MIT's Warehouse of the Future Initiative

IDENTIFYING THE KEY VULNERABILITIES IN THE WAREHOUSES OF THE FUTURE

Results from Field Research and a Literature Review

Miguel Rodríguez García
Kellen Betts
Eva Ponce

February 2025

MIT Center for Transportation & Logistics

MIT Omnichannel Supply Chain Lab

Table of Contents

List of Figures

List of Sidebars

Introduction

The distribution warehouse industry is undergoing a rapid transformation, driven by rapid technological advancements and an increasing demand for efficiency and automation due to the growth of e-commerce. As warehouses evolve from traditional manual operations to highly automated, data-driven environments, they face unique vulnerabilities and disruptions. Despite the extensive research on warehouse automation and digitalization, there is a notable gap in understanding how these technologies, while offering operational benefits, simultaneously introduce vulnerabilities that can disrupt the warehouse of the future (Hollerer et al. 2021; Khalid et al. 2022). The integration of advanced technologies such as Autonomous Mobile Robots (AMRs), cloud-based Warehouse Management Systems (WMS), grid-based Automated Storage and Retrieval Systems (AS/RS), and Artificial Intelligence (AI) brings both unprecedented capabilities and new vulnerabilities.

Meanwhile, supply chain risk management studies often consider disruptions on a larger network scale, with limited attention to the unique challenges faced by modern warehouses, which are typically viewed as mere nodes within the supply chain (Cheung, Bell, and Bhattacharjya 2021). This study seeks to address the fragmented approach in the existing literature by focusing on the technology-related vulnerabilities that increase the risk of disruptions, such as cyberattacks, technology failures, technology sabotage, power and network outages, and human-machine interaction.

Through interviews with more than 40 subject matter experts and insights from an extensive literature review that includes more than 200 articles, we have identified **the 26 most important technology-related vulnerabilities in the warehouse of the future (*Figure 1*)**. We classify the vulnerabilities across multiple areas of operation, including data management, software systems, automation hardware, digital network infrastructure, physical infrastructure, and human-machine interaction. Finally, we connect the 26 vulnerabilities identified with the five main disruptions. By doing this, we bridge the conceptual gap between

discussions on the warehouse of the future and the associated risks introduced by new technologies.

This final report compiles the review of more than 200 articles and over 70 hours of data collection with the interaction of more than 40 subject matter experts through 30 interviews and three focus groups, and five warehouse facility visits. The report is organized as follows: The next section describes the methodology used. Each subsequent section focuses on one of the vulnerability categories identified in this research project. Finally, the report concludes with a summary of the project's findings and a list of references used for preparing this final report.

Methodology

This report is based on field research, including one-on-one interviews with industry subject matter experts and focus group discussions. It also incorporates insights from the scientific and industry-practitioner literature.

Field Research

We conducted 30 interviews and 3 focus groups with subject matter experts. Over 40 individuals participated in these activities. They were selected based on their roles and backgrounds in companies that operate automated distribution warehouses, companies that develop technologies for this application, and others who conduct research in the domain or provide consulting services.

Two rounds of interviews were conducted in a structured manner, with questions prepared by the research team before starting. For the first round of interviews (20), the questions were designed to gain broad insight into the current state of warehouse operations and the emerging risks associated with technological advancements. A second round of interviews (10) was conducted with questions more focused on specific details of technology systems, such as the cybersecurity features of AMRs, and specific industries, such as pharmaceuticals, due to

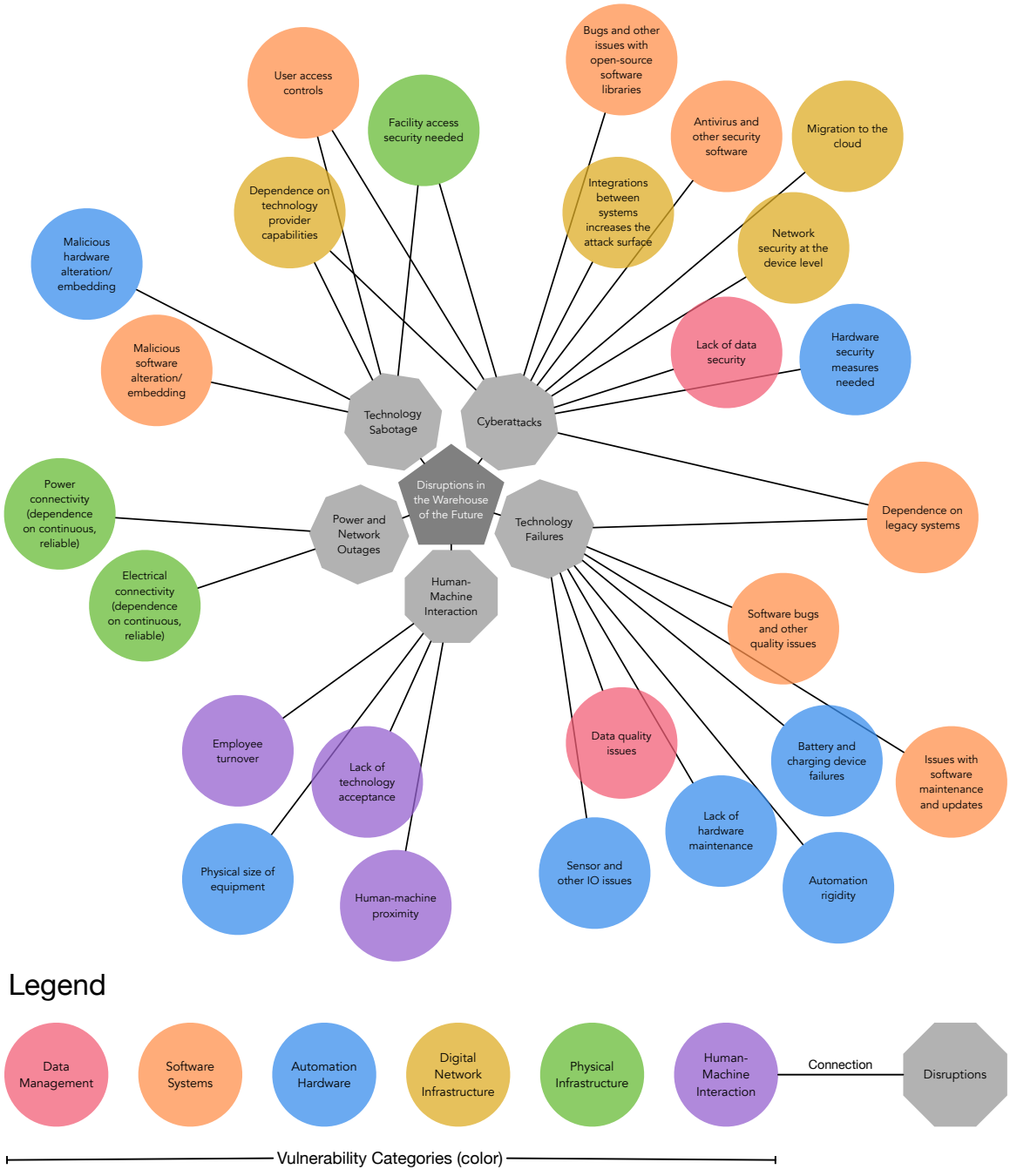

Figure 1: Vulnerabilities in highly automated warehouses and associated disruptions.

the background of the individual and the need to gain more insight into a specific area than what was shared in the first round of interviews.

We also conducted 3 focus-group discussions with 7 subject matter experts in each group. These participants had similar profiles to those interviewed, and in some cases, the individuals we interviewed also participated in the focus groups. The focus-group format provided a setting where conversations would "snowball," with each commentator building on previously shared thoughts.

The research team took detailed notes on what the participant(s) shared in the interviews and focus groups. Due to the sensitive nature of discussing technology vulnerabilities and disruptions, we did not record audio or video from the interviews and focus groups. Additionally, this report does not include the specific names of the individuals and the companies for which they currently and previously worked.

Qualitative Analysis

For the first-round interviews, we conducted a rigorous qualitative analysis of the notes we collected during the interviews. This analysis was focused on the first round of interviews due to the broader nature and standardization of the topics discussed. Insights from the second round of interviews and the focus groups were incorporated into this report after that analysis to provide deeper insight and more detailed examples in specific areas.

