The Warehouse of the Future Initiative
Key Vulnerabilities in the Warehouses of The Future

MIT's Warehouse of the Future Initiative is a research program developing cutting-edge insights into highly automated and interconnected warehouses that leverage automation and digitalization to adapt to evolving market and supply chain trends. Our research integrates a forward-thinking model that aligns operational efficiency, resilience, and technological innovation with a sustainable, human-centric approach to warehousing—pivotal to the evolution of supply chains.

The Warehouses of the Future Bring New Supply Chain Risks

The rapid adoption of automation and digital technologies in warehousing introduces new risks that could disrupt operations and impact the broader supply chain. Drawing from extensive state-of-the-art research and insights from over 40 warehousing and technology experts, our study identifies five major disruptions that can affect modern, highly automated warehouses: cyberattacks, power and network outages, technology sabotage, technology failures, and accidents caused by human-machine interaction. **Figure 1** shows the 26 key vulnerabilities (grouped by categories) and their associated disruptions in warehouses of the future. These are also summarized in **Table 1**.

Cybersecurity has become a major concern, exposing many risks within the warehouse and supply chain network. Warehouses increasingly rely on cloud-based systems and Robotics-as-a-Service—a model where technology suppliers have remote access to warehouse automation systems—while the number of technology suppliers and required systems integrations is increasing as well. All these factors expand the cyberattack surface that is vulnerable to malicious actors. **Advanced hardware**, such as Autonomous Mobile Robots (AMRs) and grid-based Automated Storage and Retrieval Systems (AS/RS), introduces new safety considerations and operational complexities, including the balance of operational flexibility and rigidity, proximity and interactions with warehouse staff, fire hazards, and business continuity in the face of power and network outages.

Table 1: Summary of the vulnerabilities in the warehouses of the future by category.

Data Management	• Data quality and a lack of data security often results from transitioning to new technologies and integrating new systems.
Software Systems	• Legacy system dependencies limit cybersecurity capabilities. • Software bugs and vulnerable open-source libraries. • The dynamic warehouse environment makes it challenging to establish robust system access controls.
Automation Hardware	• Battery and charging system failures pose new fire risks. • Sensor malfunctions and navigation errors can lead to accidents. • Rigidity from automation reduces adaptability to disruptions.
Digital Network Infrastructure	• Cloud migration exposes operations to new cybersecurity threats. • Systems integration creates points of failure and unauthorized access.
Physical Infrastructure	• Power and network outages can result in significant disruption. • Physical facility security remains a primary vulnerability.
Human-machine Interaction	• High employee turnover and low technology acceptance create security vulnerabilities and challenges to technology adoption. • The physical size of new, mobile automation equipment and the proximity of warehouse staff can compromise safety.

