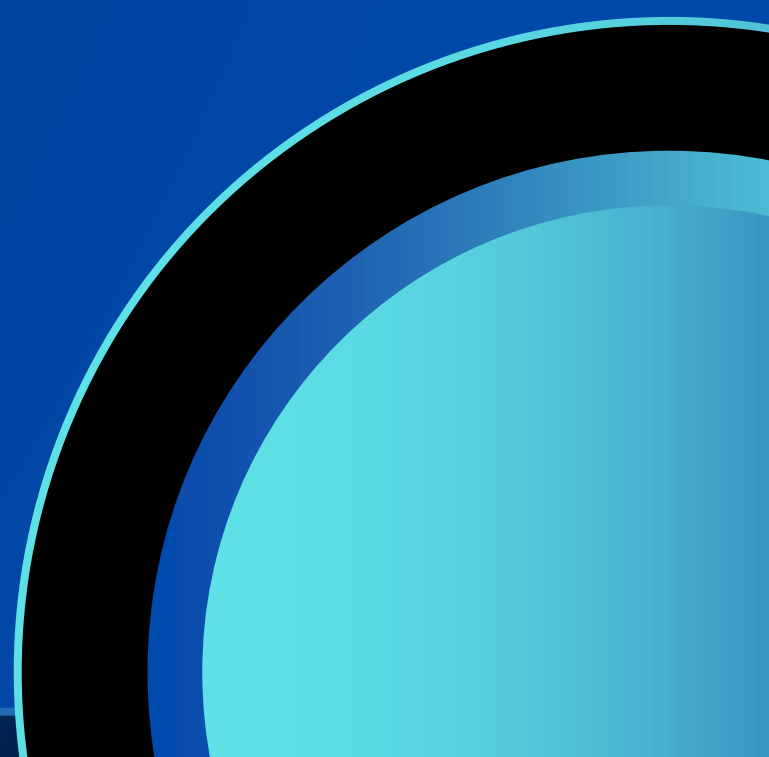




Cybersecurity Risks in Digital Supply Chains and Their Organizational Impacts



Background

Digital supply chain transformation has created new operational methods which organizations use to manage their production schedules and their logistics operations and their supplier partnerships. Supply chains now function as complex digital systems which use connected platforms and common data systems and cloud networks and analytics-based decision systems. The technological innovations have delivered operational improvements which enhanced visibility and coordination and efficiency throughout the worldwide supply chain networks.

The digital connections that support business operations also create critical security risks which make them easier to exploit by cybercriminals. Cybercriminals use attacks against suppliers and logistics systems and shared enterprise platforms to create operational disruptions which lead to financial damage that affects multiple organizations.



WHY CYBER SECURITY MATTERS

Problem Statement

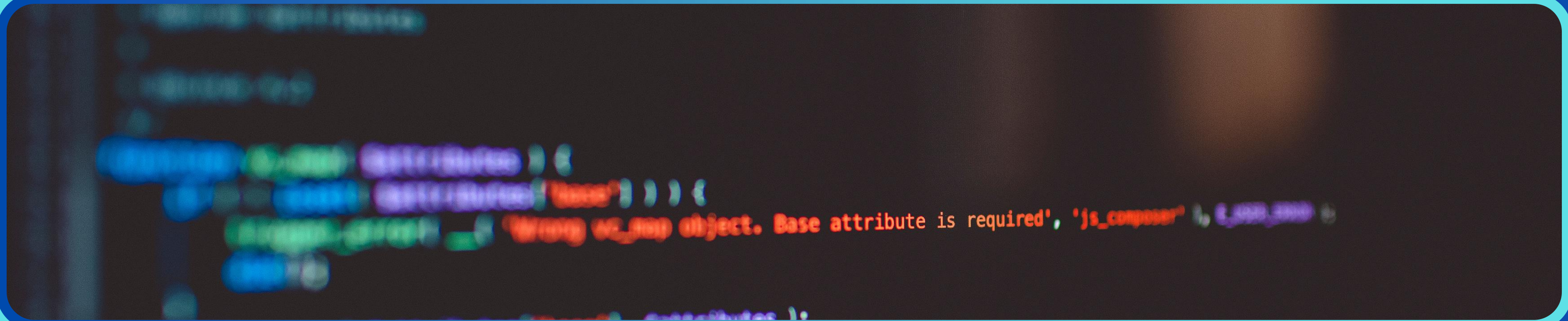
The research shows how cybersecurity affects supply chain resilience together with digital interdependence while creating value for both academic research and business management. Understanding how organizations build cyber resilience through their digital supply chains has become essential for modern business operations because digital ecosystems are constantly changing.

```
class js_composer extends Base {  
  constructor() {  
    super('base');  
  }  
  static get __() {  
    return 'Wrong vs_map object. Base attribute is required', 'js_composer';  
  }  
}
```

