



CYBERSECURITY IN THE AGE OF AUTONOMOUS MOBILE ROBOTICS

AUTHORED BY: JOE TENGA
CHIEF INFORMATION OFFICER
CHANG ROBOTICS



INTRODUCTION

The adoption of Autonomous Mobile Robots (AMRs) is transforming industries by enhancing efficiency, automating critical workflows, and reducing operational costs. From healthcare and manufacturing to logistics and retail, these intelligent systems are now central to optimizing supply chains, managing inventory, and improving service delivery. Major enterprises are deploying fleets of AMRs at unprecedented scale – for example, Amazon operated over 750,000 robots in its warehouses by 2023, a 40% increase from the previous year [cyngn.com]. However, the increasing integration of AMRs into enterprise environments also introduces substantial cybersecurity challenges.

As AMRs connect to corporate networks, interact with sensitive data, and gain access to restricted areas, they create new attack surfaces that adversaries can exploit. Threats range from unauthorized network access and data exfiltration to operational disruptions and insider misuse. Without robust protections, these systems risk becoming points of vulnerability rather than assets of efficiency. A recent report highlighted a 107% surge in IoT malware attacks in 2023 [techtargget.com], underscoring the rapid expansion of the threat landscape for internet-connected devices, such as AMRs.

This whitepaper explores the cybersecurity risks associated with AMRs and provides actionable strategies to mitigate them. We begin by identifying key threats – including rogue devices, unauthorized network access, and physical security risks – that underscore the converging cyber and physical dangers posed by AMRs. Next, we examine AMR-specific challenges across various industries, highlighting real-world incidents and tailored mitigation strategies. Finally, we outline best practices for securing AMR deployments.

By implementing a comprehensive cybersecurity strategy, organizations can confidently integrate AMRs into their operations while ensuring data integrity, network security, and business resilience. As the Cybersecurity and Infrastructure Security Agency (CISA) emphasizes, organizational resilience for autonomous systems requires a converged approach that unifies physical security and cybersecurity [cisa.gov]. Executives must recognize that effective AMR security is not merely an IT issue – it is a cross-disciplinary effort that safeguards both the digital and physical dimensions of these robotic systems.

TLDR | TOO LONG DIDN'T READ

For executives looking to secure AMR deployments effectively, several key focus areas must be considered:

- **Industry-Specific Adaptation:** Tailoring security strategies to meet the unique needs of industries such as healthcare, manufacturing, logistics, retail, and government is essential. Aligning controls with standards like HIPAA, ICS security frameworks, and ISA/IEC 62443 ensures compliance and operational resilience.
- **Network Segmentation & Isolation:** Dedicated networks for AMRs should be prioritized to reduce exposure to potential attacks and minimize the risk of lateral movement across enterprise environments.
- **Supply Chain & Vendor Trust:** Vendors and integrators must be rigorously vetted for secure coding practices, vulnerability testing, and routine patching. Building strong vendor relationships improves ecosystem resilience against supply chain attacks.
- **Physical Security & Tamper Prevention:** Implementing robust physical security measures and conducting routine inspections of AMRs can help mitigate risks associated with tampering, particularly in open or public environments.
- **Integration & API Security:** Ensuring secure connections between AMRs and backend systems, such as WMS, ERP, ICS, and retail management systems, is critical. API security and strict access controls should be implemented to protect data exchange.
- **Incident Response & Containment:** Having predefined incident response procedures for AMR-related breaches enables rapid containment and mitigation, thereby minimizing disruption.
- **Zero Trust & Access Control:** Implementing Zero Trust principles ensures continuous authentication and authorization, preventing unauthorized access to critical systems.
- **Security-Conscious Workforce:** Training and empowering employees to recognize threats and follow security best practices is essential. Regular training, clear policies, and periodic testing (e.g., rogue robot drills) build a resilient workforce that complements technical safeguards.
- **Continuous Improvement and Scalability:** As AMR deployments grow, security practices must evolve accordingly. Regular updates, scalability planning, and alignment with evolving regulations are necessary to stay ahead of emerging threats.

By focusing on these areas, organizations can build a robust cybersecurity framework that empowers safe and efficient AMR operations without compromising their business objectives.

WHAT THE EXPERTS SAY: EXCLUSIVE INTERVIEW

Don Capener: Hello, I'm Don Capener Chief Strategist from Chang Robotics, and I'll be moderating our discussion today. Before we dive in, let's start with quick introductions.

Joe Tenga: I'm Joe Tenga, Chang Robotics' Chief Information Officer and acting Chief Information Security Officer.

Don Capener: Thank you. Josh?

Josh Steinman: My name is Joshua Steinman. I'm the CEO and co-founder of Galvanick, a cybersecurity company focused on industrial infrastructure like manufacturing facilities and hospitals.

Don Capener: Great. Jeremy?

Jeremy Smyth: I'm Jeremy Smyth, and I lead the Electrical and Automation Practice at Bootleg Advisors. While Bootleg supports a wide range of operational and strategic initiatives, my focus is on delivering end-to-end automation and electrical solutions — from data integration and robotic systems to energy savings, power quality improvements, and logistical automation.

Don Capener: Thank you. And Shaun?

Shaun Flaharty: I'm Shaun Flaharty, co-owner of Bootleg Advisors. I spent 37 years in manufacturing at Kraft Heinz, first in supply chain and later in engineering and plant operations. At Kraft Heinz I oversaw 42 plants in North America. Since joining Bootleg, I've worked on everything from data acquisition projects to building new manufacturing facilities. Cybersecurity has become critical in the last few years — we aim to make our systems as “fireproof” as possible because the threat is always there, and we have to minimize that risk every day.



Don Capener
Interviewer
Chang Robotics



Joe Tenga
Chang Robotics



Joshua Steinman
Galvanick



Jeremy Smyth
Bootleg Advisors



Shaun Flaharty
Bootleg Advisors



01 | AMRS AS A CYBER-PHYSICAL THREAT

Before addressing industry-specific challenges, it's essential to consider the foundational security risks posed by AMRs. While much of traditional cybersecurity focuses on digital threats, AMRs also introduce significant physical security concerns due to their ability to move autonomously through facilities and interact with secure infrastructure. An AMR can navigate hallways, enter spaces accessible via badges or keycards, and interface with devices like elevators and door controllers – capabilities that blur the line between cyber and physical security.

For example, AMRs often carry secure digital keys or credentials to access restricted elevators or doors as part of their routine. If an internal or external threat actor compromises an AMR, they can use those capabilities to gain unauthorized access to sensitive areas. Additionally, the physical mobility of AMRs introduces risks such as malicious hardware attachments or tampering. Without safeguards such as tamper-proof hardware designs, lockable access panels, regular inspections, and real-time location monitoring, an attacker could exploit an AMR as a moving platform to carry rogue devices into secure areas. In essence, a hacked or hijacked robot becomes a cyber-physical insider, capable of undermining both network defenses and physical barriers.

These dual risks mean organizations must treat AMRs as cyber-physical systems with a broad threat profile. An incident could have both safety implications (e.g., a robot misrouting in a hospital) and data security impacts (e.g., intercepting confidential information). Recognizing AMRs as potential cyber-physical threats is the first step toward developing a security strategy that addresses both dimensions. Enterprises should enforce strict physical security protocols for AMRs, controlling who can approach or service the robots, in addition to traditional cybersecurity measures. By acknowledging that a robot with network access and wheels can bypass locked doors, security leaders can better anticipate and mitigate these unique risks.

NETWORK ATTACK VECTORS TARGETING AMRS

While physical security measures are crucial, they do not eliminate the extensive cyber threats that AMRs face. These robots are not just standalone machines; they are networked computing devices that interface with enterprise systems, making them vulnerable to a range of advanced cyberattacks. Threat actors could exploit an AMR by attaching malicious equipment or manipulating its software, thereby transforming it into a mobile platform for attacks. In effect, a compromised AMR can act as a rogue device, roaming freely within your environment.