The methodology used for the qualitative analysis was based on Gioia, Corley, and Hamilton (2013) and Mayring (2019). The approach was designed to identify common patterns across the interviews. Using a computer-assisted qualitative data analysis software (CAQDAS) system called Dedoose, we coded the notes generated during the interviews based on direct textual identification and subjective interpretation of context, focusing on coding the vulnerabilities and disruptions mentioned by the interviewees.

This process resulted in 'first-order codes' directly linked to the text of the interview notes. These first-order codes are presented here as the individual vulnerabilities and disruptions, such as

'battery and charging device failures,' discussed in section *3. Automation Hardware*. They are also visualized as circular (vulnerabilities) and octagonal (disruptions) elements in *Figure **1***.

These first-order codes were then compiled into a dataset for further analysis and classification. The classification of the first-order codes produced second-order categories. This classification was based on the patterns observed in the first-order codes and the lexicon found in our prior literature review. These second-order categories are used to organize the discussion of the more detailed vulnerabilities in this report and serve as the primary sections of the report, including *1. Data Management, 2. Software Systems, 3. Automation Hardware, 4. Digital Network Infrastructure, 5. Physical Infrastructure,* and *6. Human-Machine Interaction*. These categories are also visualized in *Figure **1*** using colors for the circular elements.

The last step in the qualitative analysis was establishing connections between vulnerabilities and disruptions. This was done based on the pattern of common occurrences within the interviews. For example, if an interviewee mentioned the risks associated with moving a software system to the cloud (vulnerability) and the increased potential for cyberattacks (disruption) on the system. We also established connections between vulnerabilities and disruptions based on clear technical connections. For example, the dependence on reliable electrical power was a vulnerability expressed by most interviewees and is clearly linked with the disruption of power outages. The connections between vulnerabilities and disruptions are incorporated within the narrative of this report. They are also visualized in *Figure **1*** as lines connecting the circular (vulnerabilities) and octagonal (disruption) elements.

Literature Review

In addition to the field research and subsequent qualitative analysis, this report incorporates insights from the academic and industry literature. For this literature review, we adopted the semi-

systematic or meta-narrative literature review methodology advocated by Snyder (2019). This methodology excels in identifying overarching themes, trends, and patterns that may not be immediately apparent through more conventional systematic reviews that focus on a well-researched topic, only include academic literature, and often limit article selection to specific research approaches. Our aim was to connect warehouse technologies with potential disruptions and vulnerabilities related to these technologies. Because we were exploring a new research area where the literature was occasionally scarce, the semi-systematic approach allowed us to expand the scope to adjacent areas, such as manufacturing and laboratory environments, as well as news sources to capture a real-time perspective. In total, 207 academic and general articles were reviewed, of which 55 were selected for this final report due to their relevance to the topic and quality.

1. Data Management

As warehouses become increasingly digitized, data management has emerged as a critical vulnerability. Data within modern warehouse software and automation equipment are hosted on local servers, private cloud servers, and public cloud services, depending on the system and application. **The following vulnerabilities (represented by red circles in *Figure 1*) have been identified within this category.**

1.1. Data Quality Issues

The integration of data across various systems, especially with the transition from local to cloud-based systems, presents significant risks to data consistency and accuracy while exposing sensitive information.

New data systems, such as digital twins and data lakes, along with upgrading legacy systems, add to this complexity. For example, a leading grocery retailer experienced disruptions to inventory management (e.g., food perishability and 'first in, first out' processes) when

transitioning from a legacy AS-400 system to a more advanced WMS supporting AI and automation. Harnessing new data and creating new data lakes were the main two challenges faced by this large corporation.

Another common vulnerability many companies face is the volume of data they have without clear strategies to reduce the risks associated with collecting, storing, and transmitting that data within their systems. Some companies have decoupled warehouse facilities from central systems, running automation on local servers and minimizing communication with enterprise-wide systems. While this may reduce the risk of sensitive data being transmitted between a facility and enterprise-wide systems, it can also lead to siloed operations and limited visibility across facilities. Looking forward, the participants mentioned the potential use of AI tools to be able to follow and audit data faster and for a lower cost.

1.2. Lack of Data Security

Privacy concerns present additional challenges. At the warehouse device level, AMRs equipped with camera systems may be capturing sensitive images of products or employees. Similarly, sensitive information can be transmitted to the warehouse, such as customer information related to orders. One strategy often discussed to mitigate risks related to sensitive data in warehouse technologies is the compartmentalization of data. For instance, some AMR systems are designed to operate with anonymized customer information related to orders, so that sensitive information is not sent to the device. However, it has been observed that some AMR providers may store various types of sensitive data within the AMR software systems, such as customer details and operational images, partly because regulations governing data storage and usage can vary significantly between countries and states. This may lead to a lack of data security unless explicitly addressed by the customer.

The growing importance of cloud-based systems introduces further complexities in data management and security. In addition to the risks associated with transmitting data from on-

premise systems to the cloud, regional data storage requirements, such as Dubai's local data storage mandate, add layers of compliance and operational difficulty. Most large companies, especially those within the pharmaceutical industry, are implementing robust data protection strategies to mitigate these risks.

In interviews with two 3PLs, a critical security insight emerged regarding the management of WMS data. They highlighted the need for a system architecture that ensures proper data handling, with the application serving as an isolation layer between the web interface and the database. This architecture ensures the database is isolated from direct communication and can only be accessed by the application. A significant red flag is when vendors provide direct access to their WMS databases, as this compromises data security. Companies should allow vendors to only work with "dead" or static data disconnected from the live database. If direct access is granted, it risks exposing all clients' data to each other. For example, one of the companies mitigates this risk by only granting read access to inventory data, with the WMS provider managing the database interactions to ensure security.

The challenge of data management within highly automated warehouses will continue to grow with the introduction of new automation technologies and the integration of advanced software systems. This means leaders need to carefully consider technology implementation, privacy concerns, and data security strategies.

2. Software Systems

While warehouses are notable for the flow of physical materials and the associated equipment, highly automated warehouses are increasingly defined by complex software systems. These systems exist across a complex landscape of on-premise and cloud-based infrastructure that connects various systems. Given the complexity of these systems and their connections, as well as the central role that many serve in the management of warehouse operations, a disruption of software systems can have a significant impact. Moreover, the attack surface for potential

cyberattacks increases dramatically as more software is being implemented in modern warehouses. The participants of the study highlighted that hackers can easily identify who is using which software out there, so once a hacker identifies a vulnerability in a software, they can attack the users. **The following vulnerabilities (represented by orange circles in *Figure 1*) have been identified within this category.**

2.1. Software Bugs

The complexity of modern warehouse environments, characterized by a multitude of interconnected systems, increases the potential for software failures. For example, the European retailer ASOS faced a critical software glitch in its Warehouse Management System (WMS), which significantly reduced available inventory to customers, leading to an estimated $25 million in lost sales (Supply Chain Dive 2019). The fact that this failure occurred in a key system highlights how critical software failures can halt operations, leading to costly disruptions.

As warehouses become increasingly reliant on automation, the proliferation of technologies—including robotics, automated storage and retrieval systems (ASRS), and autonomous mobile robots (AMRs)—introduces additional software layers that need to be properly managed. The more technologies that are integrated into warehouse operations, the greater the reliance on software to ensure their seamless functionality. However, each new technology comes with its own set of software dependencies, and failure in any one of these systems can have ripple effects across the warehouse.

According to Kumar and Mallipeddi (2022), logistics technologies can experience frequent software bugs, with some estimates suggesting one defect for every 35 lines of code, demonstrating the inherent fragility of these systems. One interviewee of our study, the Global Head of Innovation at a major third-party logistics provider (3PL), put it this way: "*We have experienced several software glitches in modern AI-driven automation. If that happens while someone is working close to automation...*" This emphasizes the immediate operational and safety risks that software

malfunctions pose, particularly when the workforce is in proximity to automated systems such as automated forklifts or robotic arms that can severely harm a person in case of an accident.

2.2. System Access

Critical vulnerabilities with warehouse software systems include not just bugs and glitches but also user access issues, as many warehouse systems allow multiple users with varying levels of permissions to access different software components. For example, legitimate remote access tools, which are common among AMR systems, could be easy targets for exploitation by an internal malicious actor (Cybersecurity and Infrastructure Security Agency 2023). This would allow them to perform unauthorized activities, such as remote code execution or data breaches, with minimal oversight. According to the interviewees, there is an increasing number of external users who gain access to their warehouse software solutions, and they believe these access points create a cybersecurity risk, especially when remote access is enabled for maintenance or troubleshooting purposes. If improperly managed, unauthorized access to these systems could lead to malicious tampering, data theft, or even operational shutdowns.

