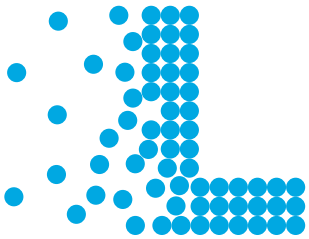

LOCUS

Securing Autonomous Mobile Robot Deployments in the Warehouse

Fouad Khalil CISA, CDPSE
Senior Director of Enterprise Security, Risk, and Compliance
Locus Robotics

Securing Autonomous Mobile Robot Deployments in the Warehouse

Executive Summary

There are significant security and privacy risks associated with warehouse robotics deployments that can negatively affect businesses. It is possible, however, to minimize both the attack surface and the business impact of any incidents by implementing best practices for security in a shared responsibility model with a robust robotics provider.

Risks to robotic deployments and related digital transformation initiatives can materialize via multiple threat and attack vectors. "While this is often faced in industries such as the defense industry, they may also surface in supply chain/logistics or retail warehouse customers.

Financially motived cybercriminals, organized threat actors such as nation state adversaries, and dishonest, or disgruntled associates create most security risks. These threat actors use phishing, malware, insider access, and other attack vectors to damage operators through ransomware, personal data breaches, and intellectual property (IP) or physical product theft. Risks can also arise from adverse regulatory actions or other consequences of non-compliance with privacy or safety laws.

Security risks apply to companies of all sizes in different ways. Smaller warehouse operators tend to have gaps in their overall security or privacy program maturity. Larger companies also face challenges managing technology deployment rollouts in a consistent and secure manner across multiple sites or regions. They face diverse staffing arrangements, warehouse management system (WMS) vendors, languages, cultures, etc. In addition, organizations of all sizes are struggling with a global cybersecurity skills shortage that accentuates these risks and challenges.

Thus, robots, robot control systems, and the WMS connected to them have many potential vulnerabilities. Using a robotics provider that operates with tight, proven security and following best practice recommendations for customer-side security together are proven ways to augment security staff and operate with sufficient assurance to match robotic risks.

Some of the key best practices are to evaluate a robotics provider’s security programs, select a provider that can help their customers establish a shared responsibility model, work closely with the legal department to ensure that privacy and compliance are addressed in vendor contracts, and implement comprehensive customer-side control mechanisms.

Introduction

The purpose of this paper is to inform warehouse business, operations, and security personnel about threats and risks to warehouse robotic systems, common gaps found in many customer deployments, and best practices recommendations for advancing security and privacy in these environments.

Locus Robotics is an innovative robotic process automation company that offers automated warehouse robots to increase productivity and order accuracy among other benefits. The company offers a cloud-based robot management platform, complete robotics system installation and integration into customers' existing WMS, and the delivery or removal of robot units on demand through the Robots-as-a-Service (RaaS) model to meet the needs of cyclical or seasonal order fulfillment.

Locus Robotics offers autonomous mobile robot (AMR) solutions as part of its service delivery model. Three core requirements for Locus Robotics' AMR solution are: security, privacy, and trust. By adopting AMRs, customers are able to eliminate many of the vulnerabilities and risks that accompany do-it-yourself installation of complex, cutting-edge robotics technology.

We assume that readers are familiar with basic IT and service terminology, and encourage all to review the Locus Robotics' white paper "Robots-as-a-Service (RaaS): Delivering Productivity and Savings with Trust and Compliance" for additional background information on AMRs and the RaaS program.

Current State

Warehouse robotics customers face operational challenges in successfully deploying and protecting rapidly changing technologies, particularly when IT or security teams face staffing and skills shortages. Customers are at greater risk of cybersecurity business risks when deploying robots in a do-it-yourself model. The most common business impacts from these risks are:

- Warehouse capability outages caused by ransomware attacks
- Lost customers due to supply chain breaches, lawsuits, or adverse publicity
- Compromised warehouse systems or robots exploited against customers, partners, or the business itself in security incidents including fraud, sabotage, and product intellectual property (IP) or physical product theft
- Costs of disclosure, fines and judgements, or reputational impact due to personal data breaches
- Privacy assessments or privacy complaints leading to fines and judgements

As noted in the first RaaS security white paper, successful warehouse robotics deployments are built on trust. The customer must ensure that the robots themselves, as well as the WMS and robot control systems, are not compromised. There are potential vulnerabilities in these systems, as well as the people and processes that control them. For example, here are a few examples of types of potential vulnerabilities in the table below.

