Genesis

Third Party Risk Management Guide for Managers 2024

whitepaper

Introduction

Success in today's business world relies on strong third-party partnerships. As businesses adapt to new strategies, changing regulations, and evolving business models, established companies increasingly depend on a variety of vendors and subcontractors. This teamwork ensures smoother operations and helps businesses quickly respond to market changes.

Organizations often rely on a hundred or more third parties to handle various tasks, making the dependency and ecosystem far more complex than what's visible through standard attack surface management or traditional security monitoring tools.

Third-Party

A third party in a business context refers to any external entity or service that is neither owned nor fully controlled by the primary organization but is involved in its operational processes or value chain. This includes IT vendors, cloud providers, financial tools, legal consultants, suppliers, and more. Essentially, it's any external organization or service that the primary organization relies on to meet its objectives, but over which it doesn't exert direct management or complete control.

Third-party Risk management

Third-Party Risk Management (TPRM) plays a pivotal role in this dynamic. TPRM is the systematic process where organizations identify, assess, and mitigate risks arising from these external associations. The approach to TPRM is tailored based on each company's size, sector, and specific operational needs. As partnerships become more complex, a robust TPRM framework becomes crucial to maintain security, operational integrity, and overall business success.

Why Third-Party Risk Management is Crucial?

Recent research from the Cyentia Institute underscores a glaring concern: 98% of global organizations are connected to at least one third-party vendor that suffered a security breach within the last two years. Since 2020, with the unprecedented shift to remote work, the reliance on third parties has significantly increased to support daily operations. For a Chief Information Security Officer (CISO), this trend is particularly alarming. Unlike direct organizational threats, third-party risks often exist outside the organization's primary security perimeter. This external positioning makes it a challenging blind spot for CISOs, making it harder to track and address the associated vulnerabilities. In essence, without a robust Third-Party Risk Management (TPRM) framework, CISOs are leaving a critical aspect of their organization's security unchecked, potentially exposing them to detrimental breaches and cyber threats