WHY CYBER SECURITY MATTERS

Research Aim

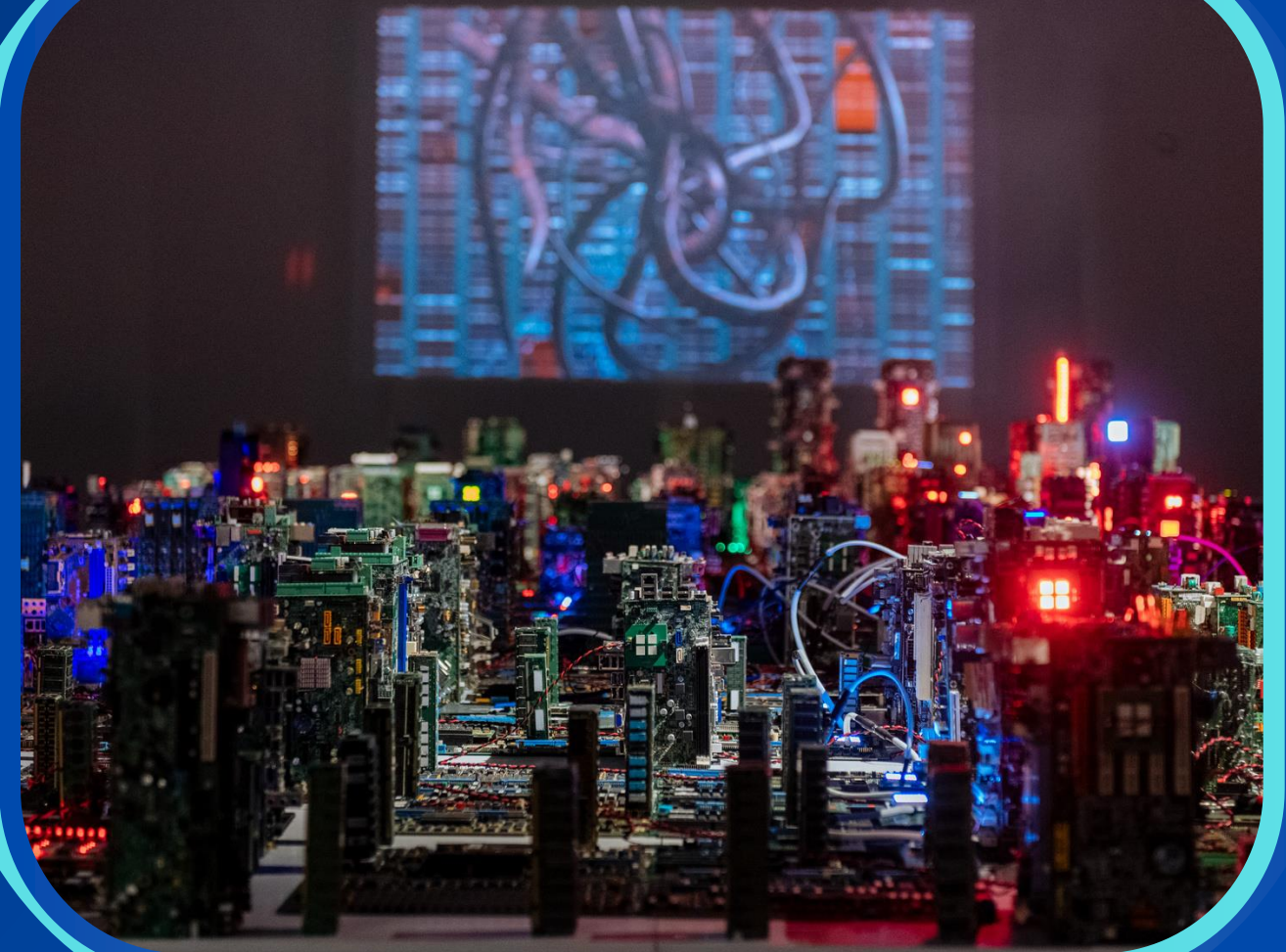
- Explore how organisations perceive, prepare for and respond to cyber risks in digital supply chains.
- Examine TPRM practices
 - Explore cross-functional incident readiness
- Evaluate governance & info-sharing.



LITERATURE REVIEW

Digital Supply Chains and Cyber Risk Exposure

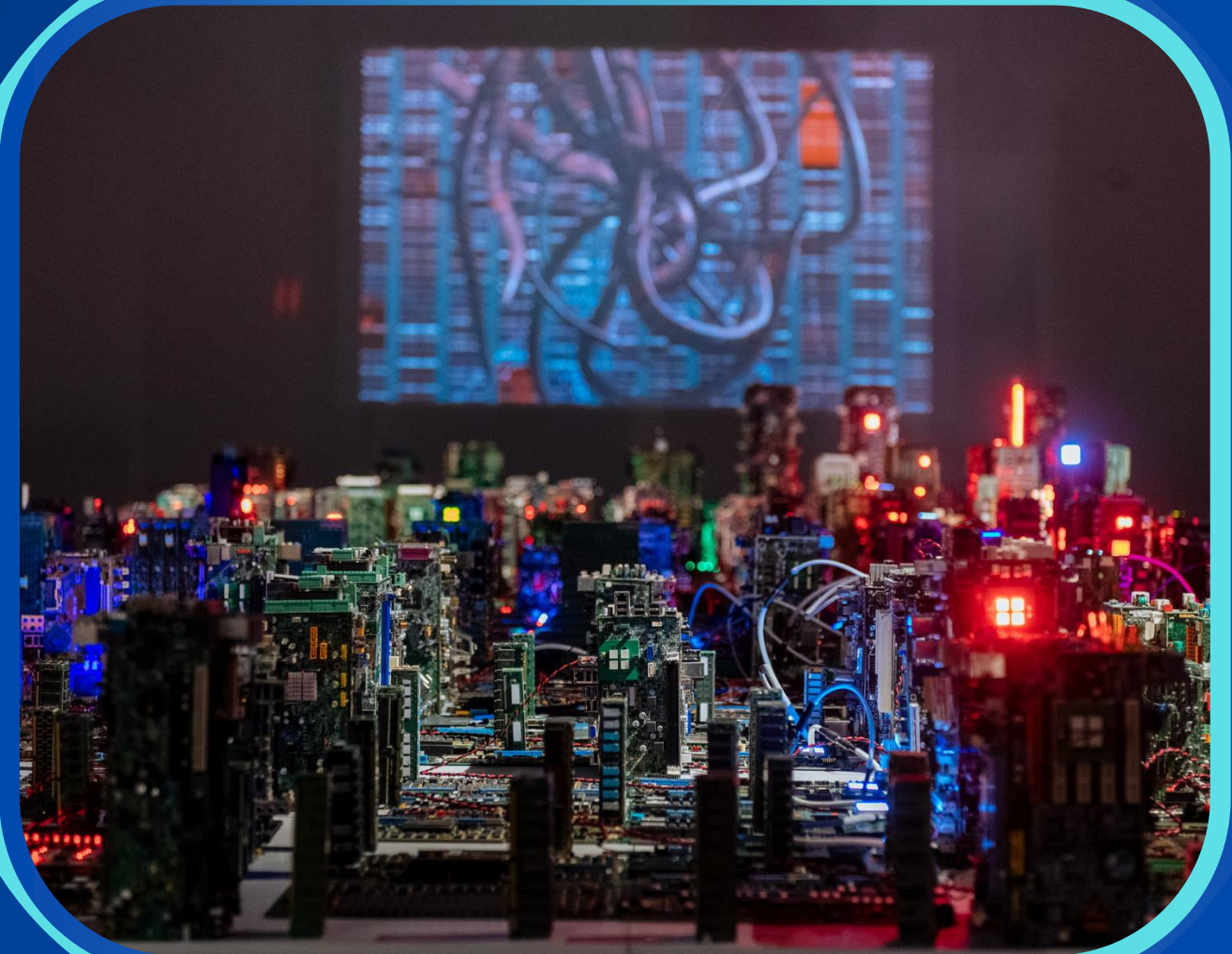
The process of digital transformation has transformed supply chains from their previous state as linear systems to their current state as complex networks that depend on data.