Common network-based attack vectors observed in IoT and robotic systems include:

- **Rogue Access Points (APs)** – A malicious actor could affix a small unauthorized Wi-Fi router or hotspot to an AMR, creating a backdoor wireless network inside the facility. This rogue AP can intercept network traffic as the AMR moves through Wi-Fi coverage zones, especially if any nearby systems use unencrypted or weakly encrypted communications. Sensitive data such as login credentials or operational commands could be captured in transit. By positioning the AMR in areas with high network traffic, attackers could amplify their surveillance. Modern encryption, such as properly configured TLS 1.3, significantly reduces this risk, as intercepted data would be unintelligible. Still, the mere presence of an unauthorized network can violate security policies and be used to trick nearby devices into connecting.
- **Network Sniffers** – An attacker might equip an AMR with packet sniffing tools to passively capture network data as the robot traverses different departments or floors. This could expose unencrypted information about operations, inventory levels, production schedules, or user credentials. In well-secured environments that enforce encryption on all network segments, the sniffer would see only gibberish. But any unencrypted traffic (or improperly segmented network) would be vulnerable. Organizations must ensure strong encryption and network segregation to prevent mobile eavesdropping.

WHAT THE EXPERTS SAY



Don Capener: I recently heard about a new, state-of-the-art factory that was down for 11 days due to a cyber incident — really drives home how real this risk is. Shaun, what are you hearing from top executives about this? What keeps them up at night when it comes to cybersecurity in advanced manufacturing?



Shaun Flaharty: Every CEO is thinking about cybersecurity now. It's happened to so many companies that no one can ignore it. Five years ago, a lot of consumer goods manufacturers didn't even have a cybersecurity department. Now almost all of them do. When we discuss any new project at the executive level, the questions are always: "What are we doing to prevent cyber attacks? How are we limiting access? Who is responsible for monitoring this?" As I mentioned, we make sure new equipment and systems are behind firewalls and segmented, but we also recognize that determined attackers may still find a way in. So executives want to know we have both preventive measures and response plans in place.

In fact, many companies have changed their processes. For any new capital project, you now have to answer a checklist about cybersecurity. Just like you'd get approval from Finance or Safety, now you need approval from the cybersecurity team. We're drilling this into everyone involved, starting with the project engineers. If the people designing and proposing a new system don't understand the cyber risks, those issues might get overlooked entirely. So it's become standard to consider cybersecurity requirements alongside everything else — electrical, structural, you name it. It's a big shift in mindset from a few years ago.

- **Man-in-the-Middle (MitM) Devices** – Taking the attack a step further, an adversary could insert a device that actively intercepts and alters communications between the AMR and its control systems. For instance, a MitM attacker could spoof commands or sensor data: redirecting an AMR to the wrong location, causing delays, or injecting false readings into inventory databases. Such manipulation could even induce unsafe behavior or collisions if safety commands are blocked or altered. Employing end-to-end encryption with mutual authentication (e.g., TLS with client and server certificates) thwarts most MitM attacks by ensuring the AMR only accepts commands from authenticated controllers and that data in transit cannot be tampered with undetected.
- **Hardware Implants** – An incredibly stealthy threat is the insertion of a hardware implant inside the robot. These miniature devices could be embedded during maintenance or concealed as an upgrade component. Once in place, an implant can provide persistent remote access to the AMR's internals, enabling attackers to monitor data or alter functionality at will. Because implants piggyback on the robot's legitimate hardware, they often go undetected by everyday software-based security tools. Only physical tamper-proofing measures (e.g., seals, enclosure locks) and regular hands-on inspections can detect these issues promptly. For high-security deployments, organizations might implement randomized inspections of robots' hardware or use sensors to detect changes in weight or power draw that could indicate a hidden device.
- **IoT Exploit Modules** – Attackers may target AMRs as part of broader network exploits. For example, a compromised robot could roam within range of other IoT devices or computers and scan for open ports or unpatched vulnerabilities. If an AMR connects (even briefly) to a less secure network segment, it might serve as a bridge for malware to spread into more sensitive systems. Past IoT malware, such as Mirai, demonstrated how vulnerable connected devices can be co-opted into botnets.

In an enterprise, an infected AMR could attempt to propagate ransomware or spyware to every system it encounters. Strong network segmentation and rigorous patch management are crucial for containing such threats. Each robot and its communications should be isolated such that even if one AMR is compromised, it cannot freely access other corporate assets.

- **Proxy Access Abuse** – This often-overlooked risk stems from the legitimate capabilities of AMRs. Many AMRs are authorized to enter secure areas (e.g., badge-restricted floors or locked storage rooms) to perform their duties. An insider threat or clever external attacker could exploit this by piggybacking on the robot's access permissions. For instance, a malicious employee might load a payload onto an AMR knowing it will be taken into a secure lab, or could remotely instruct a compromised AMR to open doors and let unauthorized personnel through. In one real scenario, researchers demonstrated that vulnerabilities in a hospital delivery robot allowed them to take control of elevators and door systems via the robot, potentially accessing floors that would otherwise require an authorized badge [ivanti.com, ivanti.com]. This proxy risk involves using the robot as a Trojan horse to circumvent physical security controls. It highlights why security teams must account for where robots are allowed to go and what they're allowed to do.

The stakes are high. A successful attack exploiting any of these vectors could result in data breaches, system downtime, or even compromise human safety. Notably, many IoT and robotic attacks often go undetected for long periods. Enterprises should assume that if a device is not explicitly secured, attackers will eventually target it. The dramatic rise in IoT-focused threats in recent years supports this assumption. For example, Gartner analysts predict that by 2025, nearly 45% of organizations worldwide will have experienced attacks on their software supply chains or IoT devices [techtarget.com]. AMRs, as mobile IoT devices with privileged network access, must be treated as high-value assets in threat models.

MITIGATING NETWORK-BASED THREATS

To mitigate the above risks, organizations must adopt a layered security approach that integrates both robust cyber defenses and physical safeguards for their AMR fleets. Key strategies include:

- **Secure Hardware and Tamper Prevention:** Utilize tamper-evident seals, chassis locks, and intrusion sensors on robots to deter and detect unauthorized physical access to their internal components. Regularly inspect AMRs for signs of tampering or unfamiliar devices attached. Staff should be trained to promptly report any unusual occurrences (e.g., a USB stick being plugged into a robot, or an extra antenna being visible on the unit). By increasing the effort required to plant rogue devices, you reduce the window of opportunity for attackers.
- **Strong Encryption and Authentication:** All communications to and from AMRs should be encrypted using modern protocols (such as TLS 1.3) and authenticated. Implement certificate-based mutual authentication so that the AMR only communicates with trusted servers, and vice versa. This protects against eavesdropping (sniffers) and spoofing (Man-in-the-Middle, MitM) devices by ensuring data in transit remains confidential and unaltered. Additionally, storing sensitive data on the robot (if any) should be minimized, and any stored data should be encrypted at rest.
- **Network Segmentation:** Treat AMRs as untrusted by default and isolate their network traffic. Place AMR control systems and devices on dedicated VLANs or subnets separate from the core enterprise network. Use firewall rules to strictly limit which systems the AMR can communicate with. For instance, it likely only needs to interact with the fleet management server, not every database in the company. NIST's guidance for industrial control systems explicitly advocates dividing OT networks into isolated segments with strong access controls [NIST], which also applies here. Proper segmentation ensures that even if an AMR is compromised, the attacker cannot easily pivot to more critical systems.

WHAT THE EXPERTS SAY



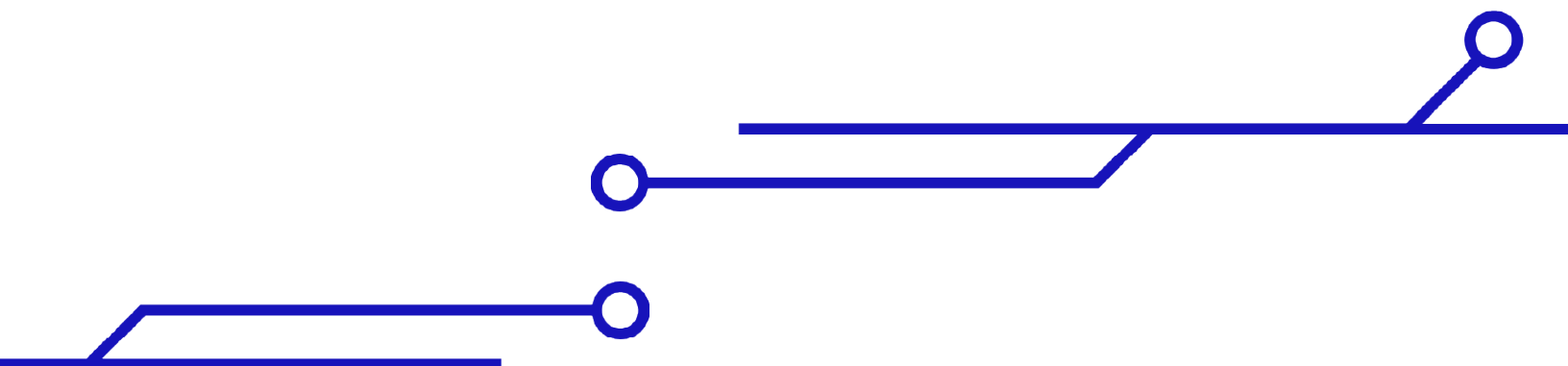
Don Capener: Shaun, have you ever had to stop production or shut down operations because of a cybersecurity threat, or even a suspected threat? If not, have you encountered any close calls like that?



