH
KARTOS THIRD PARTIES



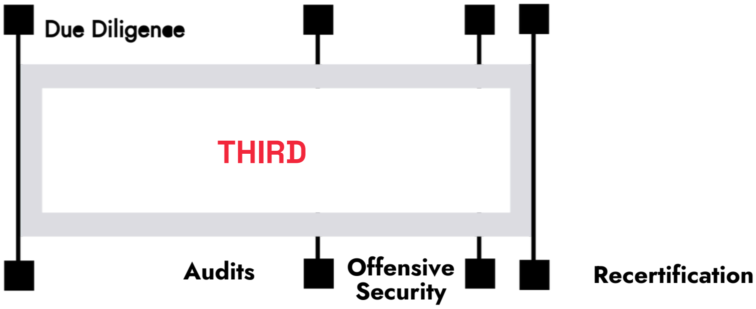
USE CASE

Covering the risk of a Cyber Policy represents a critical decision for Insurance Companies. Thanks to the continuous and automated cyber surveillance approach in assessing third-party risk, an Insurance Company obtains a more accurate and rigorous assessment of the risk of each Cyber Policy and the maturity of the potential client's cybersecurity strategy, while being able to increase its overall offering to its policyholders with the Corporate Cyber Risk Analysis Service.

APPLICATIONS

CONTINUOUS ASSESSMENT OF THIRD PARTY RISK

WHITOUT
KARTOS THIRD PARTIES



Due Diligence

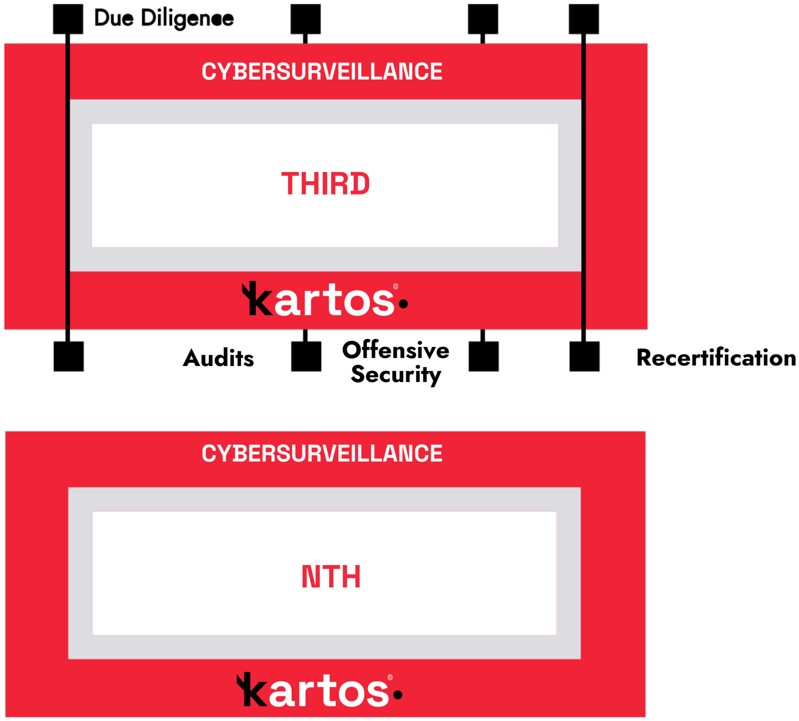
THIRD

Audits

Offensive Security

Recertification

WITH
KARTOS THIRD PARTIES



Due Diligence

CYBERSURVEILLANCE

THIRD

kartos

Audits

Offensive Security

Recertification

CYBERSURVEILLANCE

NTH

kartos

USE CASE

Financial and banking data are considered sensitive information and any leak of such data, apart from being a threat, carries heavy financial penalties. Thanks to the continuous and automated cyber surveillance approach to assessing third-party risk, a Bank continuously and in real time monitors the risk of its third parties and others to control their protection against information leaks.

APPLICATIONS

THIRD PARTY RISK ASSESSMENT AND MANAGEMENT STRATEGIES WITH A CTEM CYBERSURVEILLANCE APPROACH:

Preview

Evaluation of potential third and nth parties

- Due Diligence.
- Automated monitoring of the mastery of the potential third party during the evaluation time.
- Automated monitoring of the domains of critical nth potentials during the evaluation time.
- Evaluation of information obtained:
  - Ability to affect the organization.
  - Estimated remediation time of the risk.