LITERATURE REVIEW

Third-Party Risk Management in Supply Chains

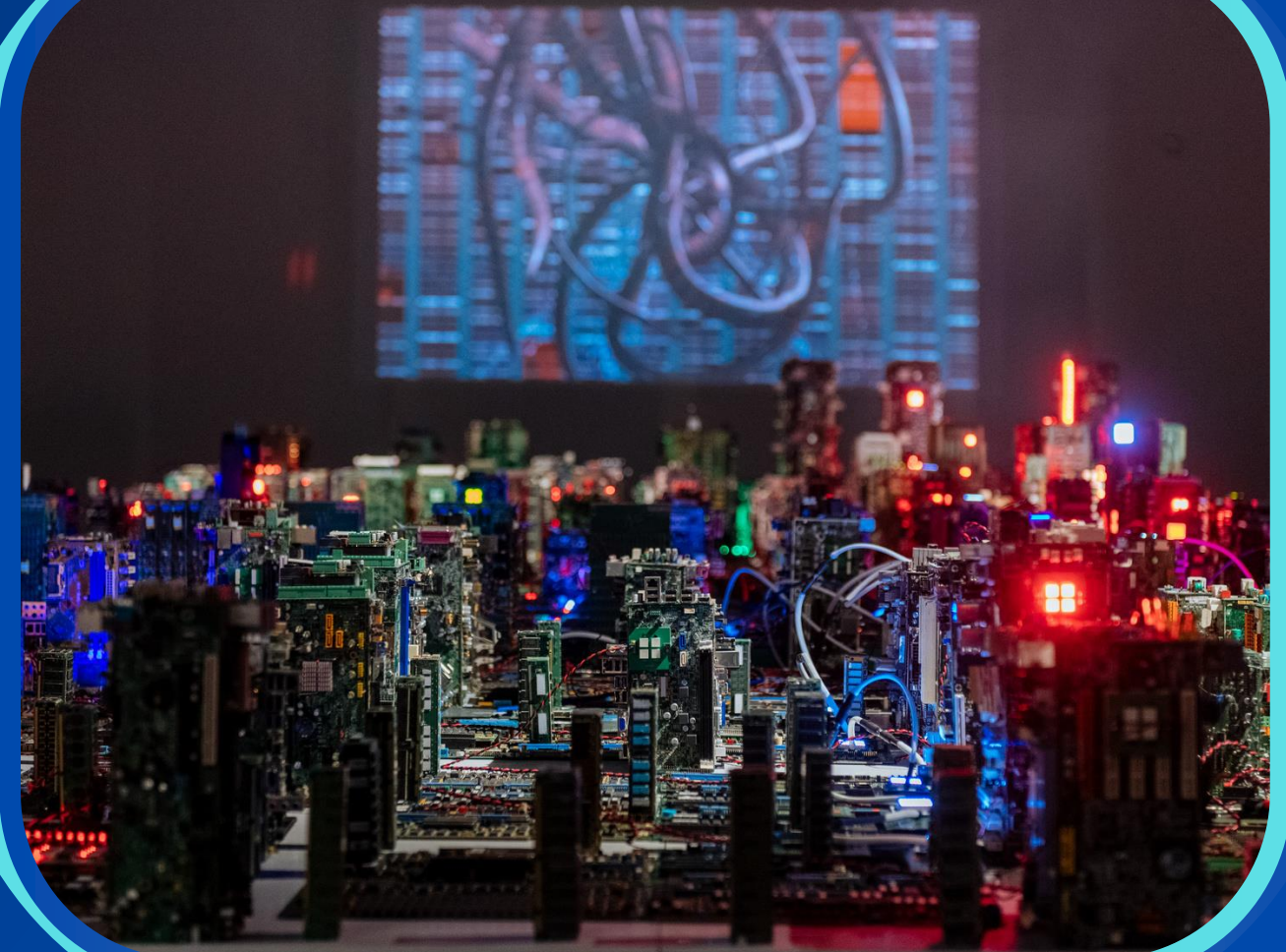
Third-party risk management (TPRM) has become an essential aspect of supply chain management. The traditional methods of assessing suppliers concentrated on three main factors which included cost and quality and delivery performance and reliability.



LITERATURE REVIEW

Cybersecurity Governance and Organisational Integration

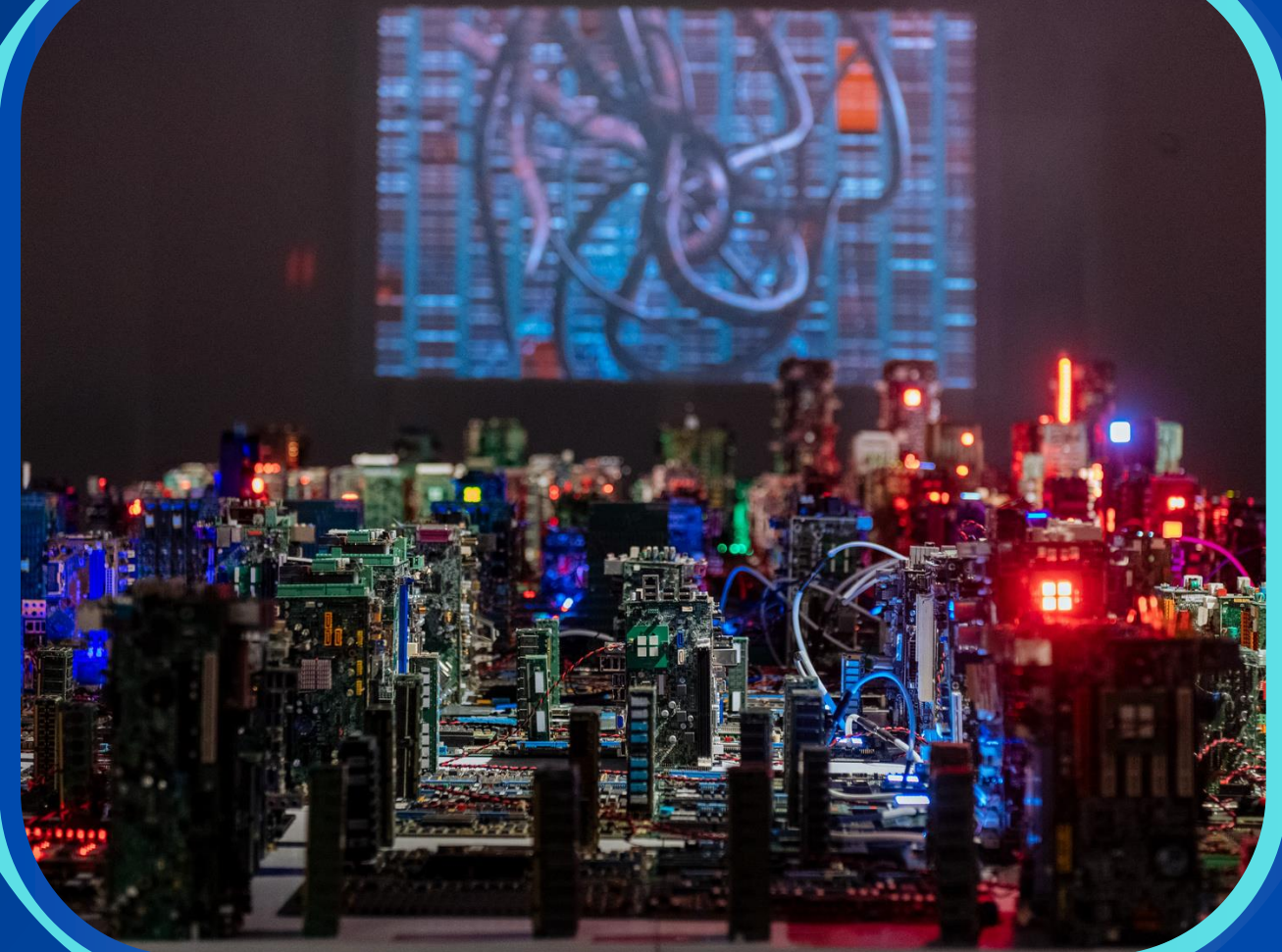
The cybersecurity governance literature requires organizations to implement risk management across all their operational areas. Cybersecurity developed as a technical field which IT departments controlled throughout its history. Digital supply chains demand their various teams which include procurement, operations, legal and executive staff to work together