In particular, the growing trend of Robotics as a Service (RaaS) adds complexity to system access management because it involves not just physical access but also remote control of software and robotics through cloud platforms. Any weakness in the vendor's security protocols could become a potential entry point for attackers. Smaller companies, in particular, may be at greater risk due to limited resources to manage and monitor vendor access effectively (Crowe 2021). The participants of the study suggested that role-based access is essential for these systems, with a focus on multi-factor authentication and monitoring both employee and vendor access. Vendors often claim they need constant access, but a more secure approach should involve constant monitoring and recording of their actions.

According to the participants, system access also presents a specific challenge in the warehouse environment from a labor-management perspective. Many warehouses, especially

those serving the retail market, face staffing challenges and significant seasonal fluctuations in workloads. Ideally, companies need a robust onboarding process for new employees with the appropriate level of access to technology systems. According to a cybersecurity executive at a third-party logistics provider, companies need to strike a balance with efficient onboarding in an environment with high turnover and seasonal fluctuations.

2.3. Open-source Software

The widespread use of open-source software such as the Robot Operating System (ROS), commonly used to operate AMRs and other robots, increases the risk of malicious actors exploiting unpatched vulnerabilities or inserting malicious code. While there may be weaknesses with some open-source libraries, the widespread use and high visibility of popular open-source libraries like ROS means that the vulnerabilities within the system are usually well-known and publicized. According to a former engineer at an AMR provider, the development of ROS is still focused on research applications, and an enterprise-grade version similar to what was done with the Android operating system is needed to increase the robustness and security of the library.

For instance, the widely publicized Apache Log4j vulnerability in 2021 allowed attackers to exploit a flaw in a widely used open-source library, affecting everything from industrial control systems to internet applications (U.S. Cybersecurity and Infrastructure Security Agency 2022). Given that modern warehouses increasingly depend on both proprietary and open-source software solutions, ensuring robust cybersecurity measures is essential to prevent such incidents.

2.4. Integration Challenges

Integrating various systems—including the WMS, warehouse control and execution systems (WCS/WES), enterprise resource planning (ERP) systems, and others—presents a significant challenge in modern warehouses. This complexity becomes even more pronounced when different vendors supply these systems. The lack of standardization across the industry often

leads to compatibility issues, where certain warehouse technologies do not work seamlessly with others, which can result in unexpected operational failures. In the literature, Cheung, Bell, and Bhattacharjya (2021) note that gaps in software integration are common, leading to inefficiencies and system vulnerabilities.

As one interviewee from our research highlighted, there are frequent instances where "*certain warehouse technologies simply don't work with other solutions*," resulting in delayed implementations and lost productivity. This lack of standardization across warehouse systems creates major challenges, particularly for smaller companies that are more dependent on external technology providers. While larger firms may have the capacity to develop custom integration solutions, smaller firms may experience delays due to vendor prioritization, which can hinder their ability to implement automation technologies. Moreover, the need to coordinate multiple vendors for software updates and patches introduces another layer of complexity, leading to increased exposure to software vulnerabilities.

Sidebar 1: Denial of Service (DoS) Attack Impact on Warehouse Automation

A Denial of Service (DoS) attack occurs when a system is overwhelmed with excessive traffic or requests, rendering it unable to function properly. In warehouse automation, DoS attacks can cripple critical software systems like SaaS applications and Order Management Systems (OMS), leading to major operational disruptions. As described by the Chief Information Security Officer of a large warehouse automation solution provider, *"Overloading their SaaS application using a DoS attack would be the worst thing to happen."* This could halt fulfillment operations across multiple facilities, creating widespread chaos. Similarly, attackers could exploit the OMS by creating "fake orders" to overload the system, collapsing the service, and stopping all order processing. These attacks can bring warehouse operations to a standstill, affecting overall business continuity until the systems are restored.

Several companies in the study mentioned that they are working on developing a software interface platform that will allow them to plug and play various software solutions to facilitate

these integrations. One downside of this approach is that if the interface is compromised during a cyberattack, all the software might be affected.

Finally, during new acquisitions or mergers, one of the companies in the study reported a 200% increase in cyberattacks. This rise is attributed to the vulnerabilities introduced during these transitions as new systems, employees, and processes are integrated. The company mentioned that hackers exploit weaknesses in software security that may arise from these changes. New acquisitions may be targeted because they are often the weakest link in the security chain, and the integration process creates opportunities for malicious actors to gain access to sensitive software systems.

2.5. Dependency on Legacy Systems

Another persistent challenge in warehouse software management is the continued use of legacy systems, such as the AS-400, which still prevails in many industrial settings. Legacy systems, while often reliable, can be costly to upgrade and difficult to integrate with modern technologies. According to the literature, these older systems frequently lack the flexibility and scalability required by today's fast-paced, highly automated environments. This not only creates operational bottlenecks but also exposes the warehouse to significant security risks, as older systems may not be designed with modern cybersecurity in mind. As an example, the Chief Solutions Officer of an automation supplier highlighted that they have no encryption in their current automation solutions. The reason for this is that they send information through their own old protocol with only 8 bits, and encryption would require 32 bits. This shows how outdated systems struggle to adopt stronger security measures due to technical limitations, leaving operations more exposed to cyberattacks.

The participants also mentioned that AS-400, a mainframe system widely used in warehouses for inventory management and order fulfillment, can be difficult to integrate with newer cloud-based systems. Such integration challenges often require custom software solutions,

which increases both cost and the likelihood of bugs or vulnerabilities. Moreover, maintaining these legacy systems can strain IT resources, as older platforms may no longer receive updates or patches from the original vendors. This creates an environment where systems are more prone to cyberattacks due to unpatched vulnerabilities.

Furthermore, reliance on legacy systems can hinder a company's ability to adopt new automation technologies. These older systems may not be compatible with emerging warehouse software solutions, such as real-time analytics platforms or AI-driven inventory management tools, making it more difficult for companies to stay competitive in an increasingly automated industry.

2.6. Software Maintenance and Updates

The need for frequent updates in modern warehouse systems creates additional risk. As companies increasingly adopt cloud-based software solutions for their warehouse management systems (WMS) and other critical applications, they are subject to the schedules and processes of third-party vendors. Many providers, such as Blue Yonder and Körber, offer cloud-based solutions that rely on regular updates and patches (Blue Yonder, n.d.; Körber Supply Chain 2020). While cloud-based systems offer scalability and flexibility, they also expose companies to potential disruptions if an update introduces bugs or requires downtime, as occurred during a recent Microsoft Azure outage (Kunert 2023).

In some cases, software updates can introduce critical failures, as was the case with Tesla's recall of over 11,000 vehicles in 2021 due to a bug introduced through an over-the-air (OTA) update, which caused the vehicles to suddenly brake while in motion (Barry 2021). Warehouses that rely on OTA updates for their AMR fleets face similar risks, as a single flawed update could disrupt operations across multiple facilities where the robots are deployed. This risk is compounded by the increasing reliance on cloud-based services that require constant internet connectivity to ensure smooth operation. Disruptions in these services, such as AWS outages, have

already been shown to cause significant operational delays, data inaccessibility, and financial losses due to stalled warehouse automation (Moss 2021).

2.7. Antivirus and Other Security Software

The 2024 CrowdStrike incident when millions of Microsoft Windows operating systems crashed worldwide is an example of how an issue with antivirus and other security systems can cause operational disruptions on a large scale. In modern warehouse automation systems, antivirus software, which is intended to protect systems from malware, can itself become a critical vulnerability. One of the participants mentioned in the interview that most antivirus solutions are ineffective at handling Operational Technology (OT) traffic, which is common in warehouses. This creates a significant security gap, as traditional antivirus programs fail to address the specific needs of warehouse systems like Warehouse Management Software (WMS) and automated robotics. Furthermore, another participant mentioned that if an attacker targets the antivirus software itself, they could gain control over the robots it protects. The antivirus's high-level access makes it a key vulnerability, potentially opening the door for system-wide attacks, such as halting robotic operations if the antivirus fails or is compromised.