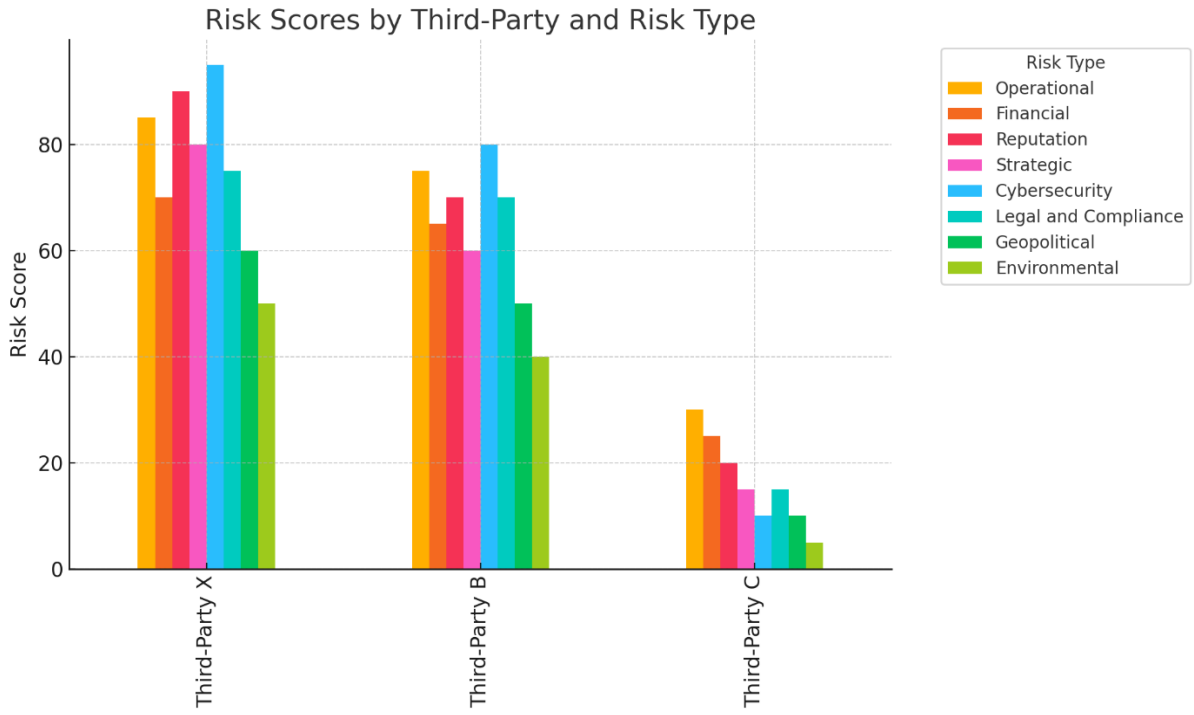
Risk Assessment

Every organization deals with a variety of third parties, and not all of them pose an equal risk. The nature and degree of risk often depend on the type of data or services that these third parties handle or provide. Understanding this dynamic is pivotal for effective risk management. To put it practically:

Third-Party X: This entity manages your cloud data, which could contain sensitive and confidential information. The potential breach or mishandling of this data can have severe implications, placing this third party in a high-risk category.

Third-Party B: This entity handles your marketing data. While some marketing data can be sensitive, others might be public or less critical. The risk associated with this third party might be moderate, depending on the exact nature of the data they hold.

Third-Party C: This is a cleaning service company. Their interaction with your sensitive data or core operations is minimal, if at all. As such, the risk they pose is relatively low in terms of data security.



These external partnerships, while bringing a host of advantages like specialized expertise and cost-efficiency, also introduce varied threats to an organization. Therefore, a structured categorization of these risks associated with third parties becomes essential. By systematically breaking down and examining each type of risk, organizations can implement more effective controls, ensuring smoother operations and safeguarding their interests.

1. **Operational Risks:** Disruptions that can affect daily operations, such as service outages or delays.

2. **Financial Risks**: Potential losses from third-party financial failures, fraud, or contractual disputes.

3. **Reputation Risks:** Damage to the company's brand or public image due to third-party actions or failures.

4. **Strategic Risks**: Issues arising from third parties not aligning with the company's long-term strategic goals.

5. **Cybersecurity Risks:** Threats related to data breaches, malware incidents, or other cyberattacks stemming from third parties.

6. **Legal and Compliance Risks:** Legal repercussions from third-party actions or omissions, including non-compliance with laws and regulations.

7. **Geopolitical Risks**: Challenges related to third parties operating in politically unstable regions.

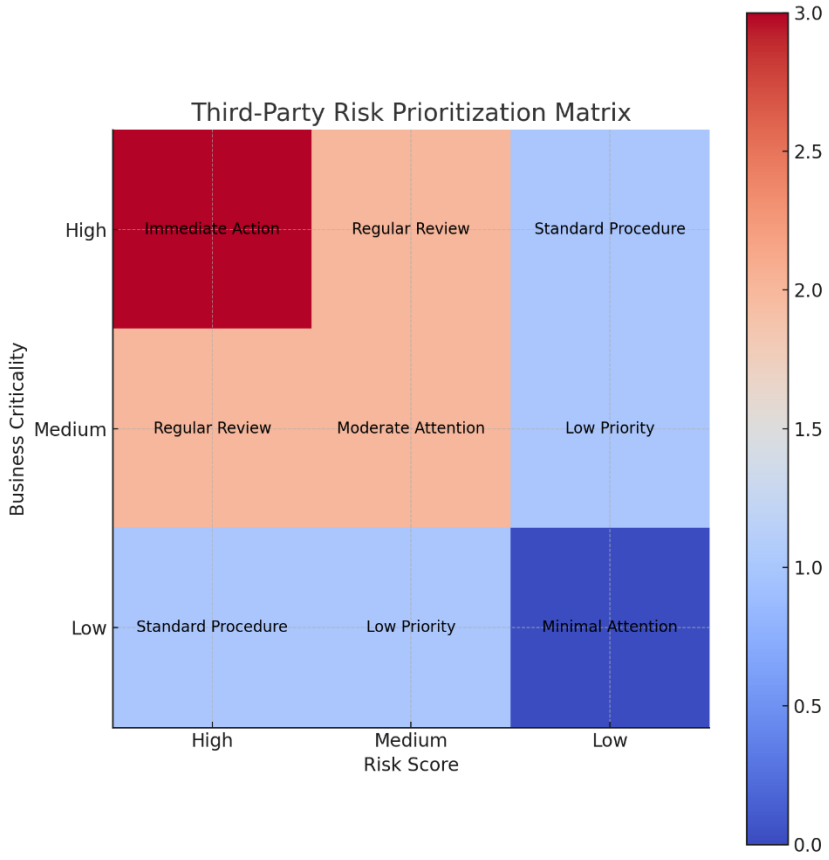
8. **Environmental Risks:** Concerns about a third party's environmental footprint, which could impact the company's sustainability goals.