Shaun Flaharty: We haven't had a full-blown compromise that forced a shutdown yet, but we have had situations where we thought something might be wrong and we proactively shut down to investigate. We run tests, and we've recently put in tracers to detect if someone has breached our systems. The biggest issue I see is companies not separating IT and OT (operational technology). Over the years some companies merged their corporate IT network with the plant's operational network for cost reasons. Right now, I'm working with a client to split IT and OT apart again, so the plant floor stays behind its own firewall. I always say you should have one way in and one way out. On the plant floor, machines need to talk to other machines and robots need to communicate, especially as we automate more due to the labor market. But the more automation you have, the more signals and potential vulnerabilities there are. So, in my view, we've got to separate IT and OT to protect the manufacturing floor.

- **Intrusion Detection and Monitoring:** Deploy intrusion detection systems (IDS/IPS) and continuous monitoring on the AMR network segments. Monitor for unusual patterns such as an AMR sending traffic to an unknown external IP or large data dumps leaving the AMR network. Advanced monitoring solutions can utilize AI to learn normal AMR behavior and autonomously detect and raise alerts on anomalies (e.g., a robot communicating at odd hours or deviating from normal data volumes) [Darktrace]. Early detection of a rogue device or malware on an AMR can prevent an incident from escalating.
- **Access Control and Zero Trust:** Implement the Zero Trust principle for all AMR-related systems – every access request should be continuously authenticated and authorized. Use role-based access control (RBAC) to ensure only necessary personnel and systems have credentials to interact with AMRs. For example, an engineer in one facility shouldn't, by default, have admin access to robots in another location. Enforce multi-factor authentication (MFA) for any human access to AMR management consoles or remote controls. These measures limit opportunities for attackers to misuse stolen credentials or for insiders to abuse privileges.

By combining physical hardening, encrypted communications, network isolation, and vigilant monitoring, organizations can significantly reduce the likelihood and impact of network-based attacks on AMRs. No single control is sufficient on its own – the goal is defense in depth. Just as importantly, incident response plans should specifically cover AMR-related scenarios (for instance, how to shut down or quarantine a compromised robot safely) so that security teams can react quickly if an issue is detected. A swift, coordinated response can make the difference in containing an AMR breach before it spreads to the broader enterprise.



THE THREAT OF SHARED NETWORKS

Many organizations deploy AMRs onto shared networks, where robots communicate over the same wireless LAN or internal network as other IoT devices, corporate PCs, or even industrial control systems (ICS). While convenient and cost-effective, using shared infrastructure in this way introduces significant cybersecurity risks. Unlike a segregated network that isolates devices, a shared network broadens the attack surface, making AMRs more susceptible to threats such as unauthorized access, data interception, and lateral movement by attackers.

In industries where AMRs handle sensitive data or interface with critical systems, a shared network means that a breach of one device can quickly affect others. A compromised AMR on a flat network could serve as an entry point for cyber threats, allowing attackers to pivot into more critical systems, disrupt operations, or exfiltrate confidential data. For example, consider a hospital where an AMR is connected to the general hospital's IT network. If that robot is compromised, an attacker might leverage it to access electronic health record (EHR) databases or medical device networks. Similarly, in a manufacturing plant, a hacked AMR on the plant's main network could probe and interfere with ICS, potentially halting production or damaging equipment.

Beyond direct cyber threats, shared networks can also introduce reliability challenges. Although most AMRs operate with self-contained instructions and localized decision-making, they may still rely on network communication for reporting, receiving updates, or coordinating with other systems. In scenarios where multiple devices compete for bandwidth, such as high-resolution video streams from security cameras, network congestion can delay non-critical data exchanges or status updates. While this may not directly interrupt the robot's core functions, it could impair real-time coordination with centralized systems or cloud platforms, potentially leading to inefficient operations or delayed responses to changing conditions. Thus, the predictability and quality of service on a shared network are concerns alongside security.

In summary, while shared networks are commonly the norm, they merge the risks of IT and OT environments, potentially magnifying existing vulnerabilities. An exploit anywhere on the shared medium – whether it's a vulnerable smart TV in a lobby or a malware-infected laptop – can potentially reach the AMR.

This interconnectedness means that securing AMRs must also involve securing the broader network and managing the interplay of all connected devices. Many high-profile breaches in recent years have originated from less critical devices being used as footholds; an AMR should not become the weakest link that opens the door.

MITIGATING SHARED NETWORK RISKS

Ideally, network segregation is the best practice: keeping AMRs on dedicated networks with tightly controlled gateways. When that isn't feasible due to cost or operational needs, organizations should implement enhanced security measures to harden the shared environment. Key mitigations include:

- **Virtual Network Segmentation (VLANs):** Even on a shared physical network, create logical segmentation using VLANs for AMR traffic. For example, all AMRs and their management systems could be on VLAN 50, separated from the corporate office VLAN 10. Configure access control lists so that VLAN 50 only communicates with necessary services (such as the robotics management server on VLAN 51) and nothing else. This limits the blast radius if an AMR is compromised and prevents it from freely communicating with unrelated endpoints.

- **Quality of Service (QoS) Policies:** Implement QoS to prioritize AMR communications over other traffic. Time-sensitive commands or sensor feeds from robots should not be delayed by bulk data transfers elsewhere on the network. By marking AMR traffic with high priority and reserving bandwidth, you reduce the chance that network congestion will cause robotics operations to lag. This is especially important for real-time or safety-critical AMR functions.

Lightweight, Efficient Encryption: Ensure that even within the local network, AMR communications are encrypted, but use protocols optimized for speed to minimize latency. Algorithms like AES-128-GCM, which efficiently combine encryption and integrity checking, are commonly used for IoT devices. In higher-security contexts, AES-256-GCM can be deployed, and alternatives such as ChaCha20-Poly1305 can be considered for devices that lack AES hardware acceleration. The goal is never to send data in plain text, even internally. Lightweight encryption protects against an attacker who might already have a foothold on the network and is attempting to sniff or manipulate robot traffic.

- **Continuous Network Monitoring:** Deploy real-time monitoring that analyzes both the network traffic and the AMR behavior on the shared network. This could be an extension of your intrusion detection system, tuned to look for anomalies in the AMR VLAN. Suspicious signs might include an unknown device trying to communicate with an AMR, an AMR suddenly transmitting large amounts of data to a new server, or repeated failed connection attempts (which could indicate scanning or brute-force attempts). Automated alerts should be set to notify IT staff of these events so they can be investigated immediately.
- **Zero Trust Access Controls:** Adopt a Zero Trust approach, where each device on the shared network is assumed to be hostile until proven otherwise. Concretely, this means continuously verifying identities and permissions. Utilize network access control (NAC) solutions to authenticate devices when they join the network and to check their compliance posture (e.g., is the AMR running approved firmware?). Implement strict role-based access controls for any systems that interface between the AMR network and other networks, ensuring that even if credentials are stolen, they cannot be used to pivot broadly. Multi-factor authentication should be required for any remote access into the AMR network segment.