3. Automation Hardware

The adoption of advanced automation technologies in warehouse operations brings both opportunities and challenges. While more traditional automation systems, such as conveyor belts and cranes, are generally considered robust and low-risk, more advanced technologies like autonomous forklifts, AMRs, and collaborative robots ('cobots') introduce higher risks. Some interviewees suggested that the most critical vulnerabilities with warehouse technology systems, especially as they relate to cybersecurity, reside within the digital network and enterprise software systems. However, we identified multiple hardware-level vulnerabilities in both the literature and comments from many experts we interviewed. **The following vulnerabilities (represented by blue circles in *Figure 1*) have been identified within this category.**

Sidebar 2: AI Impact on Software Vulnerabilities

Artificial Intelligence tools can both improve and worsen software vulnerabilities. While AI is highly effective in detecting vulnerabilities, the participants also mentioned that it is becoming a powerful tool for hackers to automate the identification of weak points in warehouse software systems, leading to faster and more sophisticated attacks. If hackers use AI to scan systems and identify which automation tools a company is using, they can more easily exploit known vulnerabilities and compromise entire supply chain operations. Access to these systems is another risk. According to the senior vice president of a third-party logistics company, *"When systems are controlled by AI, who can access that central system is key. Tech providers should never have access."*

3.1. Sensor and Other IO Issues

Environmental factors, such as wet floors or extreme temperatures, can impact the performance of AMRs and similar systems, highlighting the need for robust and adaptable hardware solutions in the warehouse environment. According to a former engineer at an AMR provider, the biggest vulnerability with AMRs is mislocalization or poor navigation, which results in the device going where it shouldn't or collisions.

Highly automated warehouse systems require robust and precise hardware to prevent hazardous situations. According to an interview with a strategic advisor at an integration company, *"In modern cube storage systems, cobots run super close to each other, with a precision of millimeters. A slight movement might cause a collision. This can be an issue during natural disasters or simple maintenance procedures."*

One incident that illustrates this vulnerability is a fire in a highly automated Ocado warehouse caused by a performance failure: in this case, the collision of three robots. The company had previously improved the safety systems after an earlier fire, and only a certain part of the grid was affected. Nonetheless, this new incident led to the cancellation of approximately 300,000 customer orders due to the automation system being shut down for several days, which resulted in an estimated £35 million (approximately $45 million) in lost sales. In addition to the lost sales, Ocado confirmed additional operating losses of about £10 million as the site ramped back up to full capacity. Finally, the impact of stock and fixed asset write-offs and other incremental costs associated with the fire was estimated at around £10 million (Digital Commerce 360 2021).

3.2. Battery and Charging Device Failures

More rigid automation systems, such as grid-based AS/RS, present new risks as well. For instance, the density of flammable inventory, plastic totes, and other materials within these systems increases the risk of fire. At the same time, fire suppression standards often lag behind technological advances, and local fire departments often lack expertise in managing these high-tech environments. This disparity increases the potential for catastrophic losses in the event of a fire., *"Battery-powered cobots running on a metal grid increase the risk of a fire starting. Moreover, fire suppression systems don't work as well in high-density systems that often also use plastic totes."*

Another fire in 2019 at a cube-storage (grid-based AS/RS) warehouse operated by Ocado illustrates these vulnerabilities well. This fire was caused by a defect in a robot's charging unit

(Ocado Group 2021). Multiple vulnerabilities led to the final outcome. First, an electrical fault in a battery-charging unit of one of the thousands of robots caused the plastic lid on the robot to ignite; second, the grid continued to operate while the fire spread (Baker 2018); and third, the fire-detection system failed, allowing the fire to spread throughout the facility (Cante 2021). Warehouse operators manually reported the fire and activated the sprinkler system, but the fire ultimately burned for four days, damaging most of the facility and its contents (Beioley 2019). Fortunately, the fire did not result in any injuries or fatalities, but more than 370 workers were laid off, and it took two years to rebuild the facility at a cost of £100 million (approximately $130 million). (Ocado Group 2021; Rovnick 2019; BBC 2021).

After the incident, FM Global, the insurance company that covered the expenses resulting from the Ocado fire (Bradshaw and Dalton 2019), highlighted the vulnerabilities that created specific fire risks associated with these highly automated systems. These included: (1) the use of plastic totes within highly automated, high-density storage systems, which can burn much more severely than cardboard or wooden containers; (2) high storage density, which facilitates the rapid spread of fire and leaves limited space for sprinkler water to flow down through the grid, where the water is most needed; and (3) an inadequate automation-shutdown protocol (Baker 2018).

3.3. Lack of Hardware Maintenance

Mechanical failures in hardware components like robots, shuttles, cranes, and robotic arms can significantly disrupt operations. Maintenance and the availability of spare parts are additional key factors in minimizing hardware downtime in highly automated warehouses, especially when comparing one large facility to multiple small facilities. With multiple small, highly automated warehouses, the challenge of ensuring immediate support increases since each site might not have the specialized talent or spare parts on hand. This dispersed setup raises the risk of extended downtime if a critical component fails. Proactive maintenance—through regular system checks

and fast fault identification—becomes even more essential, as minor issues can quickly cascade into major operational disruptions.

Standardization across all warehouses is another key to overcoming these challenges. By using uniform tools, inventory, and system designs (such as identical electrical connections, color codes, and hardware configurations for all automation equipment in the warehouse), maintenance personnel can efficiently resolve issues regardless of the location. This consistency minimizes downtime by enabling technicians to swiftly identify and fix problems, even when unexpected incidents occur—like a small sensor misalignment halting a conveyor. Ultimately, robust standardization, proactive maintenance, and well-trained staff are vital to sustaining the high efficiency of automated warehouses.

3.4. Automation Rigidity

Automation rigidity in highly automated warehouses poses a significant vulnerability, as highlighted by various industry experts. Fully automated systems, while efficient, lack flexibility. If a part of the system fails—such as an autonomous robot or conveyor—the entire facility might stop, as seen in cases where rigid automation systems couldn't quickly switch to manual operations. This issue is particularly evident in high-density systems, where, as a VP of Supply Chain Strategy in retail stated, *"Most high-density systems such as ASRS, OSR, and Cube Storage, when something fails, you have to stop completely and cannot operate."* This vulnerability is exacerbated by the increasing complexity of integrating multiple automation technologies, which makes these systems harder to troubleshoot or recover from failures quickly, particularly in scenarios involving critical infrastructure like warehouses.

3.5. Hardware Security Measures Needed

Vulnerabilities exist with the hardware necessary for information technology systems as well. For instance, in October of 2023, the retail cooperative Ace Hardware was hit with a cyberattack that disrupted its warehouse distribution network right before the critical holiday shopping season in the U.S. (HBSDealer 2023a). The cyberattack compromised servers running the warehouse management system (WMS) (HBSDealer 2023a). This prevented the company's distribution centers from fulfilling online orders and replenishing retail store inventories for weeks.

There are examples of attacks on other hard devices as well. The Mirai botnet in 2016 was a cyberattack that affected millions of digital video recorders, routers, and closed-circuit television cameras. The Persirai botnet in 2017 affected over six hundred thousand Internet Protocol cameras. Botnet attacks hijack a device and deploy it for use in a network that is then used for other attacks. The

Sidebar 3: Dependence on Technology Providers

A common sentiment shared by interviewees was that many companies lack knowledge of their technology-related vulnerabilities and do not have the capability to mitigate the associated risks, especially related to cybersecurity and new warehouse technologies. Many of the new technologies being deployed in warehouses — from AMRs to cube storage — are vastly different from the radio frequency scanners and conveyor belts that companies previously worked with. As a result, many of the individuals we interviewed said their companies are dependent on technology providers.

Even companies with more advanced in-house capabilities will rely on external providers to a certain degree. This makes vendor selection and management a key strategic challenge. Many technology providers may prioritize getting solutions to market quickly, sometimes at the expense of robust cybersecurity measures. This can be especially common among startups and companies focusing on rapid innovation.

Moreover, financial stability and the availability of reliable customer service and support, especially for small overseas providers, are critical considerations. According to an automation consultant, *"There is a huge risk around the role of service and support in the successful implementation and ongoing operation of automation technologies. A new small supplier may go out of business tomorrow… what do I do if that happens?"*

BrickerBot attack in 2016, in contrast, attacked similar devices but with the intention of destroying the device (Boddy and Shattuck 2017).