Identifying and categorizing these risks is the foundational step in effective third-party risk management. By breaking down the potential threats into distinct categories, organizations can develop a clearer, more organized perspective on their risk landscape. This structured approach not only streamlines the assessment and mitigation process but also aids in strategic decision-making. With a well-defined categorization in place, organizations can better allocate resources, prioritize mitigation efforts, and create tailored response strategies.

This clarity ensures that the most significant and potentially damaging risks are addressed promptly, safeguarding the organization's assets, reputation, and operational integrity. In essence, a categorized risk framework serves as a roadmap, guiding organizations in navigating the complex web of third-party interactions and their associated challenges.

Third-party Risk Prioritization

When it comes to managing third-party risks, organizations often utilize both quantitative and qualitative methodologies to score vendor risks effectively. Quantitative methods involve assigning numerical values to different risk factors based on data such as breach history, financial stability, and compliance track records



These scores can then be aggregated to form a composite risk score, providing a clear, objective measure of risk. On the other hand, qualitative methods rely on subjective assessments typically derived from expert opinions, industry knowledge, and past experiences with vendors. These assessments might categorize risks into levels such as low, medium, or high based on perceived risk factors and impact scenarios.

To prioritize vendors effectively, organizations can use a prioritization framework that considers both the risk score and the business criticality of each vendor. This approach involves mapping vendors on a matrix where one axis represents the risk score and the other represents their criticality to business operations. Vendors that fall into the high-risk and high-criticality quadrant are prioritized for immediate action, such as enhanced monitoring, more stringent controls, or even reconsideration of the vendor relationship. This structured approach helps organizations allocate their risk management resources efficiently, focusing efforts where they are needed most to mitigate potential disruptions and safeguard business interests.

Quantitative Risk Scoring

The organization might score these vendors based on specific data points:

- Cloud Service Provider: Assigned a risk score of 85 out of 100 due to its access to sensitive data, previous minor security breaches, and its critical role in data storage
- Payment Processing Company: Scored 75 out of 100, reflecting its access to financial data, excellent compliance record with PCI DSS, but moderate susceptibility to financial fraud risks.
- Office Supplies Distributor: Receives a lower score of 30 out of 100, as it involves minimal operational risk and does not handle sensitive company data.

Qualitative Risk Assessment

Next, the organization evaluates these vendors qualitatively:

- Cloud Service Provider: Considered high risk because any service disruption could directly impact the organization's operations and data security.
- Payment Processing Company: Assigned a medium risk due to its robust security measures but still requires attention due to the potential impact of financial data compromise.
- Office Supplies Distributor: Deemed low risk as issues with this vendor would cause minor inconvenience rather than significant operational disruptions.

Prioritization Framework

Using a risk matrix, the organization places each vendor at an intersection of risk score (quantitative) and criticality (qualitative):