14 Categories of Direct Attack on Systems that Could be Used Against the Robots Themselves	
1. Distributed Denial of Service (DDoS)	8. Jamming Attack
2. Spoofing	9. Hardware Backdoor Attack
3. Man-in-the-Middle (MitM)	10. Remote Access Trojan (RAT)Attack
4. Tampering	11. Stealthy Attack
5. Replay Attack	12. Homing Attack
6. Fault Injection Attack	13. Teardrop Attack
7. Sybil (Network Layer) Attacks	14. Hijacking Attack

Table 1: Potential Cyberattacks on Robots
Source: "14 Popular Cyberattacks on Robotics Systems," Robotsbiz.com[1]

When customers deploy warehouse robots on their own, their security capabilities vary significantly, and can make them vulnerable. With the do-it-yourself deployment model, it can be quite difficult to source the skills and expertise needed to meet risk challenges. If the company does have a security and/or operations team, those teams may not have sufficient knowledge or training in robotics, resulting in them working at cross-purposes.

In contrast, companies adopting autonomous mobile robots from a trusted robotics provider can benefit from a more consistent, scalable, trustworthy, and turnkey solution. AMR customers can:

- Verify the robotic provider's security program
- Work within a shared responsibility model to leverage the robotic provider's team of experience security
- Follow best practices for customer-side security capability deployment
- Dramatically reduce the cybersecurity business risks described above

Threats and Attack Vectors

The threats putting warehouse robotics customers at most risk include:

- Financially motived criminals
- Organized crime, unscrupulous competitors, or nation state adversaries
- Dishonest, disgruntled, or accident-prone associates

Financially Motivated Criminals

The bulk of the risk to most warehouse robotics customers comes from external, financially motivated cybercriminals who are behind most ransomware, data breach, and distributed denial of service (DDoS) incidents. These threat actors take advantage of a vast, amorphous network of cybercrime underground resources including botnet infrastructure, commercialized exploit kits or malware, stolen credentials or data, and money laundering, training, and other services. Cybercriminals' national origins, tactics, and skill levels vary significantly. Most operate as small groups or individuals, and their primary attack vectors include ones that can hit any industry:

- **Broad-based phishing attacks delivered via email, websites, or other communications mechanisms:** These attacks use social engineering techniques to induce users to reveal credentials, sensitive information, or just expose their browser to cyberattacks. Phishing content may impersonate trusted organizations, capitalize on interest in hot news or current events, or create a sense of urgency about fake malware, expiring accounts, lost orders, etc. to attract the user's attention.
- **Automated malware delivery:** Cybercriminals can deliver malware to users as part of a phishing exploit, or through other network interactions.
- **Automated DDoS attacks:** These attacks could disable any exposed warehouse networks, systems, or interfaces.

Once a warehouse user's credentials are compromised via phishing, the cybercriminal can impersonate the user or gain access to resources the user is authorized for, such as robotic system dashboards or administrative resources. The cybercriminal could also manually plant malware on the user's computer, or into parts of the warehouse network and/or applications the user can access. The criminal typically uses such access to steal information (e.g., triggering a data breach), initiate a ransomware attack, or as a steppingstone to expand access into the warehouse for the same reasons.

Similarly, if users' computers, or the warehouse networks and VPNs become infected by malware, cybercriminals can gain access to warehouse systems. Ransomware can spread to many systems through the addressable network. Once activated, the ransomware encrypts and/or steals information from the warehouse and any facilities connected to it. Not only does the information become inaccessible, but entire systems or interfaces depending on the information fail and may be difficult to restore even with backups. The attacker then posts extortion messages on the systems demanding payment to decrypt information and/or not to publish any breached personal data.

Organized Crime, Unscrupulous Competitors, or Nation State Adversaries

Unlike financially motivated cybercriminals who attack more or less randomly, organized cyber-attackers often select their targets carefully. The overlap between cybercriminals, organized threat actors, and disgruntled associates can be seen in Figure 1.

.