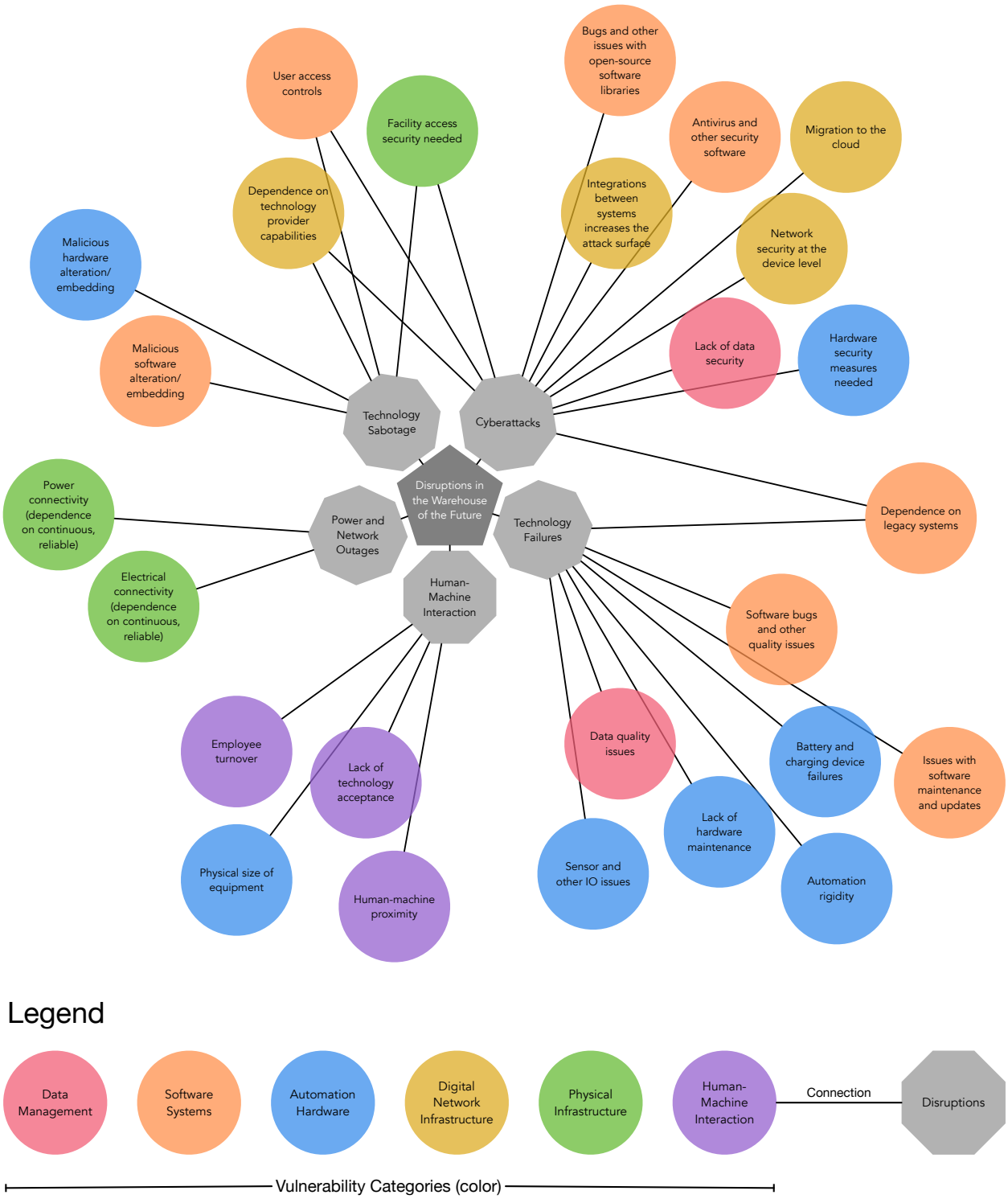

Figure 1: Vulnerabilities and associated disruptions in the warehouse of the future.

Building Resilience in the Warehouses of the Future

The path toward increasing automation and technological sophistication in warehouses requires a multifaceted approach to risk management. Companies need to focus on developing new detection and mitigation capabilities against technology-related risks, while maintaining flexibility in their operational strategies and building redundancy for the worst-case scenarios. Our research has identified three key areas for companies to focus on.

First, new approaches to technology evaluation, systems integration, and vendor management are needed to account for increasing **cybersecurity** risks. Robust, standardized security practices are critical, including for smaller firms adopting and supplying new technologies, which can present access points for cyberattacks on large supply chain networks. There are many examples where an attack on a key technology supplier has had devastating effects on multi-firm supply chains.

Second, high employee turnover leads to a loss of operational knowledge over time and can result in unsafe practices. The complexity of modern warehouse systems will necessitate continuous **training and upskilling** of the current workforce It will also allow companies to create safer and more rewarding jobs in warehouses that can increase retention rates. Fostering a culture that embraces technological advancements while recognizing the continued importance of human expertise will be critical for the success of such training programs.

Third, there is a need for new **business continuity plans**. This could be done by employing high-availability approaches for critical systems. For example, companies can safeguard their warehouse management systems (WMS), which represent the brain of interconnected warehouses, with three copies: a local host, their own server, and a cloud backup. In case of a failure, the backups should allow for a seamless, fast recovery by switching systems. In terms of power and network connectivity, warehouses can also build redundancy by establishing multiple access points with different telecom providers. Additionally, companies should have manual fallback options for their facilities in case of complete system failures.

Finally, our research underscores the need for more **collaboration** within the industry to address emerging challenges and capitalize on new opportunities. Fostering stronger partnerships among stakeholders, including competitors, 3PLs, reliable vendors, researchers, and government agencies, will be key to maintaining a balance between technological advancement and the right risk management strategies. This will be crucial for the long-term success and resilience of the warehouses of the future and entire supply chains.

IMPACT: This research highlights the need for a balanced approach to warehouse automation that considers both technological advancement and risk management. It also highlights the need for executives to develop a deeper understanding of the vulnerabilities that arise in highly automated warehouses. Our work could help companies account for new technology-related risks and develop the right prevention, mitigation, and recovery strategies, defining the path toward resilience in the warehouses of the future.

TEAM

- Dr. Miguel Rodríguez García is a Research Scientist at the MIT Omnichannel Supply Chain Lab at MIT CTL, and leads the Warehouse of the Future Initiative – miguelro@mit.edu
- Dr. Eva Ponce is the Founder & Director of the MIT Omnichannel Supply Chain Lab at MIT CTL – eponce@mit.edu
- Mr. Kellen Betts is a researcher and program manager at MIT CTL – kellenb@mit.edu