Key Organizational Factors to Consider

1. **Supply-Chain Stakeholder Integration & Relationships**
    - The organization needs to map out *all* relevant actors: internal teams, suppliers, third-party vendors, distributors, etc.
    - These stakeholders have different roles, access, and potential vulnerabilities.
    - Understanding who the "actors" are is critical because supply chains are highly interdependent.
2. **Organizational Goals vs. Security Goals**
    - Define *organizational goals* (e.g., business growth, product delivery) and *security goals* (e.g., confidentiality, integrity, availability).
    - Threat modelling should align with both sets of goals so that security efforts support business objectives.
    - This alignment helps prioritize which threats are most critical to the organization's mission.
3. **Threat Intelligence Capabilities**
    - The organization must be able to gather, share, and analyse intelligence on potential threat actors, their Tactics, Techniques, and Procedures (TTPs), and their motivations.
    - Without good threat intelligence, threat modelling can miss realistic or emerging attack patterns.
4. **Vulnerability and Risk Management Practices**
    - Identify vulnerabilities not just within the organization, but also in the supply chain (including third parties).
    - Consider risk categories: technical/IT risk, non-IT risk (e.g., organizational or environmental), and cascading risk (how an attack in one supply chain partner could affect others).
    - Continuous risk assessment is needed because supply chains evolve and new threats emerge.
5. **Audit and Assurance Mechanisms**
    - The paper highlights "lack of third-party audit mechanisms" as a big challenge.
    - Organizations should have formal audit processes (internal or external) to ensure suppliers adhere to security standards.
6. **Cascading Threat Effects**
    - Because supply chains are interconnected, a compromise in one node can propagate ("cascading effects").
    - The threat model must account for *inbound* (e.g., supplier to organization) and *outbound* (organization to customer/distributor) chain threats.
    - Modelling should include conditional probabilities of compromise, propagation, and impact. In the paper, they used a discrete probability method for this.
7. **Organizational Process & Governance Structure**
    - How decisions are made around security: who leads threat modelling, who defines controls, who is responsible for third-party risk, etc.
    - Roles and responsibilities: defining "actors" properly (not just threat actors, but internal actors in the supply chain system).

- The organization's maturity level in terms of risk management, security policy, and resource allocation.

8. **Controls and Security Measures**
    - Based on modeled threats, define controls to mitigate them — e.g., technical controls, policy controls, procedural controls.
    - In the paper, they recommend building a *strategic team* that can identify, evaluate, and oversee these controls.
    - Use of standards and frameworks might help (they used STIX for threat intelligence modeling).
9. **Incident Reporting & Threat Reporting Mechanisms**
    - There needs to be a way for stakeholders (especially third parties) to report security incidents or suspicious behavior.
    - Threat reporting should be structured so that intelligence about attacks or near-misses can feed back into the threat model.
10. **Organizational Culture and Training**
    - The human factor matters insiders (employees, contractors) could be threat actors, so understanding insider risk is important.
    - Security awareness and training across all supply chain partners will influence how likely certain threat vectors are (e.g., phishing, misconfigurations).