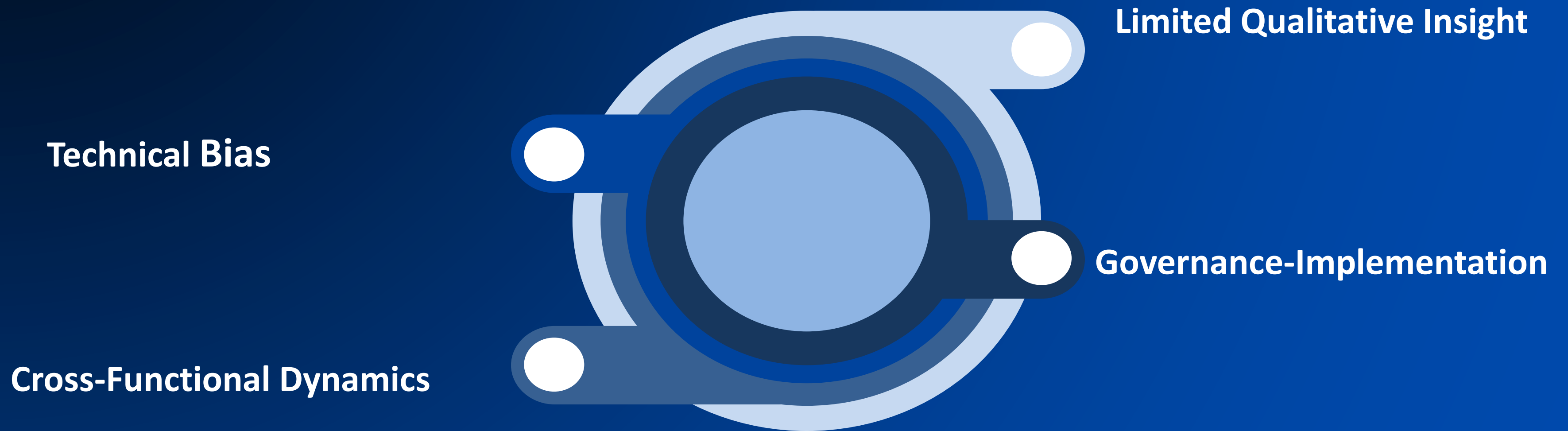
LITERATURE REVIEW

Information Sharing and Collaborative Security

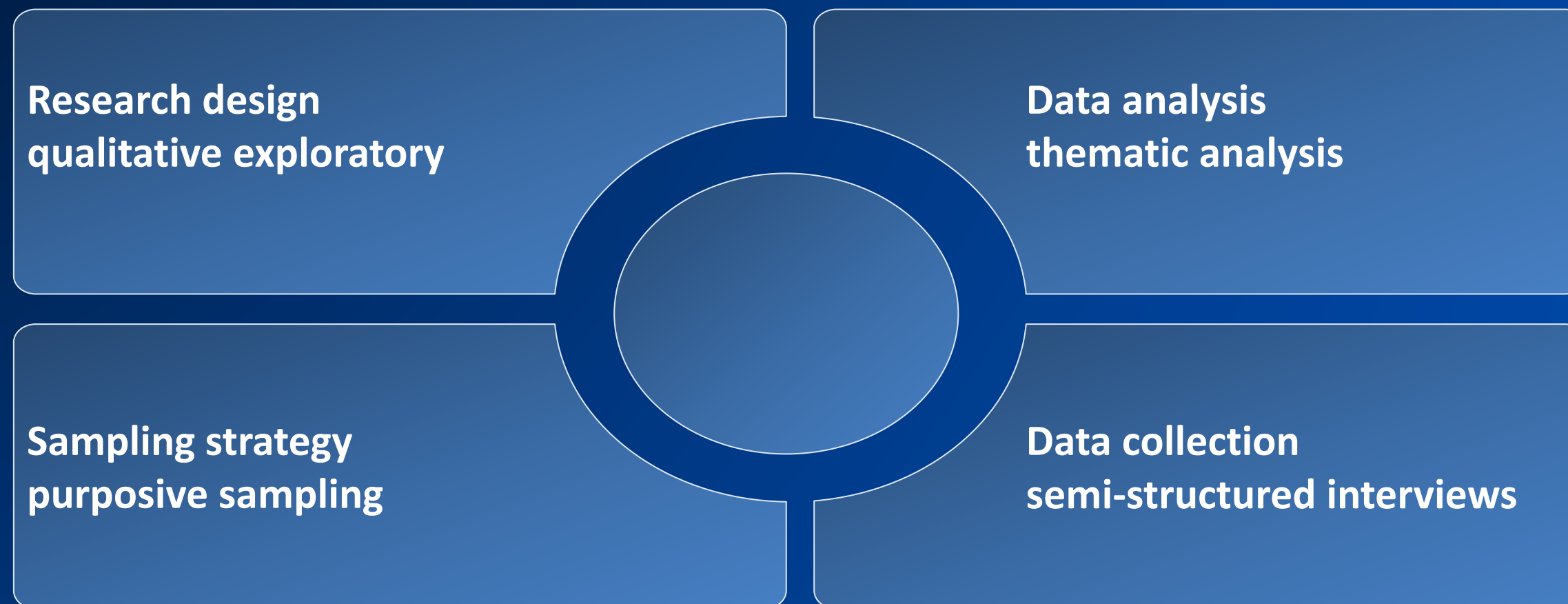
Inter-organisational collaboration plays a crucial role in mitigating supply chain cyber threats. Information-sharing frameworks such as ISACs (Information Sharing and Analysis Centers) aim to disseminate threat intelligence among sector members to reduce detection time and coordinated vulnerabilities.