3.6. Malicious Hardware Alteration/embedding

Based on a study by Véronneau and Roy (2014) about securing supply networks at the source, modern warehouse technologies, including robotics, AMRs, and IoT devices, could be compromised in the upstream supply chain, where the software and hardware are manufactured or assembled by vendors. Malicious additions or modifications, such as hardware trojans, can be used to modify the output value of these circuits (Lacava et al. 2021; Ramadan 2021). Plosz and Varga (2018) found that the hardware (sensors and actuators) is the most vulnerable layer in vision-based AGVs and AMRs, and is potentially subject to hardware tampering, vision manipulation, device displacement, and jamming of global positioning system (GPS) signals. Drones are vulnerable to intentional sabotage of their hardware components as well (Yaacoub et al. 2020). These vulnerabilities are compounded by the complexity of hardware supply chains. Moreover, most AMR providers acknowledge that their systems are manufactured in China, which may introduce additional risks as geopolitical tensions escalate between the West and BRICS nations.

3.7. Physical Size of Equipment

Safety concerns are paramount with these new technologies. The absence of protective cages around many systems (e.g., AMRs) and issues related to power sources were reported as significant potential safety hazards. The physical size of equipment is an important consideration for safety as well. Many interviewees discussed the risks associated with new autonomous forklift technologies, both due to the complexity of control and navigation systems as well as the physical size of the forklift and the materials it handles.

4. Digital Network Infrastructure

Historically, warehouse systems operated on local servers with minimal emphasis on network security. However, the shift to modern, interconnected systems often operated in separate infrastructure provided by third parties ('cloud services') has exposed warehouses to new vulnerabilities.

The industry-wide impact of major cyberattacks, such as NotPetya in 2016, has underscored the critical importance of comprehensive cybersecurity measures. The NotPetya attack began after hackers broke into the computers of a little-known Ukrainian company (Intellekt Servis) that makes the country's most popular tax software, M.E. Docs. The hackers infected the software with a malicious virus ("NotPetya") that looked like ransomware but had no means of decrypting files, so it was meant to cause damage rather than extort money. (McMillan 2017) Other victims of the attack include FedEx's TNT courier operations in Europe, the French construction giant Saint Gobain, pharmaceutical giant Merck & Co., and the law firm DLA Piper. In total, the monetary damages of the attack are estimated to be as much as $10 billion (Greenberg 2018).

Cyberattacks affecting the broader supply chain and industrial context have increased dramatically since NotPetya, and are one of the main intentional, exogenous disruptions firms need to be aware of (World Economic Forum 2023). According to Accenture, one-third of attempted cyberattacks are successful, with large firms receiving more than a hundred attempted attacks each year on average (Accenture 2016). **The following vulnerabilities (represented by yellow circles in**

***Figure 1*) have been identified within this category.**

4.1. Migration to the Cloud

The transition to the cloud involves the WMS and other enterprise systems as well as systems that directly control automation hardware. According to a former engineer at an AMR technology provider, the industry is moving toward an architecture where navigation and

optimization capabilities are processed in separate control systems (i.e., 'offboard' systems not operating on the AMR). This allows new and more complex computing capabilities due to the greater processing power outside of the AMR device. However, many of these systems are currently operating in, or are moving to, the cloud with the associated vulnerabilities.

While cloud-based software reduces the burden on in-house teams and the capital investment in computer hardware, it introduces new risks related to system integration, information transmission over the internet, vendor lock-in, loss of control over update schedules, and the need to ensure operational continuity during network outages or cloud service interruptions. According to an IT Consultant we interviewed, *"As more systems integrate with cloud technologies, the potential for cyberattacks increases. This includes both direct and indirect attacks."*

For example, in November 2024, a ransomware attack on supply chain software provider Blue Yonder caused significant disruptions to major companies like Starbucks and Morrisons. Starbucks faced small difficulties in

Sidebar 4: Cloud Supply Chains and the Tech Industry

As companies shift from on-premise hardware to cloud solutions, this concentration further centralizes critical supply chain operations. Most of the cloud infrastructure is concentrated in the hands of three major providers—Amazon, Microsoft, and Google—leading to concerns about over-reliance on a few dominant players. Moreover, the supply chains of the major cloud-hardware technology companies like Apple, Dell, HP, Intel, AMD, and NVidia remain largely opaque, with little public information available about their warehouse operations.

Most of these companies outsource their logistics operations, relying heavily on 3PLs to transport and store cargo. This means most of these companies own none or very few warehouses. Specifically, the 3PLs World Wide Technology (WWT) and Logistics+ play significant roles in managing the supply chains for major cloud providers. WWT operates large integration centers across the U.S., the Netherlands, India, and Singapore, with 5 million square feet of physical warehouse and integration space. Logistics+, on the other hand, manages 8 million square feet of warehouse space in the U.S. alone, with additional facilities in Mexico, South America, Europe, and Asia.

managing employee schedules and tracking work hours. Meanwhile, Morrisons experienced the disruption of its WMS for fresh food and produce, which required them to go back to manual operations in most warehouses and rebuild their WMS. This incident underscores the vulnerabilities inherent in cloud-based services and the critical need for robust cybersecurity measures and contingency plans to address such risks.

The cloud also brings new challenges with regulatory compliance. Dubai's local data storage mandate and the European Union's General Data Protection Regulation (GDPR) are two examples of complex regulations that global operations face. The lack of corporate standards in these areas leaves organizations vulnerable as they transition to new systems and digital network infrastructure.

4.2. Integrations Between Systems Increase the Attack Surface

Similar to the use of cloud services, the interconnectivity of systems, while beneficial for operations, expands the attack surface and increases vulnerability. Cyberattacks on the WMS or WES can be particularly destructive, given their central role in controlling the warehouse operation and, in the case of the WES, controlling physical automation within warehouses. These systems are increasingly connected to other enterprise systems within the company, as well as external systems operated by carriers, third-party logistics companies, and other supply chain partners.

This risk is particularly significant for smaller companies, which may lack comprehensive cybersecurity measures, increasing the potential for cyberattacks to spread through the supply chain (Kellermann and McElroy 2021). Emerging models such as Robotics-as-a-Service (RaaS) offer advanced capabilities but also heighten dependency on smaller warehouse suppliers. While these smaller entities are adopting RaaS technologies rapidly, many are still in the early stages of addressing IT security requirements, potentially exposing interconnected systems to greater risks

This is why a company's supply chain is often perceived to be a cybersecurity weakness (Melnyk et al. 2022). According to a cybersecurity executive at a third-party logistics provider, the

most likely target for a cyberattack is one step away from the primary target. A primary target, such as the WMS, will have more eyes on it and more robust security measures in place. The secondary target, in contrast, will likely be easier to compromise, and given the interconnectedness of supply chain systems, gain an access point to the network with the goal of ultimately attacking or accessing the primary target.

Sidebar 5: Common Cybersecurity Capabilities and Best Practices

1. Role-based user access control with strong password requirements, single sign-on, and multifactor authentication.
2. Reverse-proxying: A reverse proxy can block common attacks such as SQL injection and denial of service (DoS) before they reach the backend servers.
3. Single-direction communication to ensure commands to automation systems are sent through one channel, while the response comes back through a different channel.
4. Encrypting and anonymizing all data transmitted between systems (e.g., WMS, OMS, TMS, ERP, etc.).
5. Incorporate cybersecurity into employee training.
6. Encourage technology providers and clients to be transparent in communicating cybersecurity issues.

4.3. Network Security at the Device Level

Cyberattacks could target the network layer of autonomous devices and other physical systems within the warehouse as well. According to VMware, 27% of cyberattacks exploited IoT vulnerabilities in 2020, and 17% of security practitioners believed IoT exposure to be one of the most "daunting endpoint security challenges" (Kellermann and McElroy 2020). These devices often lack robust cybersecurity measures and provide access points to the company's network (Sarder and Haschak 2019; Ramadan 2021). Gil et al. (2017), for example, demonstrate in a laboratory setting how the coordination of multi-robot networks, such as drone fleets, can be disrupted by a malicious agent that gains undue influence in the network by generating or spoofing a large number of requests

('Sibyl attack'). Similarly, Khalid et al. (2018) found that attacks on collaborative cyber-physical and robotic systems, such as a vehicle operated by a drive-by-wireless system, are most likely to occur in the system's network layer.

With AMR and other warehouse automation technology, there are two or more channels that connect the device with technology providers and other external sources. A forward channel from the external source to the device is used for maintenance and updates, and a backward channel from the device to the external source is used for performance monitoring and analytics. According to a former engineer at an AMR provider, there are typically robust security measures in place for the forward channel due to the nature of access from an external source inside the warehouse. This channel, however, is the most likely vector for what they consider the worst-case scenario for AMR and similar technology systems where the technology provider is attacked and downstream customer systems are compromised through this forward channel.