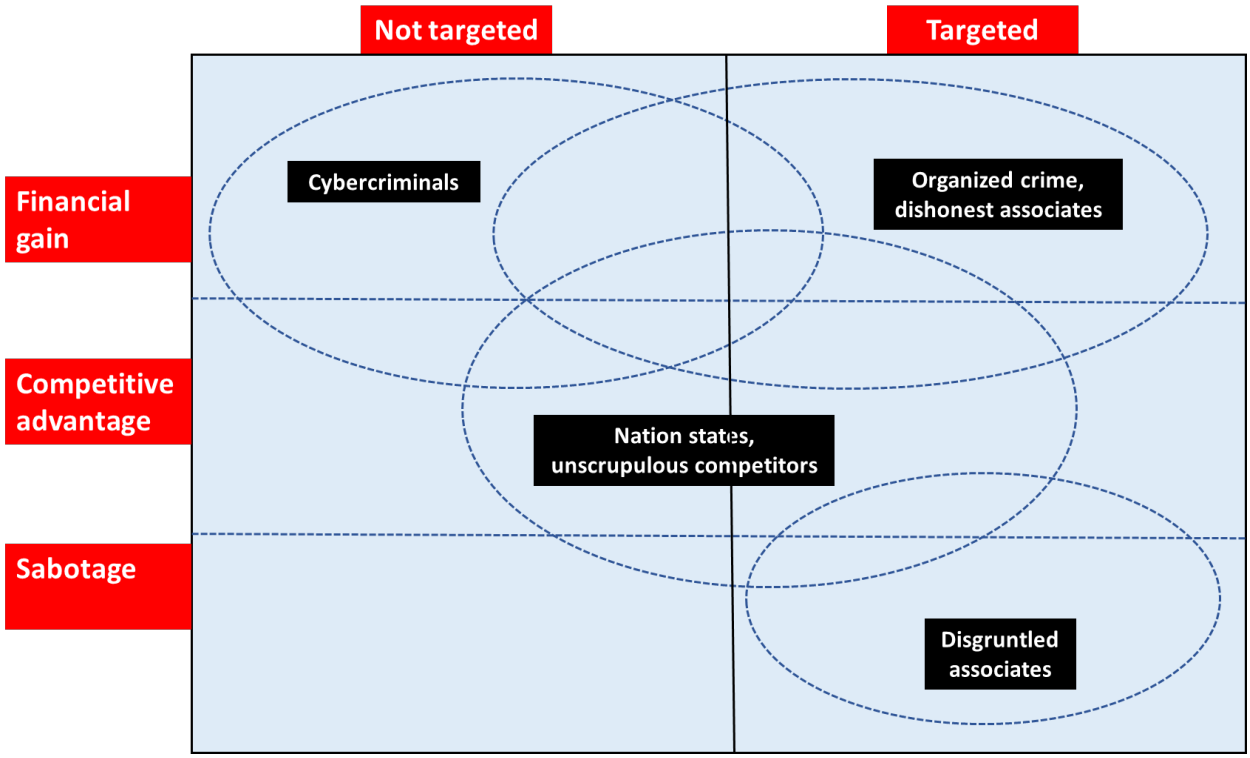

Figure 1: Overlapping Threat Actors and Motivations Affecting Warehouse Robotics Systems

Usually organized crime groups – such as carding or ransomware syndicates – have the same motivation for financial gain (and similar tactics to get it) as individual cybercriminals. However, organized threat actors have more resources to target their attacks or provide products and services enabling the whole cybercrime community to do so against specific countries, industries, or even companies. For example, waves of ransomware attacks afflicted less-prepared education and local government organizations in the U.S. a few years ago, and then moved on to food and agricultural companies more recently. It is important for warehouse operators to know what is going on in the ransomware space for their industry to prioritize the right defensive resources and efforts.

Other organized threat actors – such as unscrupulous competitors and nation state adversaries – may have broader objectives or motivations. Industrial espionage attacks could target physical products or product IP. Or, organized threat actors may try to sabotage their adversaries' or competitors' facilities, products, or operations. Warehouse operators housing valuable medical or military products (such as vaccines or weapons parts) should not only be aware of what is at stake, but also consider increased investment in threat intelligence services.

Organized threat actors can use similar phishing and malware distribution capabilities as individual cybercriminals but may also have access to more sophisticated tools such

as custom-developed malware and “zero day” vulnerabilities. Additionally, they may pay bribes to recruit dishonest employees at the warehouse or related facilities. Warehouse operators should be aware of the elevated risk that local employees could be bribed, or coerced, to help organized threat actors in their efforts to penetrate warehouses located in nations known to regularly conduct industrial espionage.