Research Gap



METHODOLOGY



Main themes extracted

Limited information sharing among supply chain partners

Limited Supplier Cybersecurity Assessment

Weak Cross-Departmental Coordination

Budget Constraints and Operational Priorities

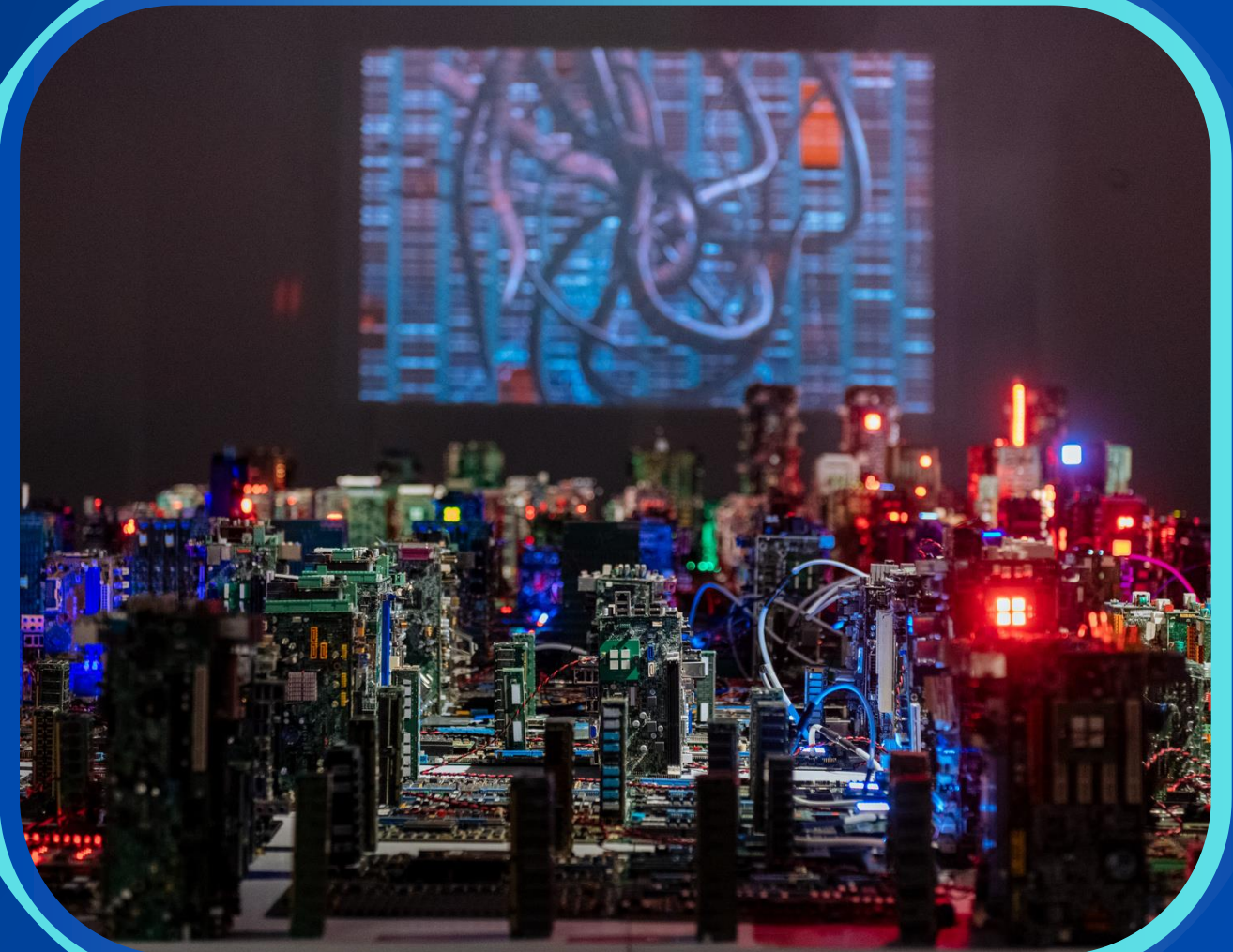
MAIN THEMES

Limited information sharing among supply chain partners

The analysis discovered its third theme which shows that supply chain partners exchange cybersecurity information at minimal levels. Only six participants from the interview sample who make up about 30 percent of the total sample reported their organizations share cybersecurity threat intelligence with their suppliers and logistics partners.

The participants explained that companies will avoid disclosing their cybersecurity incidents to the public because they want to protect their reputation and their internal security weaknesses.

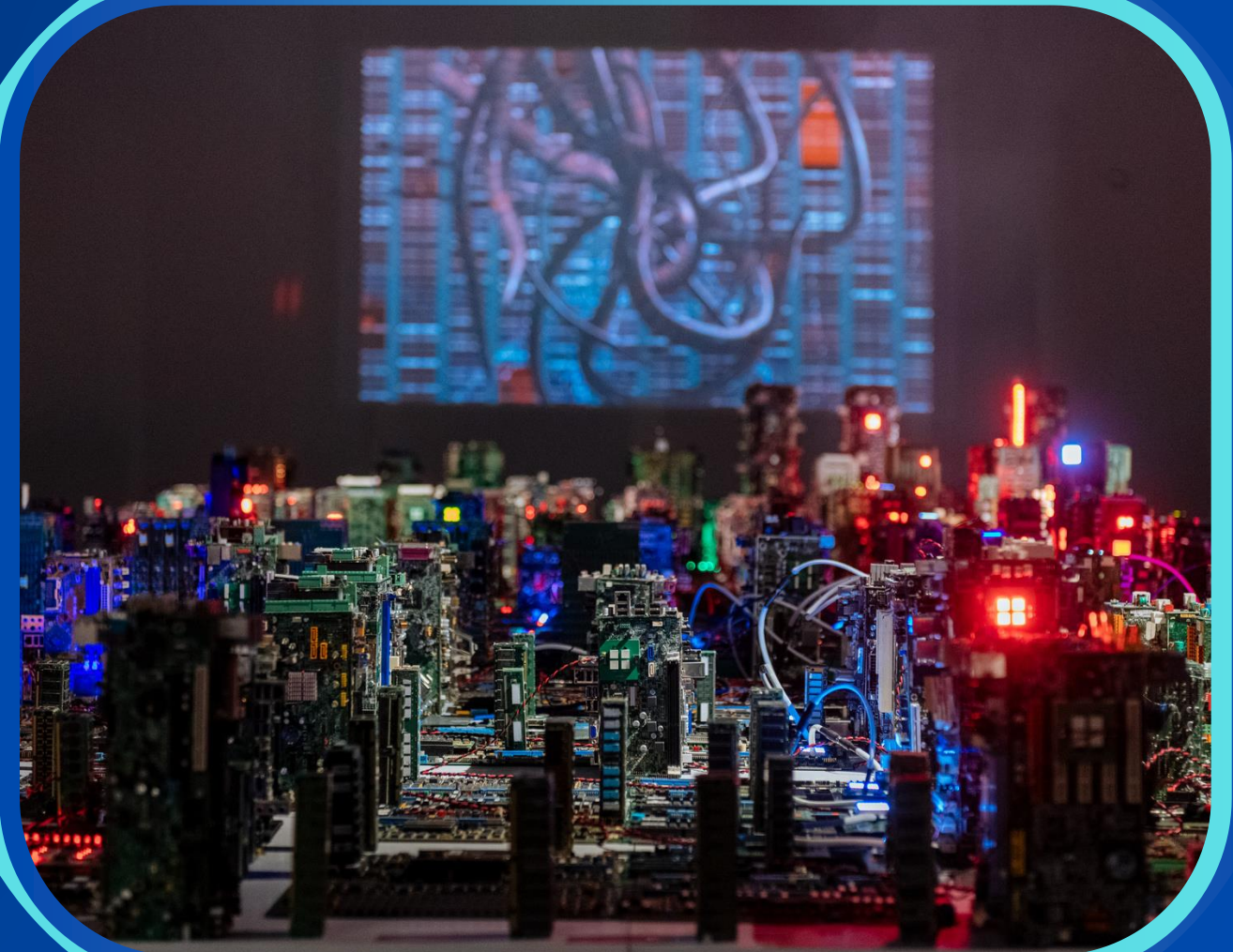
Participant P14 noted: "Organizations are often reluctant to share cybersecurity incidents with external partners because they fear reputational damage or loss of trust."