To mitigate these risks, companies are pursuing a variety of strategies — including encryption, firewalls, network segmentation, and other measures — but many organizations still lack the appropriate infrastructure to protect their networks. The use of Virtual Private Network (VPN) tunnels for secure connections to automation technology was reported to be a common practice. Encryption practices among technology providers, on the other hand, sometimes focus more on vendor lock-in than protection against cyberattacks. At the network level, some companies are implementing hybrid approaches, combining cloud and edge computing to balance scalability, operational efficiency, and security. However, many cybersecurity measures were developed for cyber-only systems and cannot be effectively applied to modern warehouse cyber-physical and robotic systems (Khalid et al. 2018).

5. Physical Infrastructure

One of the most common concerns expressed by experts in the warehouse technology space was the reliance on reliable power supply and network connectivity. The increasing reliance on

automated systems has made warehouses vulnerable to power outages and network failures. Electricity and communications connectivity can be disrupted by a variety of sources, including sabotage, fire, natural disasters, and others. The sentiment shared by the CEO of a technology provider is that *"the robustness of the U.S. power grid is questionable."* According to the vice president of customer experience at a CPG company, *"This year, we had to stop operations in 2 of our warehouses: once due to iced rain that destroyed the grid connection and the other when we lost [access to] the Internet."*

Essentially all automation technology depends on electrical power, and network connectivity is equally crucial. Automated systems like AMRs and AS/RS depend on communication with control systems that receive information from cloud-based or other systems connected through the internet. The physical layout of modern warehouses, particularly those utilizing high-density robotic systems, introduces its own set of challenges. These systems are often difficult or impossible to operate manually during outages. In some cases, the inventory within the facility is inaccessible without power and network connectivity. **The following vulnerabilities (represented by green circles in *Figure 1*) have been identified within this category.**

5.1. Power Connectivity

The risks associated with power connectivity include natural disasters and other events that can disrupt the grid. It also includes intentional attacks by malicious actors (Brown 2018). Drawing parallels with vulnerabilities found in other industries, the Aurora attack on electric power generators was a high-profile example of an attack that exploits a vulnerability in the protection mechanism and can be initiated by gaining physical access to the generator (Zeller 2011). The impact of power outages in warehouses can be substantial and has been modeled by Ivanov (2022) at different levels of the supply chain, including upstream and downstream central distribution centers (CDC) and regional distribution centers (RDC).

5.2. Network Connectivity

Modern warehouses rely on fast network connectivity, mainly a robust fiber-optic backbone, to ensure high bandwidth, low latency, and secure data transmission, but 5G networks are increasingly present to support robot operations (Das et al., 2022). Cloud computing is an essential part of the warehouse digital environment and offers numerous benefits. It also brings the vulnerability associated with continuous, reliable network connectivity. Many types of modern warehouse automation equipment, such as AMRs and cobots, rely on the cloud for real-time data transfer and low-latency connectivity, so that the robots can make adjustments on the fly and coordinate with each other (Kembro and Norrman 2022). Ocado's grid solution is a perfect example of this, as its central system runs in the AWS cloud for better scalability and speed. One potential drawback of this system architecture is the reliance on cloud connectivity without on-premise redundancy (Collins 2022). Thus, disruptions such as the recent Microsoft Azure (Kunert 2023) and AWS power issues (Moss 2021) could severely affect modern

Sidebar 6: Pharmaceutical Sector Leading in Redundancy and Business Continuity Planning (BCP)

The modern warehouse faces a complex landscape of challenges that requires strategic planning and adaptation. As warehouses progress toward full automation and AI deployment, there's a growing recognition of the need for robust business continuity plans. Some companies have manual fallback options for their facilities in case of system failures, highlighting the importance of maintaining operational resilience in the face of technological disruptions. The pharmaceutical sector stands out for its rigorous security and continuity standards, employing a high-availability approach with triple redundancy in critical systems. For example, some pharmaceutical companies safeguard their warehouse systems with three copies: a local host, their own server, and a cloud backup. Special firewalls also create barriers between data and automation to enhance security. In terms of power and connectivity, pharmaceutical firms mentioned that their warehouses are designed to withstand disruptions with dual grid access points, uninterruptible power supplies (UPS), backup diesel generators, and dual network access via different telecom providers (such as AT&T and Verizon), supplemented by LTE or 5G.

warehouse operations by causing automation halts that lead to operational delays, data inaccessibility, and financial losses due to trapped inventory.

Some of the participants stated that their facilities have backup power solutions such as diesel generators and Uninterruptible Power Supply (UPS) systems, although these often only serve as a temporary solution to maintaining full operations during extended outages. For network connectivity, few companies employ multi-layered connectivity strategies, including the use of multiple telecommunications providers and even satellite-based solutions. However, the interdependence of power and network systems means that a failure in one can render the other ineffective, highlighting the need for comprehensive contingency planning.

5.3. Facility Access Security Needed

Physical security also remains a concern, with some experts noting the ease with which unauthorized individuals could potentially access facilities. Physical access to a facility then compromises both the physical assets as well as the software and network systems that have exposed interfaces within the facility. According to an assessment of over 130 industrial control systems (ICS) by the U.S. Department of Homeland Security, 'physical access control' was one of the top vulnerabilities in general industrial settings (Hemsley and Fisher 2018). A cybersecurity executive at a third-party logistics provider shared this sentiment as well, saying that the physical security of a warehouse is the biggest risk where an intruder can have the greatest impact with the least effort. This highlights the need for stringent physical access controls and security measures to protect both physical and digital assets in the warehouse.

6. Human-Machine Interaction

The integration of new technologies in warehouses brings unique challenges to human-machine interactions. Autonomous robots like AMRs introduce varying degrees of risk to human safety, with larger robots like robotic arms and autonomous forklifts posing more significant

dangers. According to Evans (2020), there was a positive correlation between the injury rate and the level of automation used in the warehouses operated by Amazon. Their analysis was based on public reports and databases provided by the U.S. Occupational Safety and Health Administration (OSHA), to which all accidents that result in an injury or casualty must be reported in the U.S. Moreover, research has shown that warehouse workers are less attentive when working with robots and other technologies (Cymek, Truckenbrodt, and Onnasch 2023), which can lead to accidents in the workplace and other operational disruptions. This shift requires a reevaluation of safety measures and protocols. **The following vulnerabilities (represented by purple circles in *Figure 1*) have been identified within this category.**

6.1. Human-machine Proximity

According to Massachusetts-based Hanover Insurance Group Inc., human-machine proximity is a common issue with robotics and other automation. The lack of collision-prevention systems, whether it be a floor sensor, guardrail, or virtual fencing around the robot, can lead to accidents. These situations are more typical during non-routine tasks, such as during maintenance or updates being made to the robot (Wilkinson 2022). In December 2018, an accident occurred at a retailer's warehouse in Robbinsville, New Jersey, when a robot accidentally punctured a can of bear repellent, which led to the hospitalization of 24 workers. The incident raised concerns about the safety protocols in automated warehouses and the potential hazards of robots working alongside human employees (Youn 2018). According to the human-robot interaction (HRI) risk levels introduced by Bdiwi, Pfeifer, and Sterzing (2017), modern warehouses with AMRs or collaborative robots should be classified at the highest level (4), where physical HRI is necessary to fulfill a warehouse task. In most e-commerce warehouses, for instance, AMRs can either bring totes to humans who are located near storage shelves or can move mobile shelves, so that workers can pick up products and place them in the robot or shelves before the robot moves to a different position (Boysen and de Koster 2024).

6.2. Employee Turnover

Human factors remain a primary concern in warehouse operations. High employee turnover rates lead to a loss of operational knowledge over time, and insufficient training can result in unsafe practices. The complexity of modern warehouse systems necessitates continuous training and simulation exercises, but high turnover rates and operational demands (e.g., peak season in retail) often hinder these efforts. According to a director of human resources at a retail company, *"We are afraid of warehouse operations knowledge not being transmitted as everything becomes automated (physically and digitally). What if something goes wrong and we have to go back to manual?"* Another expert added, *"The training is a huge risk because these facilities can't stop to simulate mitigation actions [so they only do it once a year]… but there is a huge turnover rate, so a lot of people miss that because they only stay in the company for a few months."* This constant churn means that crucial operational knowledge can be lost, leaving new employees unprepared to handle complex automated systems.