Dishonest, Disgruntled, or Accident-Prone Associates

Disgruntled or dishonest employees, associates, or partners may steal from warehouse facilities, sabotage them, or both. It is also possible for them to work with external threat actors (individuals or organizations) providing them with additional access and attack vectors. Because they already have authorized access to the warehouse's systems, networks, social media, and physical facilities it becomes extremely dangerous for a warehouse when an insider augments the cyber-skills of an organized cyber-attacker.

Lastly, even honest associates may commit errors that result in warehouse systems becoming unavailable, reducing system integrity, or increasing vulnerabilities.

Legal and Regulatory Risks

Other actors who aren’t – strictly speaking – “threats” can impact warehouse robotics customers as follows:

- **Regulatory authorities:** Failed privacy assessments or adverse audit findings can result in more audits, fines, or delays to carrying out business initiatives.
- **Honest employees:** Employee privacy or safety complaints can cause or exacerbate labor or PR problems, and may lead to audits, fines, or litigation costs.
- **Customers and partners:** May file privacy-related complaints and/or litigate against the company.

Considering these challenges, customers should consider improving their security posture by outsourcing some of the robotic deployment technology burden to a specialist robotics provider and managing security tightly through a shared responsibility model.

Common Gaps

There is a wide range of warehouse robotics customers across a variety of industries, including retail, supply/chain logistics, industrial, medical, and other sectors, but they all face many of the same types of problems when it comes to protecting their environments and managing their risks.

Larger organizations tend to have global security programs. They may also have established processes and procedures for deploying robotics across multiple warehouse sites in a secure manner. On the other hand, smaller organizations tend to be less prepared for robotics deployments. It is not, however, uncommon for even larger organizations to exhibit significant variations in maturity levels or capabilities between warehouse environments or locations. In addition to the expected differences in language, culture, and regulatory requirements across regions, organizations may also have:

- A mix of wholly owned and outsourced warehouse facilities
- Multiple warehouse, IT, and security staffing arrangements (direct employees, contractors, unions, local or remote support)
- Diverse WMS
- Uneven physical security requirements, facilities, and tools

These gaps in cybersecurity maturity and/or the ability to implement robust, consistent security practices across warehouse environments create risks and vulnerabilities to the threat actors noted earlier. Associates in control of warehouse robotics and related systems could be more vulnerable to phishing attacks, malware could spread undetected, and vulnerabilities in the WMS or the robotic systems themselves could be exploited to create the risks discussed previously.

Using a common robotics solution can increase consistency or stability across diverse environments and serve as a force multiplier for resource constrained organizations. Customers should expect the robotics provider to:

- Address all questions about how the organization's associates will use and manage the system.
- Help customers assess potential security, safety, and privacy vulnerabilities (and offer remediation recommendations)
- Offer a streamlined integration and deployment process for diverse warehouse environments.

Privacy Matters

Many customers are trying to deploy cloud systems globally but compliance regulations covering privacy, safety, security, and data retention vary between regions and this can cause difficulties in providing consistent policies, practices, and solutions. In some situations, stakeholders are pushing for a high bar on privacy compliance, but the organization lacks the maturity to practice what it preaches.

For example, some warehouse operators throughout the organization may not to be up to speed on privacy practices covering training, policy/procedures, and underlying security controls (e.g., access control, encryption, sensitive data discovery. Like other

vendors, robotics providers should propose and/or agree to clear contracts and agreements that assure sufficient information is available to meet compliance requirements.

Best Practices Recommendations

Warehouse operators deploying robotic solutions can manage risk in the following manner:

- Analyze the security programs of robotics providers
- Look for providers that proactively help customers establish a shared responsibility model,
- Work closely with the in-house legal department on privacy and compliance in vendor contracts
- Implement a comprehensive customer-side control framework