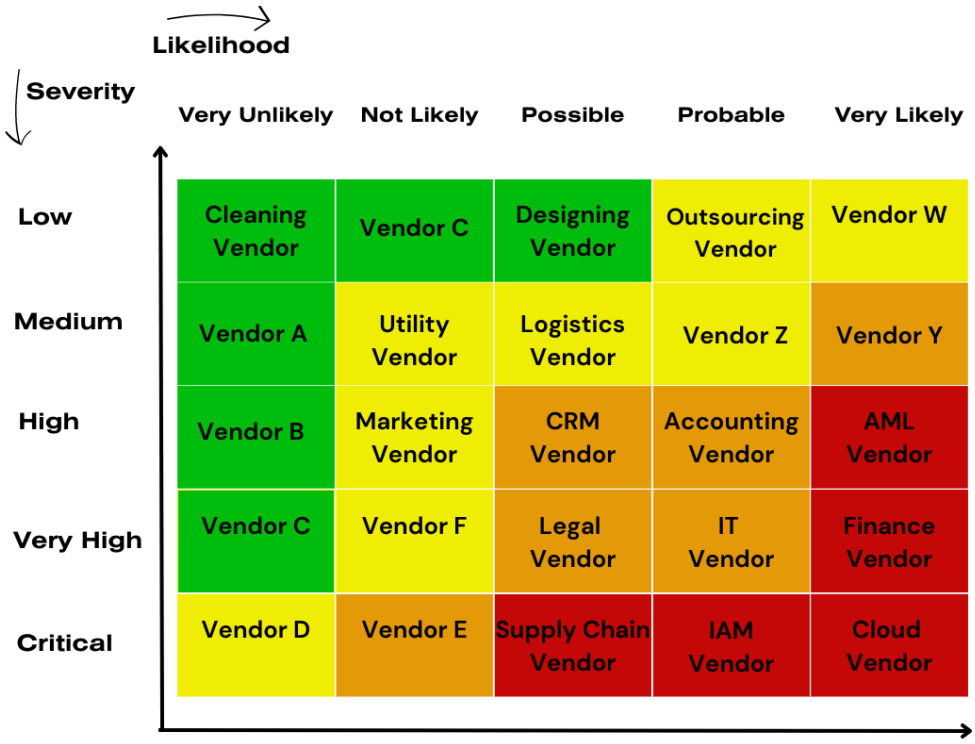
- Cloud Service Provider: Falls in the high-risk, high-criticality quadrant. This vendor is critical to operations and presents a significant risk, requiring immediate and ongoing risk management efforts, such as frequent security audits and strong contractual safeguards.
- Payment Processing Company: Placed in the medium-risk, medium-criticality quadrant. It necessitates regular reviews and moderate risk mitigation measures, including compliance checks and contingency planning.
- Office Supplies Distributor: Positioned in the low-risk, low-criticality quadrant, warranting standard procurement procedures without the need for intensive oversight

Implementation

- For the Cloud Service Provider, the organization might decide to implement more stringent security protocols, increase the frequency of third-party audits, or even consider a backup provider to reduce dependency.
- For the Payment Processing Company, they might focus on enhancing transaction monitoring and regularly reviewing compliance with financial security standards.
- The Office Supplies Distributor may only require annual performance reviews and basic contractual terms regarding delivery and quality standards.

Risk Classification

Risk Classification can make the job easier to differentiate between the criticality of your vendors, but it can become a little complex and the risk decision can be in the dark. There are some methods which can be followed to classify the risks of the third parties:



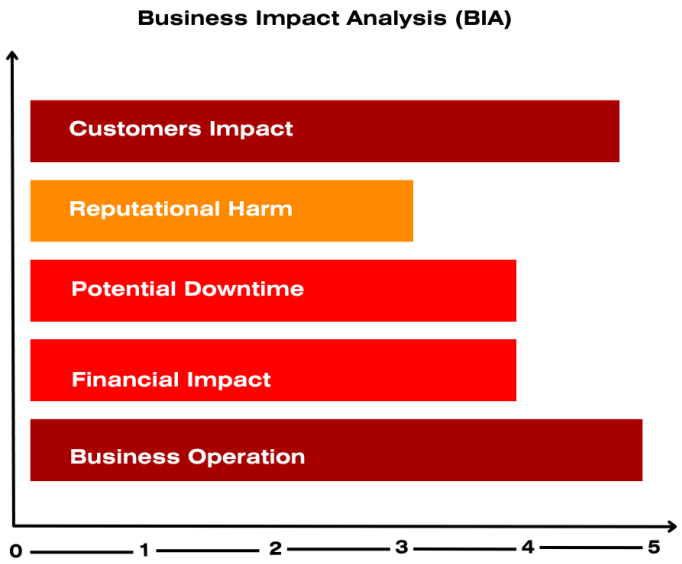
Genesis Risk Heatmap

1. **Business Impact Analysis (BIA):**

   Process: Determine which third parties, if compromised, would have the most significant impact on your business.

   Factors to Consider: Business operations affected, financial impact, potential downtime, reputational harm, and customer impact.

   Implementation: Use a BIA tool or software to streamline the assessment. Rank third parties from highest to lowest impact.



2. **Data Sensitivity Classification:**

   Process: Classify third parties based on the sensitivity of data they handle.