Continues

Third and nth party evaluation

- Audits.
- Offensive Security Testing.
- Continuous Monitoring and automated from third-party domains.
- Continuous monitoring and automated domain of critical nths.
- Evaluation of information obtained:
  - Ability to affect the organization.
  - Risk remediation time.
  - Communication to the third party when the exposure of information detected through Cyber Surveillance affects the organization.

APPLICATIONS

By adding a Cyber Surveillance strategy for Continuous Threat Exposure Management (CTEM) to the third-party risk assessment, the organization gains the ability to automatically, continuously and in real-time monitor the exposed information of a third party or potential third party and the detection of their security breaches, as well as the umpteenth critical ones associated with them.

1. More accurate assessment of the risk of potential third parties and evaluation of the maturity of your Cybersecurity strategy.
2. More effective management of third-party and third-party risk throughout the contractual relationship and continuous evaluation of your Cybersecurity strategy.
3. Automated, real-time detection of third-party and third-party security breaches and assessment of the threat level of risk to the organization.
4. Notifying third parties of security breaches affecting the organization and monitoring their remediation.
5. Communication to third parties of the risk of nths associated with their organizations and monitoring of their remediation.

ENTHEC

WHITEPAPER

kartos©

Kartos Corporate Threat Watchbots: Continuous Threat Exposure Management (CTEM)

Automated, continuous, real-time monitoring of the organization's threat exposure, focused on cybersecurity and business criteria.

EXTERNAL ATTACK SURFACE

Location of the Company's open and exposed information and vulnerabilities on the Internet, the Deep Web, Dark Web and Social Networks: Phishing, fraud and scam campaigns; CVEs; DNS health; leaked passwords and credentials; leaked and exposed documentation and databases.

DIGITAL RISK PROTECTION

Detection of contextual information about potential attackers, their tactics and processes for carrying out malicious activities. Elimination of malicious activities on behalf of the Company. Brand, domain and subdomain protection. Corporate email protection. Ransomware protection. Web security and threat removal.

THIRD PARTY RISK

Real-time monitoring of third-party risk. Objective data on ongoing threats related to the value chain. Comprehensive view of any organization's cybersecurity maturity using a non-intrusive, external approach. Extension and weighting of information provided by traditional third-party risk assessment methods.

COMPLIANCE

Monitoring of corporate and third-party legal compliance based on objective data taken in real time.
ISO 27001. PCI - DSS. ENS. RGPD.
Justification of compliance with legal and regulatory requirements for associations, mergers and acquisitions, audits, certifications and contracts with the administration

CYBERSECURITY SCORING

Enables security information to leave the CISO's office and be easily presented to people who need to be involved in security management without technical training. Own and third-party cybersecurity scoring for partnerships, audits, mergers, acquisitions, and government contracts.

Analysis of 9 threat categories

- **Network**
- **DNS Health / Phishing**
- **Patch Management**
- **IP Reputation**
- **Web Security**
- **Email Security**
- **Document Filtering**
- **Credential Filtering**
- **Social Networks**

kartos©

AI layer that enables 100% automated operation without human intervention anywhere of the process.

Strictly non-intrusive tool.
The research is carried out on the Internet, the Deep Web and the DarkWeb and the IT perimeter of the organizations is not attacked, so its operation and the information obtained strictly comply with the imposed limits.
by legislation.

The only platform that analyzes **conversations on social networks from the threat and attack detection perspective,** beyond the relating to reputation and branding.

Continuous operation 365x24x7, allowing detection of leaks of new information practically in real time.
real time.

Maximum ease of use. Does not require no complex configuration. Simply enter the domain into the platform and it works autonomously, without the need to configure search parameters or any other information location criteria.

Automated, objective and continuous monitoring of the risks caused by third parties belonging to the External Attack Surface of the organization.

Learn more about our licenses.
Try our tool for free.
Start using Kartos and control your Third-Party Risk.

→ hello@enthec.com

Enthec Solutions is a Spanish technology company that develops cybersecurity software for the protection of organizations and people. Enthec Solutions has established itself as one of the Deep Tech companies with the most innovative and effective Cyber surveillance solutions thanks to the success of its **Kartos Corporate Threat Watchbots** platform, which provides organizations with Cyber Security, Cyber Intelligence, Cyberscoring, Compliance and Third-Party Risk Management Capabilities, and its innovative **Qondar Personal Threat Watchbots** platform for the individual online protection of the organization's relevant people.

www.enthec.com