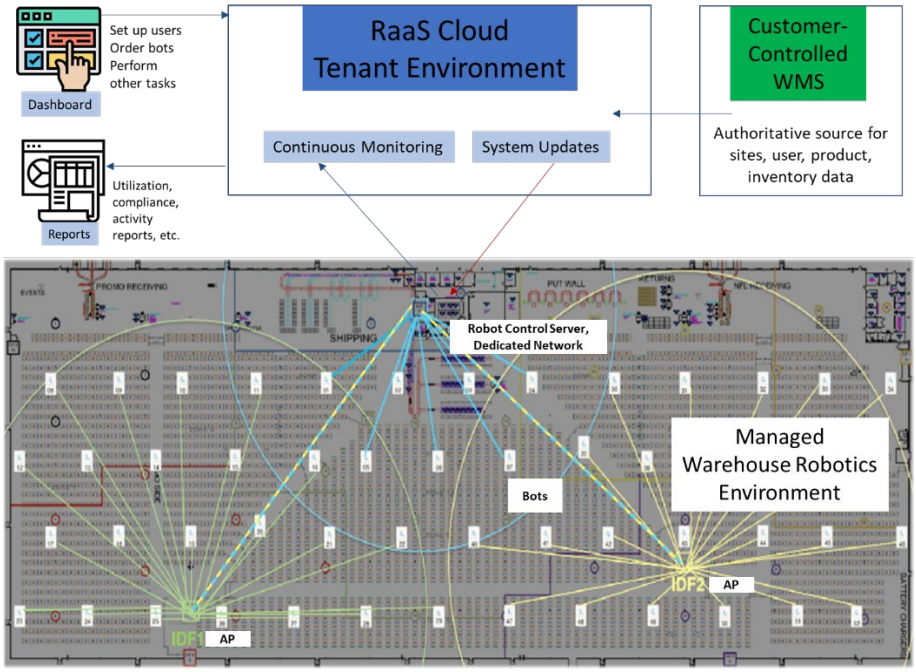

Figure 2: Warehouse Robotics Security Architecture Pattern

Assure the Robotics Provider Meets Your Security Needs

Customers should adopt the RaaS model for the ability to scale up and down as needed and select a robotics provider with best-in-class security. Begin by ensuring your provider has successfully completed a SOC 2^2 audit and has worked with multiple referenceable customers in your vertical industry and geographic area for successful, secure warehouse robotics deployments.

Consider a provider who will help you set up a shared responsibility model tailored to your deployment footprint. As part of this model, the provider should specify the security and privacy capabilities that it offers. In addition, it should clearly describe the practices that it will follow to deliver these capabilities. As well, it should identify the customer's security and privacy responsibilities and specify how the service provider helps fulfill those responsibilities. For more information on the shared responsibility model, see the Locus Robotics' RaaS Security White Paper.

It is critical that contracts, such as Master Service Agreements (MSA), entail an Operations Level Agreement (OLA) describing the provider's operational responsibilities and providing continuous monitoring or reporting to support your compliance commitments.

To determine how you will evaluate the features of the robotics provider, which features you will prioritize, and how you will perform any additional assessments of the provider and plan your own customer-side security operations, please review the RaaS Security Control Framework (introduced in an Appendix of the RaaS Security White Paper). The following sections highlight aspects of the control framework.

Some key capabilities to emphasize in when evaluating robotics providers are the ability to:

- **Minimize customer operations responsibilities:** The more functionality offloaded to the provider, the more consistent the deployment across sites and the less risk of vulnerabilities due to lack of staff resources or skills.
- **Separate the robot control network from customer networks and other warehouse systems:** The provider should offer its own hardened local robot control server and dedicated WLAN solution. This can isolate the robots from rogue network traffic, and greatly reduces the attack surface.
- **Encrypt all traffic between robots, robot control servers, other warehouse systems, and the cloud.** This protects against the many vulnerabilities to robots listed in Table 1 as well as protecting other systems and data.
- **Anonymize personal data for employees in picker roles, or other roles:** This can make it possible for the AMR solution to operate without handling any of the customer employees' personal data. Thus, the customer may be absolved from having to audit or certify its robotics implementation per privacy regulations or defend the solution against litigation or regulatory scrutiny.

Implement Warehouse Robotics Controls

The following sections explore some key controls selected from the Robotic Security Control Framework in more detail. We outline the key controls according to the NIST Cybersecurity Framework (CSF) categories of Identify, Protect, Detect, Respond, and Recover.

Identify Security and Privacy Controls

Identify warehouse robotics risks, vulnerabilities, governance and operations processes, and applicable policies.

- Which policies and procedures can be applied uniformly across all your warehouses/regions? Should any require localization?

Identify all logical and physical systems that are important to securing the warehouse environment through an asset inventory and system specification.

- What physical facilities can house robotic customer premise-based equipment (CPE) such as robots, dedicated network hardware, and the robot control server? What customer-side assets such as WMS servers, consoles, or printers are needed for the robotics deployment?
- What network vendors and WMS systems are used?
- How will the provider integrate with the WMS?

Identify how to perform third party management

- Who are the points of contact on both the customer and the vendor side for each other, and for other vendor solutions in the environment?
- What operations, or service level agreements (SLAs) are in place?