Another example highlights the risks associated with untrained workers resorting to unsafe workarounds. Companies agreed that employees tend to bypass standard procedures to quickly address issues when they lack expertise, potentially causing damage to equipment and increasing operational risks. This challenge becomes even more difficult with high employee turnover, as more workers lack adequate training or experience with the technology.

6.3. Lack of Technology Acceptance

The perception of technology among workers is also critical. A cultural shift towards accepting automation is essential for successful implementation, especially in highly automated environments where human involvement is minimized. The Director of Fulfillment Automation of a 3PL noted, *"Another main risk is how people perceive technology. There needs to be a cultural shift or it won't work."* The participants agreed that resistance to change will lead to improper use or avoidance of automation tools, as noted in another example brought up by the former Software

Director of an automation supplier: *"Companies are not aware of the new risks. [If they are not accepting the technology] An employee can break a robot as an excuse to avoid working. 'My robot is not working, I can't work.'"*

To address these challenges, companies are shifting their focus toward managing the complex interplay between humans and machines, ensuring proper training, maintaining operational knowledge, and fostering a culture that embraces technological advancements while recognizing the continued importance of human expertise and oversight. These measures are crucial as companies navigate the balance between automation and human oversight.

Conclusion

The transition to highly automated and technologically advanced warehouse operations presents a complex array of vulnerabilities to disruption. A total of 26 technology-related vulnerabilities have been identified in this research project, classified into 6 groups. An additional contribution has been the connection of these 26 warehouse vulnerabilities with five main disruptions, as *Figure **1*** shows. Finally, the analysis of over 200 articles, 30 interviews with relevant industry actors (including 3PLs, CPGs, retail, and warehouse technology providers), 3 focus groups with subject matter experts, and 5 site visits conducted during this research project reveals several key findings:

1. **Cybersecurity and data management** have emerged as critical concerns, particularly as warehouses increasingly rely on cloud-based systems, integrated systems, and Robotics-as-a-Service. The need for robust, standardized security practices is paramount, including for smaller companies adopting new technologies that may present an access point for cyberattacks on the supply chain network.

2. **Software integration and legacy system** upgrades pose significant challenges, often leading to implementation issues and operational disruptions. The industry must address the growing complexity of connecting various systems while ensuring operational continuity.

3. Implementing **advanced hardware**, such as AMRs and grid-based 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.

4. Highly automated warehouses and their surrounding **physical infrastructure** are intrinsically linked. Automation technologies' dependence on reliable power and network connectivity necessitates robust backup systems and comprehensive continuity plans.

5. **Human factors** remain crucial despite increasing automation. High turnover rates and the need for specialized training present ongoing challenges, highlighting the importance of effective knowledge management and skills development programs.

6. **Strategic approaches** to technology adoption, vendor management, and risk mitigation are evolving. Companies are increasingly focusing on building redundancy, developing in-house detection and mitigation capabilities, and maintaining flexibility in their operational strategies.

The modern warehouse's path toward increased automation and technological sophistication requires a multifaceted approach to risk management. 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.

Future success will depend on developing comprehensive strategies that address cybersecurity, operational resilience, human capital development, and adaptive infrastructure. This research project underscores the need for ongoing research and collaboration within the industry to address emerging challenges and capitalize on new opportunities. As warehouses become increasingly central to global supply chains, their ability to navigate these complex issues will play a pivotal role in shaping the future of logistics and commerce.

References

Accenture. 2016. "Building Confidence: Facing the Cybersecurity Conundrum." https://newsroom.accenture.com/news/2016/accenture-survey-one-in-three-cyberattacks-result-in-a-security-breach-yet-most-organizations-remain-confident-in-their-ability-to-protect-themselves.

Baker, Weston. 2018. "Protect Your Warehouse From Emerging Fire Risks." FM Global. April 12, 2018. https://www.fmglobal.com/insights-and-impacts/2018/automated-warehouse-fire-protection.

Barry, Keith. 2021. "Tesla Full Self-Driving Software Recall for Phantom Braking." *Consumer Reports*, November. https://www.consumerreports.org/cars/car-recalls-defects/tesla-recall-full-self-driving-software-phantom-braking-a5626328806/.

BBC. 2021. "Ocado Warehouse Fire Rebuilt Andover Centre Fully Operational," August. https://www.bbc.com/news/uk-england-hampshire-58190969.

Beioley, Kate. 2019. "Robot Electrical Fault Blamed for Ocado Warehouse Fire." *Financial Times*, April. https://www.ft.com/content/d22d1298-683e-11e9-a79d-04f350474d62.

Bdiwi, Mohamad, Marko Pfeifer, and Andreas Sterzing. 2017. "A New Strategy for Ensuring Human Safety during Various Levels of Interaction with Industrial Robots." *CIRP Annals - Manufacturing Technology* 66 (1): 453–56. https://doi.org/10.1016/j.cirp.2017.04.009.

Blue Yonder. n.d. "Future-Proofing Your Transportation Management System." Accessed September 19, 2024. https://blueyonder.com/it-it/resources/future-proofing-your-transportation-management-system.

Boddy, Sara, and Justin Shattuck. 2017. "The Hunt for IoT: The Rise of Thingbots." *F5 Labs*, August. https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot-the-rise-of-thingbots.

Boysen, Nils, and René de Koster. 2024. "50 Years of Warehousing Research—An Operations Research Perspective." *European Journal of Operational Research*. https://doi.org/10.1016/j.ejor.2024.03.026.

Bradshaw, Gavin, and Rachel Dalton. 2019. "FM Global Faces £100mn Property Loss from Ocado Warehouse Fire | Insurance Insider." Insurance Insider. February 15, 2019. https://www.insuranceinsider.com/article/2876h63r4zcvj1yxz3h1c/fm-global-faces-100mn-property-loss-from-ocado-warehouse-fire.

Brown, Nick. 2018. "Puerto Rico Power Utility Hacked but Customer Data Not at Risk." Reuters. March 18, 2018. https://www.reuters.com/article/us-usa-puertorico-cyberattack/puerto-rico-power-utility-hacked-but-customer-data-not-at-risk-idUSKBN1GV30A/.

Cante, Lorena Cifuentes. 2021. "Verifying Fire Safety of Top-Load Storage and Retrieval System: A Case Study." Ghent University. https://imfse.be/s/Thesis-Lorena-Cifuentes_Ghent.pdf

Cheung, Kam-Fung, Michael G.H. Bell, and Jyotirmoyee Bhattacharjya. 2021. "Cybersecurity in Logistics and Supply Chain Management: An Overview and Future Research Directions."

Transportation Research Part E: Logistics and Transportation Review 146:102217. https://doi.org/10.1016/j.tre.2020.102217.

Collins, Jon. 2022. "How Ocado Migrated Its On-Premise Robotic Control System to AWS Outpost on Christmas Eve." *Diginomica*. January 14, 2022. https://diginomica.com/how-ocado-migrated-its-premise-robotic-control-system-aws-outpost-christmas-eve.

Crowe, Steve. 2021. "Locus Robotics Scaling AMR Deployments with DHL Supply Chain." The Robot Report. June 2, 2021. https://www.therobotreport.com/locus-robotics-scaling-amr-deployments-dhl/.

Cybersecurity and Infrastructure Security Agency. 2022. "Apache Log4j Vulnerability Guidance," April. https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance.

Cybersecurity and Infrastructure Security Agency. 2023. "Protecting Against Malicious Use of Remote Monitoring and Management Software." January 23, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a.

Cymek, Dietlind Helene, Anna Truckenbrodt, and Linda Onnasch. 2023. "Lean Back or Lean in? Exploring Social Loafing in Human–Robot Teams." *Frontiers in Robotics and AI* 10:1249252. https://doi.org/10.3389/frobt.2023.1249252.

Das, Ashok Kumar, Sandip Roy, Eranga Bandara, and Sachin Shetty. 2022. "Securing Age-of-Information (AoI)-Enabled 5G Smart Warehouse Using Access Control Scheme." *IEEE Internet of Things Journal* 10(2): 1358-1375. https://doi.org/10.1109/JIOT.2022.3140463.

Dieber, Bernhard, Benjamin Breiling, Sebastian Taurer, Severin Kacianka, Stefan Rass, and Peter Schartner. 2017. "Security for the Robot Operating System." *Robotics and Autonomous Systems* 98:192–203. https://doi.org/10.1016/j.robot.2017.09.017.

Evans, Will. 2020. "How Amazon Hid Its Safety Crisis." *Reveal*, September. https://revealnews.org/article/how-amazon-hid-its-safety-crisis/.