MAIN THEMES

Limited Supplier Cybersecurity Assessment

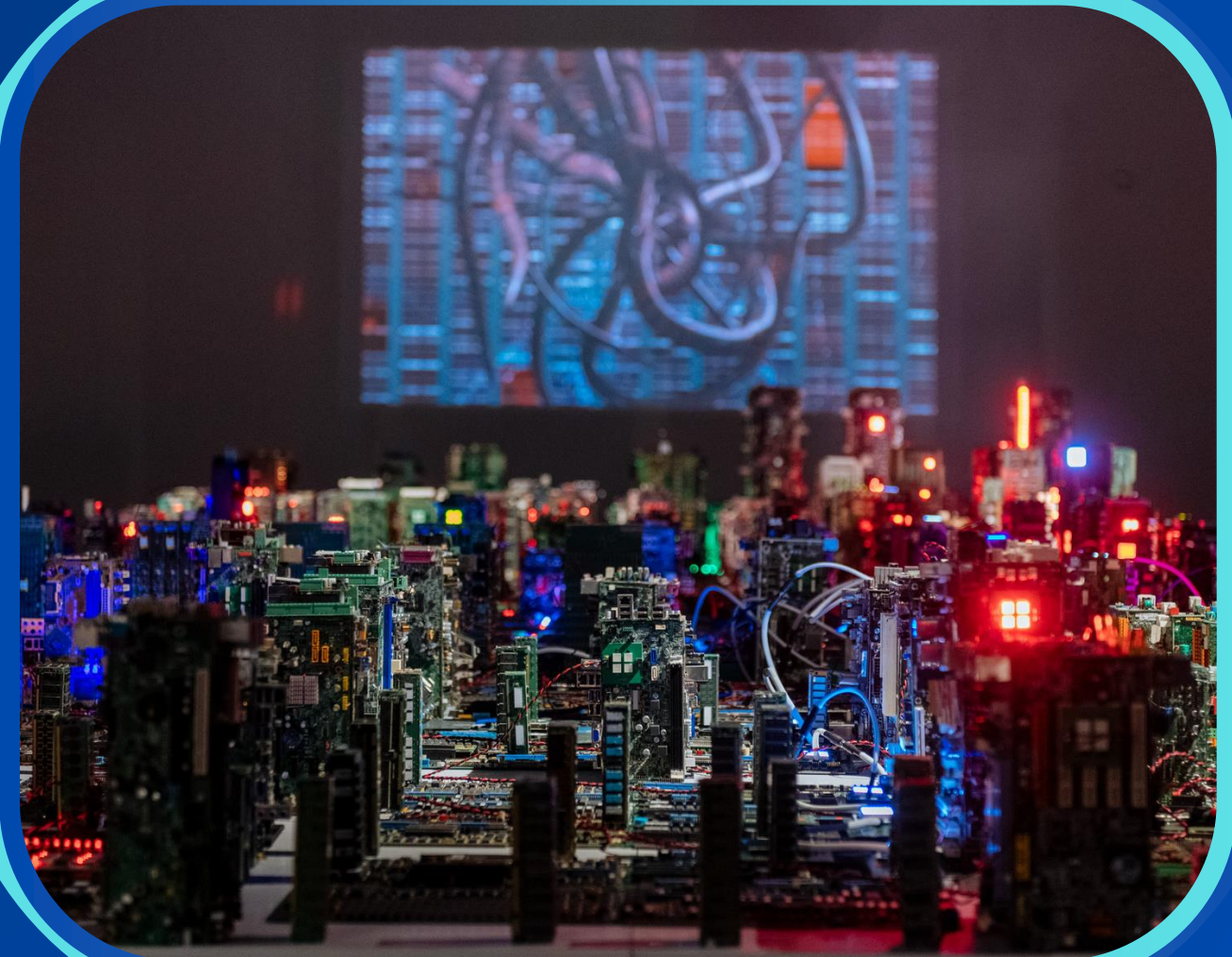
The most frequently reported issue among participants was the limited evaluation of cybersecurity risks when selecting or managing suppliers. This concern was mentioned by 14 out of the 20 participants, representing approximately 70% of the interview sample. Several participants indicated that supplier selection decisions are often driven by operational considerations such as cost efficiency delivery speed and logistical reliability while cybersecurity assessments receive less attention.