Identify, interpret, and deliver on compliance requirements

- What privacy, safety, data retention, or security regulations cover each warehouse region, or site?
- What existing customer policies cover privacy data sharing with vendors such as robotic providers?

Warehouse operations managers need to be prepared to explain technical privacy characteristics of a robotic deployment to privacy attorneys or regulators.

Address regulatory requirements in master service agreements (MSAs) with providers and other third parties in the warehouse robotics environment. Note that it can be challenging to keep MSAs up to date in the face of changing privacy requirements. The best practice is to create a data processing addendum (DPA) for privacy. Wherever possible, DPAs should reference standard contractual clauses (SCCs) as they are available in some jurisdictions such as the EU.

Protect Security Controls

The following types of security controls should be used to protect the environment:

- **Physical:** Control physical access to the warehouse(s) and to critical areas such as electrical closets, network centers, server rooms, etc.
- **System:** Configure all warehouse systems interacting with the robotics environment for least privilege operation. Enable security updates from the provider to its system (if not performed automatically) and apply security updates regularly to all customer provided systems. Updates should be made quarterly, or more often.
- **Network:** Isolate the robotics WLAN. Control remote access to the environment via a secure VPN. Manage VPN certificates or credentials tightly.
- **Identity and access management:** Consider anonymizing robotics user data (e.g., identities and activities of warehouse pickers). Minimize personnel assigned to higher privilege administrative roles (e.g., administrators having the ability to add/remove users).
- **Data:** Ensure that the provider encrypts customer data both on-premises and in the cloud. Encrypt sensitive customer-side data such as reports and configuration manifests. Perform backups of operational robotics data, including any software or configuration information needed for robotic solution to WMS integration.
- **"Human" layer:** Ensure the provider offers training for safely interacting with robots, protecting robotic CPE, maintaining robotic solution-WMS integrations, and performing user administration and reporting. Provide general security awareness and training for IT employees running the WMS or performing robotic administration and reporting duties.

Detective Security Controls

To gain the necessary visibility needed to secure the warehouse robotics environment:

- **Monitor the logical and physical warehouse environment:** Ensure the provider monitors for intrusions, suspicious access, and other indicators of compromise. Conduct similar customer-side monitoring.
- **Collect information for continuous compliance assessment and perform compliance reporting:** Ensure the provider scans cloud-based and CPE systems for vulnerabilities regularly. Conduct similar customer-side scanning.
- **Review any reporting data or monitoring dashboards from the provider regularly and follow up on issues to learn root causes**: Know your point of contact (POC) with the provider to follow up on any anomalies seen customer side.

SLAs should include an annual pen test of the WMS, warehouse robotics, and associated facilities. Providers should monitor for vulnerabilities and provide notification of zero days or other emergencies in their environment or if visible to them in the customer environment.

Responsive Security Controls

Customers should:

- Coordinate in advance with the provider on response plans.
- Conduct tabletop exercises to prepare IT, legal, HR, and security teams to execute procedures for containing or remediating incidents.
- Contain or mitigate robotics system breaches or failures.

Recovery Controls

Customers should:

- Coordinate with the provider on recovery plans for outages or ransomware incidents
- Periodically perform local testing of recovery procedures with IT
- Manage public relations, or employee relations, in the aftermath of security or safety issues and incidents

Conclusion

Risks to robotics deployments and related digital transformation initiatives in warehouses can materialize via multiple threat and attack vectors. Risks are also significant for supply chain/logistics or retail warehouse customers. Common gaps – such as immature security and privacy programs, inconsistent security and privacy policies or practices across sites, and staffing or skills shortages – are most prevalent in do-it-yourself robotics deployments.

Risks can be significantly reduced by using a trusted robotics provider and implementing proven best practices. By leveraging the provider's security capabilities and robotics expertise, in-house teams can establish a shared responsibility model with the provider and diligently implement customer-side security measures. By ensuring security, privacy, and trust as a baseline, customers can confidently and successfully deploy automated warehouse robotic solutions, thereby substantially increasing productivity and order throughput.

References

[1] “14 Popular Cyberattacks On Robotics Systems,” Robotsbiz.com, January 2022, Accessed At: https://roboticsbiz.com/14-popular-cyberattacks-on-robotics-systems/

[2] SOC for Service Organizations,” AICPA, January 2018, accessed at: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html