Gil, Stephanie, Swarun Kumar, Mark Mazumder, Dina Katabi, and Daniela Rus. 2017. "Guaranteeing Spoof-Resilient Multi-Robot Networks." *Autonomous Robots* 41 (6): 1383–1400. https://doi.org/10.1007/s10514-017-9621-5.

Gioia, Dennis A., Kevin G. Corley, and Aimee L. Hamilton. 2013. "Seeking Qualitative Rigor in Inductive Research." *Organizational Research Methods* 16 (1): 15–31. https://doi.org/10.1177/1094428112452151.

Greenberg, Andy. 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*, September 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

HBSDealer. 2023 (a). "Ace Hardware Hit with Cyber Breach HBS Dealer," October 30, 2023. https://hbsdealer.com/ace-hardware-hit-cyber-breach.

HBSDealer. 2023 (b). "Ace Says Systems Are Restored HBS Dealer," November 6, 2023. https://hbsdealer.com/ace-says-systems-are-restored.

Hemsley, Kevin E., and Ronald E. Fisher. 2018. "History of Industrial Control System Cyber Incidents." *Idaho National Laboratory*. https://doi.org/10.2172/1505628.

Hollerer, Siegfried, Clara Fischer, Bernhard Brenner, Maximilian Papa, Sebastian Schlund, Wolfgang Kastner, Joachim Fabini, and Tanja Zseby. 2021. "Cobot Attack: A Security Assessment Exemplified by a Specific Collaborative Robot." *Procedia Manufacturing* 54:191–96. https://doi.org/10.1016/j.promfg.2021.07.029.

Ivanov, Dmitry. 2022. "Blackout and Supply Chains: Cross-Structural Ripple Effect, Performance, Resilience and Viability Impact Analysis." *Annals of Operations Research*, 1–17. https://doi.org/10.1007/s10479-022-04754-9.

Kellermann, Tom, and Rick McElroy. 2020. "COVID-19 Continues to Create a Larger Surface Area for Cyberattacks." *VMware*. See the files provided in the project Dropbox.

Kellermann, Tom, and Rick McElroy. 2021. "Global Incident Response Threat Report." *VMware*. See the files provided in the project Dropbox.

Kembro, Joakim, and Andreas Norrman. 2022. "The Transformation from Manual to Smart Warehousing: An Exploratory Study with Swedish Retailers." *The International Journal of Logistics Management* 33 (5): 107–35. https://doi.org/10.1108/ijlm-11-2021-0525.

Khalid, Azfar, Pierre Kirisci, Zeashan Hameed Khan, Zied Ghrairi, Klaus-Dieter Thoben, and Jürgen Pannek. 2018. "Security Framework for Industrial Collaborative Robotic Cyber-Physical Systems." *Computers in Industry* 97:132–45. https://doi.org/10.1016/j.compind.2018.02.009.

Khalid, Azfar, Zeashan Hameed Khan, Muhammad Idrees, Pierre Kirisci, Zied Ghrairi, Klaus-Dieter Thoben, and Jürgen Pannek. 2022. "Understanding Vulnerabilities in Cyber Physical Production Systems." *International Journal of Computer Integrated Manufacturing* 35 (6): 569–82. https://doi.org/10.1080/0951192x.2021.1992656.

Körber Supply Chain. 2020. "Cloud Solutions." https://koerber-supplychain.com/fileadmin/koerbersupplychain/Homepage/Downloads_NEU/FS_Cloud-solutions_EN.pdf.

Kumar, Subodha, and Rakesh R. Mallipeddi. 2022. "Impact of Cybersecurity on Operations and Supply Chain Management: Emerging Trends and Future Research Directions." *Production and Operations Management* 31 (12): 4488–4500. https://doi.org/10.1111/poms.13859.

Kunert, Paul. 2023. "Microsoft Admits 'power Issue' Downed Azure Services in West Europe." The Register. October 23, 2023. https://www.theregister.com/2023/10/23/microsoft_azure_power_issue/.

Lacava, Giovanni, Angelica Marotta, Fabio Martinelli, Andrea Saracino, Antonio La Marra, Endika Gil-Uriarte, and Victor Mayoral-Vilches. 2021. "Cybsersecurity Issues in Robotics." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 12 (3): 1–28. https://doi.org/10.22667/jowua.2021.09.30.001.

McMillan, Robert. 2017. Cyberattack Launched for Pain, Not Profit, Experts Say. *The Wall Street Journal*, June 29, 2017. https://www.wsj.com/articles/cyberattack-launched-for-pain-not-profit-experts-say-1498771601.

Mayring, Philipp. 2019. "Qualitative Content Analysis: Demarcation, Varieties, Developments." *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research* 20 (3). https://doi.org/10.17169/fqs-20.3.3343.

Melnyk, Steven A., Tobias Schoenherr, Cheri Speier-Pero, Chris Peters, Jeff F. Chang, and Derek Friday. 2022. "New Challenges in Supply Chain Management: Cybersecurity across the Supply Chain." *International Journal of Production Research* 60 (1): 162–83. https://doi.org/10.1080/00207543.2021.1984606.

Moss, Sebastian. 2021. "Data Center Power Loss Brings down AWS Services, in Another East Coast Cloud Outage." Data Centre Dynamics Ltd. December 22, 2021. https://www.datacenterdynamics.com/en/news/aws-has-another-east-coast-cloud-outage/.

Ocado Group. 2021. "Rising from the Ashes and Returning to the Community: Two Years on from the Andover Fire." *Ocado Group*, February. https://www.ocadogroup.com/media/newsroom/rising-ashes-and-returning-community-two-years-andover-fire

Plosz, Sandor, and Pal Varga. 2018. "Security and Safety Risk Analysis of Vision Guided Autonomous Vehicles." *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, 193–98. https://doi.org/10.1109/icphys.2018.8387658.

Ramadan, Rabie A. 2021. "Internet of Things (IoT) Security Vulnerabilities: A Review." *PLOMS AI*. https://plomscience.com/journals/index.php/PLOMSAI/article/view/14.

Rovnick, Naomi. 2019. "Ocado Warns Fire at Flagship Warehouse Will Hit Sales Growth." *Financial Times*, February. https://www.ft.com/content/ba55f476-29ed-11e9-a5ab-ff8ef2b976c7.

Sarder, MD, and Matthew Haschak. 2019. "Cyber Security and Its Implication on Material Handling and Logistics." *MHI*. https://og.mhi.org/downloads/industrygroups/solutions-community/white-papers/cyber-security.pdf.

Snyder, Hannah. 2019. "Literature Review as a Research Methodology: An Overview and Guidelines." *Journal of Business Research* 104 (1): 333–39. https://doi.org/10.1016/j.jbusres.2019.07.039.

Supply Chain Dive. 2019. "Warehouse Tech Glitches Cause $25M Disruption for Asos." *Supply Chain Dive*, July 23, 2019. https://www.supplychaindive.com/news/asos-warehouse-technology-glitch-millions/559211/.

Véronneau, Simon, and Jacques Roy. 2014. "Security at the Source: Securing Today's Critical Supply Chain Networks." *Journal of Transportation Security* 7 (4): 359–71. https://doi.org/10.1007/s12198-014-0149-z.

Wilkinson, Claire. 2022. "Industrial Robot Safety under Scrutiny." *Business Insurance*, September. https://www.businessinsurance.com/article/20220901/NEWS08/912351998/Industrial-robot-safety-under-scrutiny-.

World Economic Forum. 2023. "Geopolitical Instability Raises Threat of 'Catastrophic Cyberattack in Next Two Years.'" January 23, 2023. https://www.weforum.org/press/2023/01/geopolitical-instability-raises-threat-of-catastrophic-cyberattack-in-next-two-years/.

Yaacoub, Jean-Paul, Hassan Noura, Ola Salman, and Ali Chehab. 2020. "Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations." *Internet of Things* 11:100218. https://doi.org/10.1016/j.iot.2020.100218.

Youn, Soo. 2018. "24 Amazon Workers Sent to Hospital after Robot Accidentally Unleashes Bear Spray." ABS News. December 6, 2018. https://abcnews.go.com/US/24-amazon-workers-hospital-bear-repellent-accident/story?id=59625712.

Zeller, Mark. 2011. "Myth or Reality — Does the Aurora Vulnerability Pose a Risk to My Generator?" *2011 64th Annual Conference for Protective Relay Engineers*, 130–36. https://doi.org/10.1109/cpre.2011.6035612.