WHAT THE EXPERTS SAY

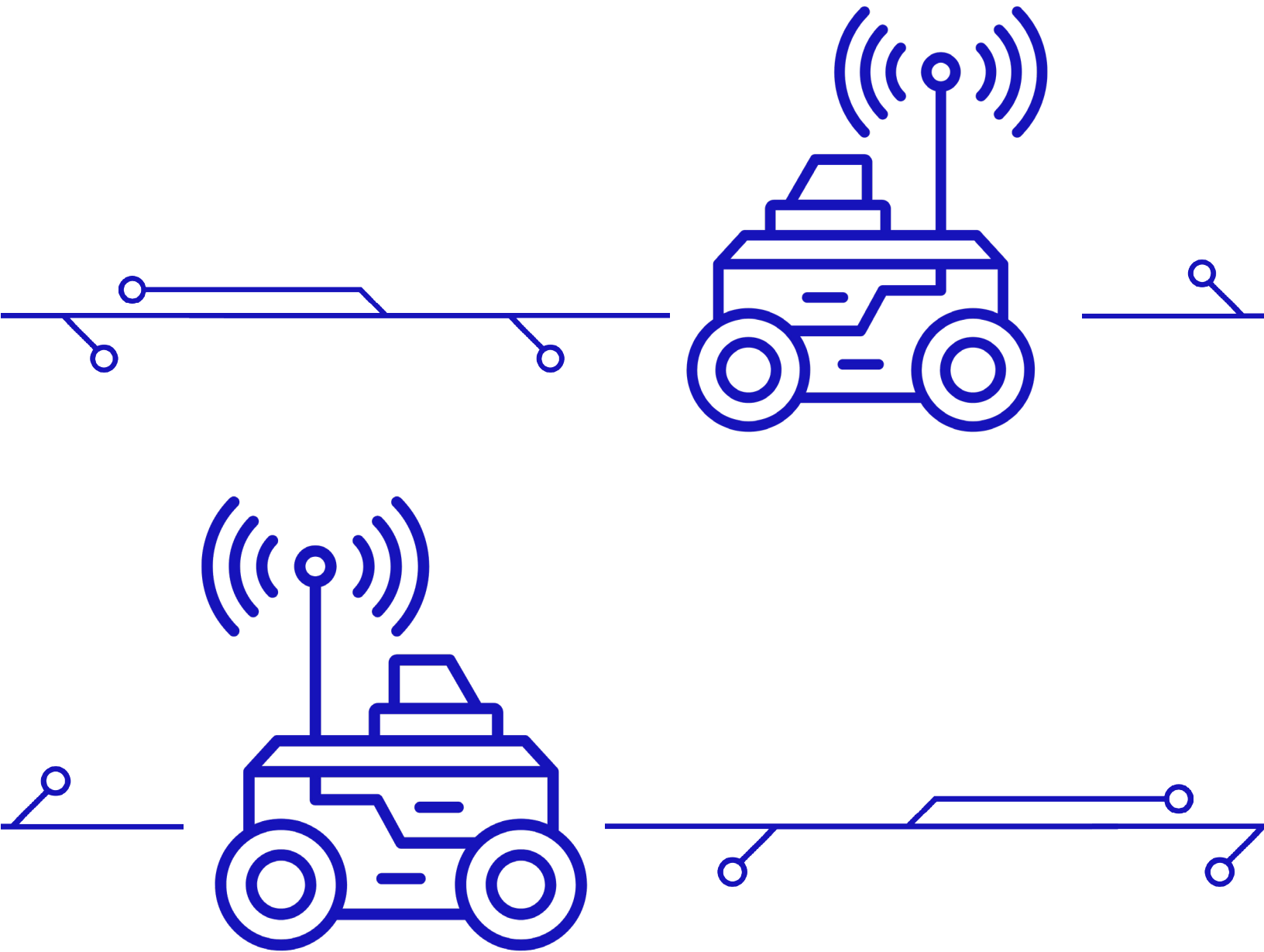


Don Capener: Josh, if you're advising large manufacturing companies — say, in food and beverage — what are the top two or three threat factors or vulnerabilities, you'd warn their leadership about? And what mitigations would you recommend, especially for plant managers or general managers who might not be cybersecurity experts?



Josh Steinman: That's a great question. A lot of people assume that having a firewall is a silver bullet, but it's not. Firewalls are important, but in our experience, most industrial networks still have some way for data (or an attacker) to get in or out. We've seen cases where certain machines can tunnel out through the firewall or even have a built-in cellular connection to "phone home" to the vendor. Folks might claim their system is air-gapped, but I've yet to encounter a facility that was truly isolated. There's almost always an unknown connection point, and that's what attackers will find. This is why I advocate for continuous monitoring. At Galvanick, we capture and watch data from the factory floor 24/7. If something anomalous happens, we immediately investigate and alert both the production team and the security team. We take this approach because we know there are hidden pathways in and out of these systems that management might not be aware of. Continuous monitoring gives you visibility into those and into everything happening in real time. For example, if a contractor plugs in a tool and starts updating a machine, our system will notice any unusual behavior instantly. In short, I tell clients to assume that breaches can and will happen. Rather than relying solely on the idea that "we have a firewall so we're safe," focus on detecting and responding quickly. It's very hard today to build a modern plant that has zero external connectivity — so knowing what's going on and catching issues early is absolutely key.

By implementing these strategies, organizations can significantly reduce the risks associated with shared network deployments of AMRs. While a fully air-gapped robot network is ideal for security, it may not be practical for all. A well-designed shared network with strong segmentation, traffic management, and vigilant monitoring can still provide a high level of protection for AMR operations. It is about compensating for the additional exposure with tighter controls and more thoughtful oversight. Treat every AMR as a critical endpoint and every other device as a potential threat. You will then design a network environment that enables robots to operate safely and reliably, even in the face of broader connectivity



02 | AMR INDUSTRY PLAYBOOKS

The security considerations for AMRs can vary significantly across different industries. In the following sections, we delve into specific sectors – healthcare, manufacturing, logistics, retail, and government – to highlight particular risks and real-world examples, as well as tailored mitigation strategies. Each “playbook” is a guide for executives to understand how AMR cybersecurity aligns with their industry’s unique operational demands and regulatory requirements.



HEALTHCARE: BALANCING AUTOMATION WITH PATIENT SAFETY & PRIVACY

In healthcare, AMRs are entrusted with critical tasks such as transporting medical supplies, pharmaceuticals, lab samples, and even devices that interface with patient data. These robots enhance efficiency and precision in hospitals, speeding up deliveries and reducing human error, but their use in clinical settings introduces significant security vulnerabilities. Both physical and cyber threats to healthcare AMRs can directly impact patient safety and privacy, making this a particularly high-stakes environment.

One immediate concern is that AMRs could act as vectors for cyberattacks against hospital networks. Even if a robot isn't carrying apparent sensitive data, it often transmits information between systems (e.g., updating an inventory database or signaling its location). If an attacker intercepts or alters that data, they might expose or corrupt information from Electronic Medical Records (EMRs) or other healthcare systems. A breach of this nature would violate regulations such as HIPAA, erode patient trust, and expose the hospital to potential legal penalties. Notably, an AMR doesn't need to directly handle Protected Health Information (PHI) to pose a risk. If it operates on a shared hospital network and is compromised, an attacker could use it as a bridgehead into clinical systems containing PHI. In other words, the robot could open a backdoor that ultimately leads to patient data theft even without the robot itself carrying patient records.

Beyond data interception, there is a risk of cyber-physical harm. AMRs in hospitals often interface with IoT-enabled biomedical equipment, such as smart IV pumps or vital sign monitors, and building systems, including elevators and automatic doors. A hacked AMR could potentially send malicious commands or signals to these connected devices. For instance, an attacker who gains control of an AMR might attempt to alter settings on a nearby wireless infusion pump or turn off an elevator that the robot uses, indirectly impacting patient care. Although this scenario is complex, it's within the realm of possibility as more medical devices become networked. Similarly, an AMR that delivers medications could have its route manipulated or its contents tampered with, resulting in patients receiving missing or delayed medications. Such disruptions can have life-threatening consequences in a clinical environment.

We must also consider physical security abuses. While less likely than cyber exploits, an AMR could be intentionally misused to transport harmful substances or devices inside a hospital. The mobility and autonomy that make these robots useful could, in theory, be exploited for nefarious purposes. For example, someone could attempt to use a hospital delivery robot to carry a dangerous payload into a public area. This is a security scenario more akin to terrorism or sabotage, with no known real-world instances to date. However, it underscores why comprehensive security, including background checks for personnel with access to robots and random inspections of robot cargo, is prudent in healthcare settings.