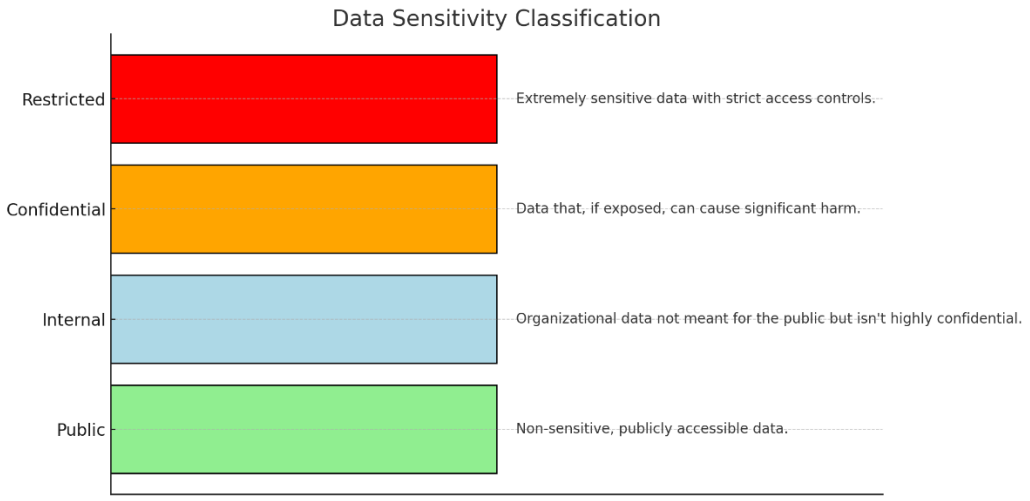
   Categories:

   Public: Non-sensitive, publicly accessible data.

   Internal: Organizational data not meant for the public but isn't highly confidential.

   - Confidential: Data that, if exposed, can cause significant harm.
   - Restricted: Extremely sensitive data with strict access controls.

   Implementation: Conduct a data inventory and map third parties to data types they handle.



3. **Relationship Duration:**

   Process: Identify risks based on how long you'll be engaged with the third party.

   Factors: Short-term versus long-term engagement risks. A long-term vendor with poor security can be a more significant risk over time.

   Implementation: Use contract length as a guide. Regularly review long-term third-party relationships for evolving risks.

3. **Service Criticality:**

   Process: Rank third parties based on how critical their services are to your operations.

   Factors: Essential services vs. non-essential services.

   Implementation: List all third parties and tag them based on whether their failure would halt, slow, or have a minor impact on business operations.

4. **Regulatory Environment:**

   Process: Classify risks based on regulatory compliance requirements associated with third parties.

   Factors: GDPR, HIPAA, CCPA, etc.

   Implementation: Tag third parties based on the regulations they fall under. Monitor them for compliance regularly.

5. **Technological Complexity:**

   Process: Evaluate third parties based on the complexity of the technology they use and provide.

   Factors: Modern, regularly updated systems vs. outdated, potentially vulnerable systems.

   Implementation: Technical audits or assessments can provide insights. Rank vendors based on their tech stack's security and complexity.

6. **Historical Performance:**

   Process: Consider the track record of the third party.

   Factors: Past breaches, security incidents, and responsiveness to incidents.

   Implementation: Maintain an incident log for each third party. Regularly review their historical performance.

Evaluating third-party risk is not a one-size-fits-all process; it should be carefully tailored to fit the unique ecosystem of each business. By investing time in closely observing and fully understanding the subtle details of the current business landscape, organizations position themselves to make more informed decisions.

Third-Party Risk Management (TPRM) Lifecycle

The Third-Party Risk Management (TPRM) lifecycle is a comprehensive framework designed to manage and mitigate risks associated with outsourcing business functions or services to external vendors.

1. Identification and Selection of Third Parties:

Identify potential third parties based on specific business needs and requirements. Develop and issue RFPs to invite proposals and establish security standards that third parties must meet.

- **Stakeholders**: Procurement Team, Legal Team, Information Security Team, Business Units
- **Documents:** Request for Proposal (RFP), Third Party Security Standards
- **Industry Standards:** Use of standardized RFP templates, adherence to industry-specific compliance requirements
- **Actions:**
    - Define business needs and requirements.
    - Develop and issue RFPs.
    - Establish security standards for third parties.
    - Evaluate and shortlist potential third parties based on responses to RFPs.

2. Pre-Assessment Questionnaires:

Use standardized questionnaires, such as the Standardized Information Gathering (SIG) Questionnaire, to collect initial data on the third parties' security postures.