MAIN THEMES

Weak Cross-Departmental Coordination

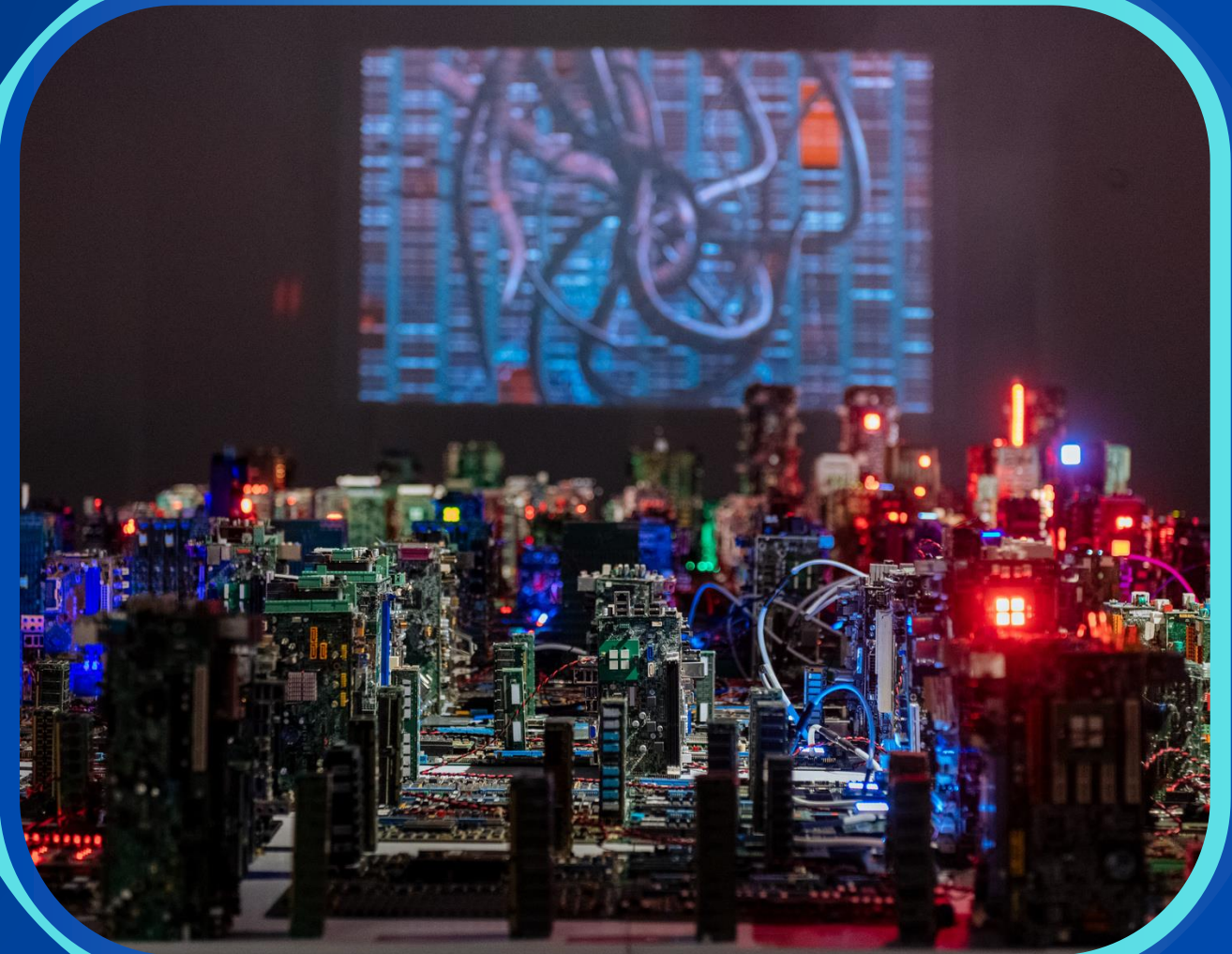
The second major theme identified during the analysis relates to the lack of coordination between supply chain management teams and information technology departments. The problem was reported by 11 participants who made up about 55 percent of the interview sample. Many respondents indicated that cybersecurity responsibilities are often managed exclusively by IT departments while supply chain managers focus primarily on operational performance indicators such as delivery timelines and supplier reliability.

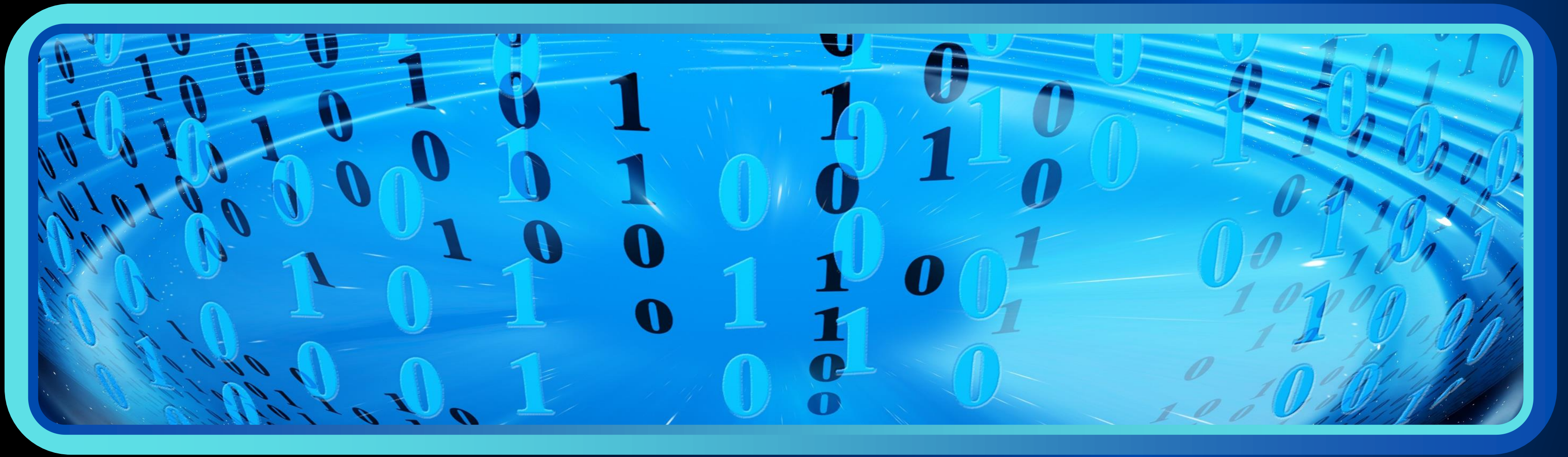


MAIN THEMES

Budget Constraints and Operational Priorities

The analysis discovered yet another important theme which shows how financial constraints and operational needs that conflict with each other create operational difficulties for organizations. This issue was mentioned by 9 participants, representing approximately 45% of the interview sample. Participants frequently indicated that cybersecurity investments must compete with other operational expenditures, including logistics infrastructure, supplier development programs, and digital transformation initiatives. Participant P7 stated: Cybersecurity investments are important, but they often compete with other operational priorities such as logistics infrastructure and supplier expansion





RESULTS & RECOMMENDATIONS

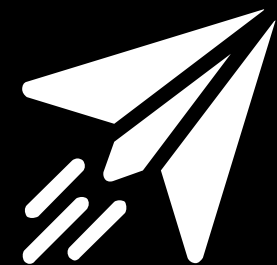
Directions for Future Research

Researchers can use quantitative methods to study cybersecurity risk management practices in multiple organizations from different industries to extend the findings of this research study. Quantitative studies will show how digital supply chain structures and cybersecurity investments impact organizational performance.