In 2022, a stark example of healthcare robot vulnerabilities came to light. Researchers disclosed five zero-day flaws (dubbed "JekyllBot:5") in the Aethon TUG autonomous robots, which are widely used in hospitals for deliveries. If exploited, these flaws could allow hackers to take complete control of the robots, enabling them to disrupt medication deliveries, interfere with hospital elevators and door locks, spy through the robots' cameras, and even hijack the robot's admin portal to spread malware into the hospital network [ivanti.com, ivanti.com]. This case illustrates that the threat is not theoretical: unpatched AMRs in hospitals have been proven vulnerable and require urgent patches to avoid potential patient safety incidents [cyberscoop.com]. As a result, healthcare executives recognized that AMR security requires the same level of attention as medical device security.

MITIGATING HEALTHCARE RISKS

To address the unique challenges posed by AMRs in healthcare, organizations must implement a multi-layered cybersecurity strategy tailored to protect both patient data and patient safety:

- **Data Encryption In Transit and At Rest:** Healthcare data is highly sensitive, so robust encryption is non-negotiable. All data transmissions involving AMRs (e.g., status reports to nurse stations, inventory updates to pharmacy databases) should use end-to-end encryption. Adopting transport standards like TLS 1.3 for robot communications ensures that even if network traffic is intercepted, the PHI or other sensitive data remains unintelligible. Likewise, any data stored on the robot, such as delivery logs or temporary patient information, should be encrypted at rest using strong algorithms (e.g., AES-256). This helps maintain confidentiality and integrity, thereby fulfilling HIPAA security rule requirements for data in transit and at rest.
- **Strict Network Segmentation and Access Control:** Hospitals should isolate AMRs on dedicated network segments separate from the general hospital network and, in particular, from life-critical systems such as surgical equipment or ICU monitoring networks. Fine-grained network segmentation, combined with role-based access control (RBAC), limits who and what can interact with the robots. For example, an AMR might only need to communicate with the hospital's logistics server and no other endpoints. Implement firewall rules accordingly. Additionally, requiring multi-factor authentication (MFA) for any user accessing the AMR control dashboard provides an extra layer of protection against unauthorized control. Only authenticated clinical engineering or IT staff should be able to send high-level commands to the robots.
- **Continuous Monitoring and Behavioral Analytics:** Given the critical nature of healthcare, real-time detection of anomalies is vital. Deploy monitoring systems that can flag unusual AMR behavior – for instance, if a robot deviates from its regular delivery route or attempts to access a network resource it has never used before. If an AMR begins sending data to an unfamiliar server or at odd hours, it could indicate malware exfiltration. Advanced behavioral analytics can establish baselines for each robot's typical patterns (routes, schedules, data volume) and alert on deviations. Early detection allows hospital IT teams to intervene before a security incident escalates. In practice, this might mean automatically pausing a robot's activity if it exhibits suspicious behavior and dispatching an investigator.
- **Physical Security and Tamper-Proofing:** Ensuring the robots are physically secure is as important as cyber measures. Healthcare organizations should invest in tamper-proof designs or retrofits – for example, Aethon's TUG robots have optional badge access panels for their payload compartments, ensuring only authorized staff can remove items. Regular physical inspections of the robots should be part of the maintenance routine. Staff should look for signs of tampering such as new devices attached, panels ajar, or tool marks on screws. Training hospital staff to recognize these signs is key. One person simply noticing "this robot has an extra cable hanging from it" and reporting it could thwart an attack.

By implementing these measures, healthcare providers can significantly reduce the risk that AMRs become conduits for breaches or safety incidents. For instance, in response to the Aethon TUG vulnerabilities, many hospitals swiftly applied firmware patches (cyber fix) and reviewed who had physical access to the robots (physical fix) – a demonstration of the dual approach needed. Ultimately, the goal is to prevent unauthorized interception or control of any data or function related to AMRs. This means thinking like an attacker: securing not just the robot, but the entire ecosystem around it, including networks, people, and processes. A hospital that treats its delivery robots with the same rigor as it treats an MRI machine or an electronic health record system will be well-positioned to reap the efficiency benefits of AMRs without compromising patient safety or privacy.

MANUFACTURING: PROTECTING OPERATIONAL INTEGRITY

Manufacturing environments present unique cybersecurity challenges due to the close integration of AMRs with industrial control systems (ICS) and the high stakes of production uptime. AMRs on the factory floor aren't just roving helpers; they are often tied directly into workflows – delivering parts to assembly lines just-in-time, fetching tools, or performing quality inspections. A disruption or compromise of these robots can thus have immediate and widespread operational impacts. In manufacturing, even a few minutes of downtime can result in substantial financial losses and lead to cascading supply chain delays.

One of the most significant risks is that a compromised AMR could be used as a pivot into the Industrial Control Systems that run production. If an attacker gains control of an AMR, they might use it to interact with PLCs (Programmable Logic Controllers), SCADA systems, or other factory equipment that the AMR interfaces with. For example, if the AMR has a module to signal a robotic arm when it has delivered a part, a hacker could manipulate that interface to send false signals, potentially causing the robotic arm to malfunction or halt. Even more alarming, if the AMR is connected to the plant's OT network, an attacker could attempt to alter production parameters (like temperatures, pressures, or calibration settings) via the compromised robot's access. This type of attack blurs into the realm of ICS cyberattacks that can sabotage physical processes, recalling incidents such as Stuxnet, which targeted centrifuges, or Triton, which targeted safety systems. Manufacturing executives should recognize that any device bridging IT and OT systems, as AMRs often do, must be hardened to ICS-level security standards to prevent such scenarios.

Intellectual property (IP) theft or exposure is another risk area. Factories often rely on AMRs to transport sensitive materials or proprietary product components, such as when an AMR carries a prototype part from one lab to another. If an AMR is equipped with cameras or sensors for navigation, those could potentially be co-opted to spy on processes or gather data on product designs. Even without direct espionage, a compromised robot might be used to exfiltrate data from nearby systems – for instance, by intercepting network traffic as it passes and capturing confidential design documents or transmitting them out. The loss of trade secrets or blueprints could be as damaging as a production stoppage. In one hypothetical example, an attacker could target a car manufacturing plant's autonomous mobile robots (AMRs) to steal designs for an unreleased model. While hypothetical, this risk is plausible enough that manufacturing companies should consider incorporating AMRs into their IP protection strategy.

Operational disruption remains the most immediate threat in manufacturing. Unlike in other sectors, where a device outage might inconvenience a few employees, an AMR malfunction in manufacturing can halt a production line. If a critical AMR that shuttles components to the line is taken down by ransomware or a DoS attack, the line may have to stop until a manual process is implemented. This downtime can quickly amount to millions of dollars, especially in industries such as automotive or semiconductor manufacturing, where throughput is tightly calibrated. Attackers are also aware of this – there have been instances where ransomware attacks have specifically targeted manufacturing firms because the cost of downtime would pressure the victim into paying. A notable example is the 2021 cyberattack on JBS S.A., one of the world's largest meat processing companies. The ransomware attack forced JBS to shut down all its U.S. beef plants temporarily and disrupted operations in Australia and Canada. To resume operations swiftly and mitigate prolonged downtime, JBS paid an \$11 million ransom in Bitcoin to the attackers. An AMR could be the avenue for such an attack. Once inside the robot's system, malware could propagate to control stations and render multiple robots inoperative, effectively bringing the factory to a standstill.

Safety is perhaps the greatest risk. Manufacturing robots, including autonomous mobile robots, operate near workers and heavy machinery. A hacked AMR could potentially bypass safety protocols – for instance, failing to stop when a human crosses its path or moving into a restricted zone. While most AMRs have built-in safety sensors to prevent collisions, an attacker with deep control may be able to override or turn off these sensors. Any cybersecurity incident that compromises safety systems could lead to physical injuries on the shop floor, elevating the consequences from financial to human harm.

In summary, manufacturing AMRs encompass multiple risk domains, including ICS/OT security, intellectual property protection, uptime and reliability, and human safety. This combination requires manufacturers to treat AMR security as part of their core operational risk management. Frameworks such as the ISA/IEC 62443 standard for industrial cybersecurity and NIST's guidelines for ICS (SP 800-82) are highly relevant here, as they provide guidance on network segmentation, system hardening, and continuous monitoring in OT environments, all of which apply to AMRs integrated with production lines.