- Stakeholders: Information Security Team, Procurement Team
- Documents: Security Questionnaire
- Industry Standards: Standardized Information Gathering (SIG) Questionnaire, Vendor Security Alliance (VSA) Questionnaire
- Actions:
    - Design detailed security questionnaires based on industry standards like SIG.
    - Send questionnaires to potential third parties.
    - Analyze responses and flag potential risks.

3. Risk Assessment:

Conduct thorough security assessments of potential third parties, evaluating their security controls and compliance with frameworks like NIST or ISO. Document the findings in a Risk Assessment Report.

- Stakeholders: Information Security Team, Risk Management Team, Compliance Team
- Documents: Risk Assessment Report
- Industry Standards: NIST SP 800-53, ISO 27001

- Actions:
    - Conduct in-depth security assessments of potential third parties.
    - Evaluate third-party security controls and compliance using frameworks like NIST or ISO.
    - Generate Risk Assessment Reports based on findings.

4. Contract Negotiation and Onboarding:

Negotiate contract terms, focusing on security clauses and the Data Protection Agreement (DPA). Once an agreement is reached, onboard the third parties into the organization's systems.

- Stakeholders: Legal Team, Procurement Team, Information Security Team, Compliance Team.
- Documents: Contract, Data Protection Agreement (DPA).
- Industry Standards: GDPR for data protection clauses, Right to Audit clauses.
- Actions:
    - Negotiate contract terms with selected third parties.
    - Include security clauses and DPAs in contracts.
    - Onboard third parties into the organization's systems.

5. Continuous Monitoring and Management:

Establish a program to continuously monitor third parties' security postures. Regularly conduct security assessments, audits, and reviews, and maintain an Incident Response Plan.

- Stakeholders: Information Security Team, Compliance Team, Internal Audit
- Documents: Audit Reports, Incident Response Plan
- Industry Standards: Continuous Security Monitoring (CSM) solutions, SOC 2 Reports
- Actions:
    - Establish a continuous monitoring program using CSM solutions.
    - Conduct regular security assessments, audits, and reviews.
    - Develop and maintain an Incident Response Plan

6. Ongoing Communication and Training:

Maintain open and regular communication with third parties regarding security expectations. Provide necessary training to ensure they understand and can meet security requirements.

- Stakeholders: Information Security Team, Third Parties, Training Team.
- Documents: Training Materials, Communication Plans.
- Actions:
    - Maintain regular communication with third parties.
    - Provide training to third parties on security requirements.
    - Update third parties on changes to security policies

7. Performance Review and Reporting:

Evaluate the third parties' performance and compliance regularly. Generate Performance Review Reports and present findings to senior management.

- Stakeholders: Information Security Team, Senior Management, Risk Management Team.
- Documents: Performance Review Report.
- Actions:
    - Regularly review third parties' performance and compliance.
    - Generate Performance Review Reports.
    - Report findings to senior management.

8. Termination and Offboarding:

When ending a relationship with a third party, issue a Termination Notice, and ensure all sensitive data is returned or destroyed, as verified by a Data Destruction Certificate.

- Stakeholders: Legal Team, Information Security Team, Procurement Team
- Documents: Termination Notice, Data Destruction Certificate
- Actions:
    - Issue Termination Notice to end the relationship with a third party.
    - Ensure sensitive data is returned or destroyed, as verified by a Data Destruction Certificate
    - Revoke third party's access to the organization's systems

9. Post-Engagement Review:

After termination, conduct a review to identify lessons learned and areas for improvement. Document these findings in a Post-Engagement Review Report to refine future third-party engagements.

- Stakeholders: Information Security Team, Risk Management Team, Senior Management
- Documents: Post-Engagement Review Report
- Actions:
    - Conduct a review to identify lessons learned and areas for improvement.
    - Document findings in a Post-Engagement Review Report
    - Use findings to refine future third-party engagements.

About the Author

Syed Amoz brings Six years of experience in cybersecurity with a specialized focus on Cyber Risk Quantification (CRQ) and Third-Party Risk Management (TPRM). Amoz has also authored two e-books that serve as practical guides for cybersecurity. Currently, Amoz is dedicating his efforts to a promising Genesis framework that aims to standardize CRQ and TPRM, addressing a critical gap in today's risk assessment landscape.

What do you do when you don't do Security?

Away from his professional life, Syed finds balance through a range of interests. He's a swimming enthusiast who also enjoys the fast-paced world of Formula One. And for a different kind of strategy and speed, he likes playing Counterstrike sometimes.