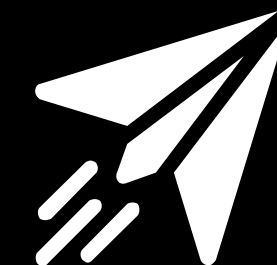
Future research will investigate how artificial intelligence and blockchain technology and advanced threat detection systems protect digital supply networks through cybersecurity resilience.

Subsequent research will investigate how collaborative cybersecurity frameworks which enable information exchange and shared risk management among supply chain partners operate.

RECOMMENDATIONS



organizations should integrate cybersecurity risk assessment into supplier selection and evaluation processes. The procurement process together with supplier management operations should include supplier cybersecurity audits and risk assessments as standard elements.



organizations need to build stronger partnerships between their supply chain management departments and their information technology departments. The digital supply chain cybersecurity risks require organizations .

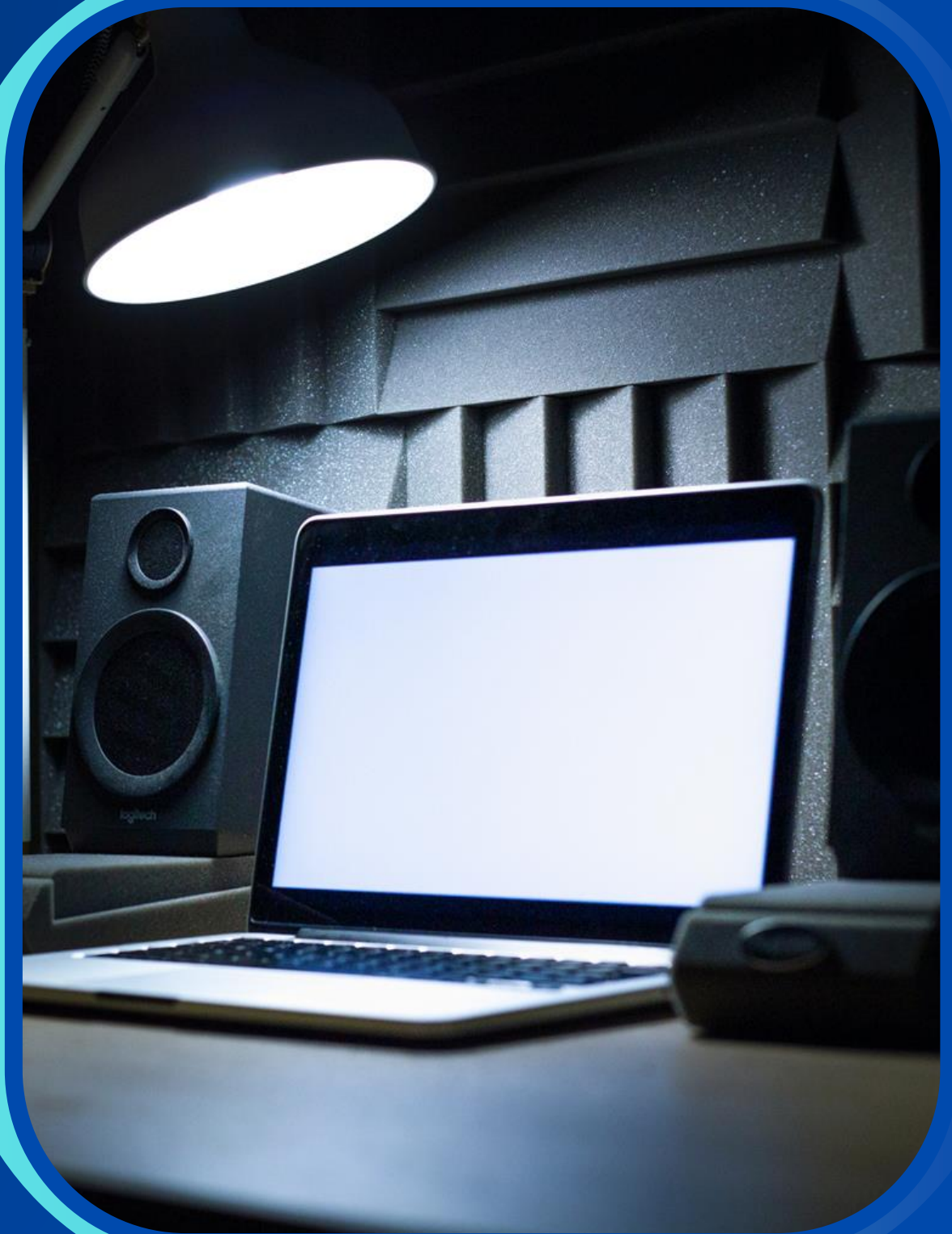


organizations should invest in continuous monitoring systems that allow them to detect vulnerabilities within third-party digital platforms and supplier information systems. The implementation of such monitoring systems will decrease the chances of cyber incidents spreading through supply networks.

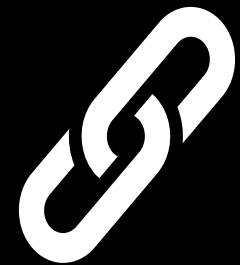


CONCLUSION

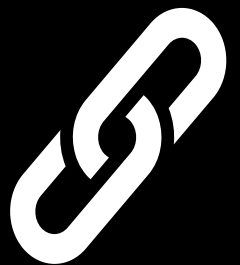
The research investigated cybersecurity threats which face digital supply chains together with their impacts on organizations in contemporary business environments that use digital systems. Organizations that use digital technologies which include cloud computing Internet of Things (IoT) systems enterprise resource planning platforms and real-time data exchange systems for their supply chain operations face new cybersecurity threats which can disrupt their business activities and damage their financial results and hinder their decision-making process. The research aimed to understand how organizations view and manage cybersecurity risks which exist in their digital supply chains.



REFERENCES



Ivanov, D. (2021). Digital supply chain management and technology to enhance resilience by building and using end-to-end visibility during the COVID-19 pandemic. IEEE Engineering Management Review, 49(1), 33–41.



Latsiou, A., & Lambrinoudakis, C. (2026). Cyber supply chain risk management: From threats to treatment. International Journal of Information Security, 25, Article 40.



Saranga, H., & Singh, H. (2024). Integrated model to optimize supplier selection and investments for cyber resilience in digital supply chains. International Journal of Production Economics.





THANK YOU

Secure Your Digital Life Today