MITIGATING MANUFACTURING RISKS

Manufacturers can take several proactive steps to secure AMRs and maintain operational integrity:

- **Dedicated OT Network for AMRs:** Whenever possible, place AMRs on a separate network segment isolated from corporate IT and even segmented within the OT network. This could mean a dedicated wireless network just for robotics, with very limited access to the broader plant network. By maintaining AMRs on their own network, organizations significantly reduce the likelihood that a compromise of an office computer or a vendor's VPN will eventually lead to the compromise of the robots. Similarly, if an AMR is breached, a segmented network ensures the attacker cannot easily reach critical controllers or databases. This aligns with the principle of zones and conduits in ISA 62443, which involves keeping critical processes in tightly controlled zones.

WHAT THE EXPERTS SAY



Don Capener: Josh, from your perspective, what threats do manufacturers face when it comes to robotics and advanced manufacturing?



Josh Steinman: By way of background, before founding Galvanick I spent four years as the senior cybersecurity official on the U.S. National Security Council at the White House. One major incident I dealt with was the "NotPetya" cyber-attack in 2017. It was aimed at Ukraine's economy, but it ended up spreading worldwide and causing billions of dollars in damage. It hit companies like Merck, Cadbury, and Maersk, and even disrupted operations at ports and hospitals. It spread so widely because it exploited unpatched Windows systems.

A lot of manufacturing environments still run older software on their engineering workstations and operator interfaces. Often a contractor installs a machine, gets it working, and says "don't update it." That can leave you vulnerable. I've heard people at companies say, "Why would anyone attack us? We just make X." But as NotPetya showed, in a connected digital world, you can get hit even if you're not the intended target. So industrial cybersecurity needs serious attention. Unlike IT, industrial operations haven't had the same security focus over the last few decades, even as they became highly digitized.



Don Capener: Jeremy, what do you see as the biggest vulnerabilities in the supply chain relative to cybersecurity?



Jeremy Smyth: A huge vulnerability is not just your own systems, but your partners'. I've seen it firsthand. I had a client that was taken down by a cyber attack on one of their vendors. So the critical thing is, what are your vendors doing about cybersecurity? It's not enough to have your own house in order; you need to ensure your suppliers and partners are also protected and that you're monitoring their security postures.

- **Hardened Interfaces with ICS:** For any integration points between AMRs and ICS equipment, use industrial-grade security controls. For example, if an AMR must interface with a PLC (say, to signal when a bin is loaded), consider using an intermediate gateway device that can validate commands and enforce limits. Ensure that all protocols in use (e.g., OPC UA, MQTT) are configured with security in mind, including encryption and authentication. Additionally, enable whitelisting on the AMR's software to ensure it only runs approved applications and services, thereby reducing the likelihood that malware on the robot could execute or initiate external communications.
- **Multi-Factor Authentication & Role-Based Access:** Only authorized engineers or operators should have access to configure or control AMRs, and MFA should be used to protect their accounts. Use role-based access control so that, for instance, an assembly line worker cannot log into the robot's management console – only control engineers or IT security should. This limits insider threats and mistakes. Additionally, maintain an access log of who accesses AMR systems and when, and review these logs for any irregularities, such as an account being used at unusual hours.
- **Regular Audits and Penetration Testing:** Schedule routine security assessments focused on the AMR systems and their connections to the rest of the plant. This might involve hiring specialists to perform penetration tests, attempting to compromise a robot or its communications. Such tests can reveal misconfigurations or overlooked vulnerabilities, such as default manufacturer passwords or unsecured maintenance ports. Findings should be remediated promptly, and the tests should be repeated periodically or when significant changes occur. These audits also help ensure compliance with standards (e.g., NIST, ISO 27001) and provide executives with an objective view of their security posture.
- **Real-Time OT Monitoring:** Extend your ICS monitoring to include AMRs. Many manufacturers utilize Security Information and Event Management (SIEM) tools or specialized Operational Technology (OT) monitoring solutions to track device behavior on control networks. Integrate the AMRs into this monitoring. For instance, if an AMR typically communicates only with the warehouse system, an alert should be triggered if it suddenly attempts to connect to the programmable logic controllers in the paint shop. Some organizations deploy “canary” signals – known benign messages – and verify that AMRs respond only to expected inputs. Anomalies might indicate a need for investigation.
- **Autonomous Response:** Nowadays, new threats emerge rapidly, some even created by artificial intelligence. However, there are technologies available that utilize AI to identify anomalies without relying on threat signatures, and then autonomously respond to these threats.

By addressing these unique challenges, manufacturers can safeguard their operations and ensure that AMRs remain a secure and productive part of their workflows. In practice, manufacturers commonly adopt rigorous assessments and safety checklists for AMRs before allowing entry into sensitive production areas. Omron Automation emphasizes the importance of comprehensive risk assessments and adherence to industrial safety standards when integrating AMRs into operational environments (Omron Automation). Similarly, MOV.AI provides detailed cybersecurity checklists recommending risk assessment, secure system design, and validation processes to ensure AMRs operate securely in industrial settings (MOV.AI). Measures like this create multiple layers of defense. The end state should be that even if an attacker manages to target an AMR, the hardness of that target and the surrounding controls make it extremely difficult to cause harm, protecting both the factory's intellectual property and its operational continuity.

LOGISTICS: MITIGATING DATA RISKS IN INTEGRATED SYSTEMS

In the logistics and warehousing sector, AMRs have become indispensable for streamlining operations. Robots zip through warehouses to fetch items, scan inventory levels, and transport goods, all tied into Warehouse Management Systems (WMS) and Enterprise Resource Planning (ERP) software that coordinate the entire supply chain. This high level of integration between AMRs and enterprise systems introduces valuable data flows, and wherever valuable data flows, cyber threats follow.

A primary concern in logistics is the exfiltration of, or unauthorized access to, sensitive business data. Modern warehouses generate and rely on real-time data such as inventory counts, shipment schedules, order fulfillment status, and even pricing information from suppliers. If an attacker compromises an AMR or its connected systems, they could siphon off this data to gain competitive intelligence or hold it for ransom. For instance, knowing a competitor's exact inventory and shipping schedule could allow industrial espionage or undercutting in the market. Even without direct theft, an attacker compromising an AMR to manipulate data in the WMS could cause significant disruption. For instance, if inventory records are altered to indicate shelves are fully stocked when they are empty (or vice versa), the resulting misinformation could severely impact inventory management and fulfillment processes. Such integrity attacks might result in overstocking, missed orders, or delivery delays that cost time and money.

Another risk is the disruption of tightly choreographed workflows. Logistics depend on timing – conveyors, robots, and human pickers must work in sync. An AMR that suddenly goes offline or malfunctions due to a cyber incident can create a bottleneck. For example, if a fleet of order-picking robots is managed via a cloud platform and a ransomware attack hits that platform, it could halt all picking operations across multiple warehouses. This is not hypothetical: supply chain software providers have been targeted by ransomware, causing multi-day outages. In late 2024, a ransomware attack on Blue Yonder, a major supply chain and WMS software provider, disrupted warehouse operations for many companies, including causing delays at supermarkets and a global coffee chain [cybersecuritydive.com, cybersecuritydive.com]. This incident highlights the critical dependence of logistics operations on software availability and integrity. While in that case the attack was on the software provider's systems, the lesson for any robotics deployment is clear – a single cybersecurity failure can cascade through third-party logistics (3PL) operations, trucking schedules, and retail stock levels before the root cause is even identified.

Privacy and regulatory compliance are also emerging issues. As retail and logistics intertwine (e.g., robots handling packages that contain customer information or scanning barcodes linked to customer orders), a breach could expose PII or break compliance with standards like PCI DSS if payment-related data in fulfillment systems is involved. Retail warehouses that share networks with stores may inadvertently expose credit card data environments to risk if their AMR systems are not isolated (more on Retail in the next section).

In summary, in logistics environments, AMRs must be viewed as part of a larger digital ecosystem that extends from suppliers to warehouses to retailers. A security incident at the robot level can have impacts up and down the chain: data can be stolen or corrupted, physical goods can be misrouted or delayed, and partners both upstream and downstream can be affected. This interconnected risk necessitates a proactive approach to cybersecurity, treating warehouse robots with the same rigor as one would an ERP server or a financial database, because, in effect, they are now just as critical to business continuity and success.

MITIGATING LOGISTICS RISKS

Securing AMRs in logistics requires a combination of effective network hygiene, vigilant monitoring, and securing the integration points with larger enterprise systems. Key measures include:

- **Proactive Threat Monitoring:** Set up monitoring to detect unusual outbound connections or data flows from the warehouse environment. For example, suppose an AMR or its management tablet suddenly attempts to send a large volume of data to an IP address in an unrelated geographical location. In that case, that should be flagged immediately as a potential breach or misconfiguration. Many logistics companies use Data Loss Prevention (DLP) tools at network egress points to catch unauthorized data transfers. Similarly, monitor for unauthorized use of cloud services – e.g., an AMR agent trying to upload inventory data to a personal Dropbox or unknown cloud – which could indicate an insider siphoning data or malware exfiltration. Early detection of these signals can prevent a full-blown data leak.
- **Behavioral Analytics for Operations:** Warehouses typically have predictable operational rhythms. Leverage analytics to identify anomalies, such as an unusual volume of data transfer during non-operational hours. If robots are usually idle at night, but you observe significant activity from them at 3 AM, it's worth investigating. Automated alerts can be tied to such patterns (e.g., if any single AMR reports more than X MB of data outside of 8 am to 8 pm, trigger an alert). This helps catch stealthy threats that may try to operate when they think no one is watching. It also helps detect failures – e.g., a robot stuck in a loop might generate abnormal traffic too, which could be caught and resolved before it impacts operations the next day.
- **Centralized Logging and Audit Trails:** Maintain comprehensive logs of all AMR-related activities and centralize them (for example, in a SIEM platform) for analysis. Logs should cover robot movements (from the fleet management system), any user access to the robots or their controllers, and integration logs for WMS/ERP transactions. In the event of an incident, these audit trails are invaluable for tracing what happened – did the robot receive a malicious command from an internal system? Did a particular account issue an unexpected update to inventory?

WHAT THE EXPERTS SAY



Don Capener: Right, that ties into the whole supply chain. Now, Sean, from a plant manager's perspective: maybe cybersecurity used to be just 5–10% of their world, but with more robots and advanced tech on the floor, it's becoming a much higher priority than it was a decade ago, correct?



Shaun Flaharty: By far. I think everyone in manufacturing now recognizes how important cybersecurity is. We all try to comply with the IT/OT policies and rules to keep things running safely. It's vital for manufacturing leaders to partner with their IT and OT teams to outline needs. We require two-way communication on the floor — machines talking to machines, robots knowing where to pick and place products. Technology has come a long way in just the last 3–5 years and generates tons of data to make everything work. Because we've introduced so much automation, having strong, robust security policies is critical, and we have to actually follow them.

In one of our current plant-build projects, we're designing the network with complete separation from day one. Even then, you can never be 100% safe. "One-way only" connections don't always stay that way — there are still ways for a determined attacker to get in. Josh's example about outdated Windows systems is a perfect illustration: everyone uses Windows, and if a vendor plugs an infected laptop into your production network, you've just opened the door to all kinds of problems without even realizing it.

Moreover, routinely auditing these logs can sometimes reveal slow-burn issues, such as a service technician occasionally logging in remotely at unusual times (which may be benign but could also be an insider-threat concern). Being able to “replay” events is crucial for both response and compliance, as auditors will want to see evidence that you track system access.

- **Secure Integration with WMS/ERP:** Since AMRs often interface with warehouse management or ERP systems, ensure those integration points are secured with authentication, encryption, and input validation. Use API keys or certificates for all API calls between the robot software and backend systems, storing them securely so they can’t be easily extracted. Implement certificate-based mutual authentication for these connections where feasible; this ensures the robot is communicating with the real WMS and vice versa. Additionally, apply the principle of least privilege. If an AMR only needs to read inventory levels and update task status, its account should not be able to pull complete customer lists or change pricing data. By limiting what the AMR systems can do in the enterprise software, you reduce the potential damage of a breach.
- **Lightweight Encryption and Data Validation:** Within the warehouse, utilize lightweight encryption for all wireless communications, as previously discussed for shared networks. Also, implement integrity checks on critical data fields. For instance, if a robot sends an inventory count to the WMS, the system can cross-verify that count against expected ranges or recent trends, flagging any discrepancies that could indicate an error or tampering. This type of validation can catch issues early – e.g., an attacker attempting to inject “10000 units” for an item when typical counts are typically two digits.

- **Regular Security Testing and Drills:** Conduct penetration tests that focus on the warehouse environment and the AMR-WMS interfaces. Testers might attempt to exploit the robot-to-WMS API or insert a rogue device into the warehouse to see if it can communicate with the robots. These tests can uncover issues such as open debug ports on robots, weak default credentials, or missing encryption on specific data channels. In addition to testing, conduct incident response drills that include scenarios such as “robot ransomware outbreak” or “data breach via AMR”. This prepares the team and identifies gaps in playbooks. For example, a drill might reveal that the team lacks a quick way to shut down all robots—a gap that can be addressed proactively.

By combining proactive monitoring, secure integrations, and regular testing, logistics organizations can protect their AMRs and the vast amounts of data they handle. The benefits of warehouse automation – efficiency, accuracy, speed – can be enjoyed without introducing new vulnerabilities to the business. It’s about diligence: ensuring that every time an AMR touches a piece of data or a package, that interaction is governed by security best practices. In doing so, companies also uphold customer trust, knowing their orders and data are safe, and maintain the resilience of the supply chain, even in the face of growing cyber threats.

RETAIL: BALANCING EFFICIENCY AND NETWORK SECURITY

Retailers are increasingly utilizing autonomous mobile robots in stores and fulfillment centers to enhance operations and the customer experience. In brick-and-mortar stores, you might see robots auditing shelf inventory or guiding customers to products. In e-commerce fulfillment, robotic systems assist with picking and packing to expedite the processing of online orders. These innovations drive efficiency and can boost sales, but they also introduce cybersecurity challenges in a highly connected retail IT environment.

Retail AMRs often share network resources with other systems such as point-of-sale (POS) terminals, customer Wi-Fi, inventory databases, and IoT devices like smart cameras or electronic shelf labels. This interconnection raises a critical concern: exposure of sensitive customer data. Retail networks often handle sensitive payment card information and personal data, including names, loyalty account details, and other confidential information. If an AMR is compromised, it could theoretically serve as a point of entry into the payment processing environment, thereby threatening PCI DSS compliance. PCI DSS requires strict isolation of payment systems; an insecure robot on the same network could be a weak link. For example, malware on an AMR could intercept network traffic for credit card numbers or masquerade as a fake POS endpoint, capturing transaction details. The infamous 2013 Target breach began with an intrusion into an HVAC system, which led to the installation of point-of-sale (POS) malware. One can imagine a future breach where a store inventory robot plays a similar role.

Network performance and reliability are another challenge in retail. Stores and warehouses depend on real-time updates (e.g., an AMR detects an out-of-stock item and triggers immediate replenishment). If the network is congested or unavailable, those timely updates fail to occur. In a busy retail environment, bandwidth may be shared among customer-facing services, such as guest Wi-Fi and in-store music or video streaming, as well as backend systems. Inadequate network management could result in an AMR not receiving a critical update that a high-demand item is back in stock, leading to lost sales. Or worse, a delay in a robot's operation could cause physical incidents (such as a safety command being delayed). Ensuring the quality of service for AMRs amidst the chatter of IoT devices is a technical and security issue. If a network is overloaded due to, for example, a denial-of-service attack on the store's Wi-Fi, it may indirectly hinder the robots.

Retailers must also consider insider threats and errors. For instance, floor staff or third-party vendors might inadvertently introduce risks, such as charging a personal device using a robot's USB port (if accessible) or connecting the robot to a rogue Wi-Fi hotspot for convenience. Retail has relatively high staff turnover and a high number of temporary workers; maintaining tight control over who can interact with or reconfigure AMR systems is difficult but necessary.

And finally, physical tampering poses a risk in open-store environments. Unlike a warehouse, a store is public – a customer could walk up to a robot. While most retail robots are designed to be tamper-resistant, there is always a possibility that someone may attempt mischief, such as pressing buttons to access a service menu or trying to open a panel. This is both a safety and security concern; for instance, a disgruntled former employee could attempt to sabotage a robot to cause disruption.

Retail AMRs sit at the intersection of customer experience and core business operations, which means a security incident can have direct financial and reputational consequences. A breach that exposes customer data can erode trust and incur compliance fines; an outage that affects inventory robots can result in empty shelves or unfulfilled orders. Therefore, cybersecurity for retail robotics isn't just about protecting devices – it's about protecting the brand and bottom line.

MITIGATING RETAIL RISKS

To address these challenges, retailers should integrate AMR security into their broader IT security and compliance efforts:

- **Network Segmentation and PCI Compliance:** Isolate AMRs onto dedicated networks or VLANs, especially segregating them from any guest network or networks that process payment card data. This helps ensure that even if a robot is compromised, it cannot directly reach POS systems or databases containing customer PII. Any connectivity between the AMR network and other parts of the retail environment should be routed through controlled gateways with established firewall rules. For example, an AMR might need to query the inventory database; set up an API service for that and allow the robot network to communicate only with that service, not the raw database. This approach supports PCI DSS requirements by limiting the cardholder data environment. Regular network scans and audits should verify that no unauthorized cross-connections exist, such as a rogue Wi-Fi access point bridging the segments.
- **Quality of Service (QoS) and Redundancy:** Implement QoS to prioritize AMR traffic over less critical traffic on store networks. For instance, ensure that an inventory robot's communications to the store server are given high priority, whereas guest Wi-Fi is assigned a lower priority. Additionally, consider implementing redundant network paths or fail-safes for AMRs, such as a backup 4G/LTE connection in case the primary Wi-Fi fails, allowing the robot to receive shutdown commands still or send alerts. Some retailers deploy edge computing appliances that cache critical data, such as planograms or inventory lists, locally for the robots, allowing them to continue operating even if the connection to the central server is lost. These measures maintain reliability, a crucial security aspect that prevents scenarios attackers could exploit (e.g., knowing an outage will disrupt operations).
- **Encrypted Communications and Authentication:** Just as with other industries, use strong encryption (TLS 1.3) for all robot communications. Retailers should also leverage certificate-based authentication for robots connecting to cloud services or store servers, ensuring rogue devices can't masquerade as legitimate robots. Many retail robots are cloud-managed – make sure the cloud service enforces device authentication and that communication channels are encrypted and integrity-protected. Any firmware updates or software patches for the robots should be delivered in a signed and authenticated manner to prevent tampering, as supply chain attacks via malicious updates are a concern.

WHAT THE EXPERTS SAY



Don Capener: Now, cybersecurity often comes with a trade-off: security measures can sometimes slow down operations. Josh, how do you balance the need for strong cybersecurity with the need to keep operations efficient and productive?



Josh Steinman: Honestly, the key is empathy for the operational side. My co-founder led Amazon's industrial control system security program, and our team includes folks from places like Caterpillar and SpaceX — people who know that in manufacturing, uptime is king. We designed our security solutions to be as passive as possible, to “fail open” and never shut down a line. In other words, we make sure the security layer doesn't interfere with production.

You also have to be smart about the tools you deploy. Some legacy security systems will overwhelm a team with alerts. I know of one global consumer products company that installed an older security platform, and it generated over a billion security alerts a day across their plants. A billion! The team bought it mainly to satisfy the board's concern, but nobody could possibly respond to that many alerts, and sure enough that company still got hit by an attack not long after. So, security measures have to be effective and practical. They should protect you without drowning you in noise or slowing down your workflow.

- **Access Controls and Insider Mitigation:** Utilize RBAC to restrict access to the AMR control systems. For instance, store associates may only have the ability to view the robot's status or pause it in an emergency, whereas corporate IT can change configurations or software. Implement MFA on any administrative interfaces. Additionally, provide training to store staff on the robots – for example, instruct them not to plug random devices into the robot or not to attempt to “help” the robot unless instructed (some may attempt to reset it if it appears stuck). Simple physical measures can also help keep charging stations or maintenance ports in staff-only areas, if possible, to reduce opportunities for public access.
- **Continuous Monitoring and Anomaly Detection:** Retail environments can be chaotic, so a robust monitoring system helps maintain security visibility. Deploy tools that monitor for anomalies, such as an AMR sending data to an unknown external site (which could indicate a breach) or unusual robot behavior on the floor. For example, if an inventory robot that usually patrols during off-hours is active at noon when customers are around, something might be wrong (it could be malfunctioning or compromised). Cameras or the robots' sensors might assist here – if the robot's camera detects someone persistently tampering, it could send an alert to security personnel. Logs from robots, such as error codes or manual interventions, should be fed into the store's incident management system. Many retailers already have centralized monitoring systems for point-of-sale (POS) and building security; integrating robot telemetry into these systems provides a fuller picture.
- **Penetration Testing and Security Audits:** Conduct regular and thorough testing of the retail environment for vulnerabilities, including AMR systems. This should involve evaluating wireless security, ensuring robots operate on a properly secured Wi-Fi network with strong encryption, and assessing whether an attacker could spoof the Wi-Fi to hijack robot communications.

Test the cloud management interface for exposed APIs and simulate insider threats to understand the potential damage a malicious employee could inflict. Additionally, review compliance to confirm that integrating robots hasn't inadvertently expanded the PCI DSS scope. For example, if an incident alert from a robot includes a list of affected products containing partial credit card numbers, that could introduce compliance risks. Address any findings promptly and treat these assessments as essential maintenance, on par with physical inventory checks or financial audits.

By taking these steps, retailers can mitigate cybersecurity risks while still maximizing the operational benefits of AMRs. The guiding principle is to embed security into the deployment: from day one, design the network, processes, and training around the robots with security in mind, rather than bolting it on later. Retail executives should see AMR security as an extension of customer data security and store resilience. With proper safeguards, AMRs can be a secure and reliable asset, scanning shelves and expediting orders without opening new avenues for attackers or causing unintended downtime. In turn, this protects the retailer's revenue and reputation in an era where both innovation and security are essential for competitive success.



GOVERNMENT TECHNOLOGY: SECURING PUBLIC SECTOR AUTOMATION

Municipal governments, law enforcement agencies, and public services are increasingly deploying AMRs to enhance operations. From autonomous street-cleaning robots to police robots for surveillance or bomb disposal, these public sector applications span traffic management, infrastructure inspection, public safety, and more. Even beyond civilian agencies, homeland security and defense organizations utilize AMRs for tasks such as munitions transport and reconnaissance, although military use falls outside the scope of this white paper. The public-facing nature of government AMRs and their integration into critical civic infrastructure present a distinct set of security considerations.

Public accessibility is one significant risk factor. Government robots often operate in open environments, such as city streets, parks, and transit stations, where they can be directly accessed or tampered with by anyone. This exposure elevates the risk of physical interference or device attachment. For example, a security robot patrolling a transit hub could have a malicious device covertly attached by a passerby, rendering it a mobile spy tool for eavesdropping on police communications. The physical security challenge is far greater than in private facilities: you cannot fully control the environment around a public sector robot.

Interconnection with smart-city infrastructure is another concern. AMRs may be integrated with traffic light systems, surveillance camera networks, or utility sensors to perform their duties. A cyberattack on an AMR could thus impact those connected systems. Consider a city that uses robots for bridge or tunnel inspections, sending data to a central municipal database. If an attacker compromised the robot, they might not only steal or alter inspection data, potentially missing a critical safety issue, but also potentially gain access to the city's broader network. Many cities have been hit by ransomware in recent years, severely disrupting services. An AMR could be an entry point if not secured, given it often operates with privileged access within secure facilities (e.g., sewer systems or electrical substations it's inspecting).

The confidentiality of law enforcement data is paramount. A breach (e.g., crime scene footage) could compromise cases or compromise officer safety. Robots may be used to handle sensitive evidence or information. A police bomb-disposal robot or a drone might send live video and data back to a command center. If such a feed were intercepted or manipulated, it could reveal investigative details or be used to spread misinformation.

Supply chain security is paramount in government contexts. Public agencies typically procure robots from private vendors via contracts. There is a risk that a vendor-supplied robot could come with hidden vulnerabilities or even deliberate backdoors. Without rigorous vetting, agencies might deploy AMRs with outdated software, known CVEs, or undisclosed remote access features (which may have been intended for maintenance but are exploitable). This has parallels with concerns surrounding the use of foreign-made drones, where some have feared the potential for built-in data exfiltration. Firmware integrity and origin are thus significant issues – agencies need assurance that the robots they purchase do not contain pre-loaded threats.

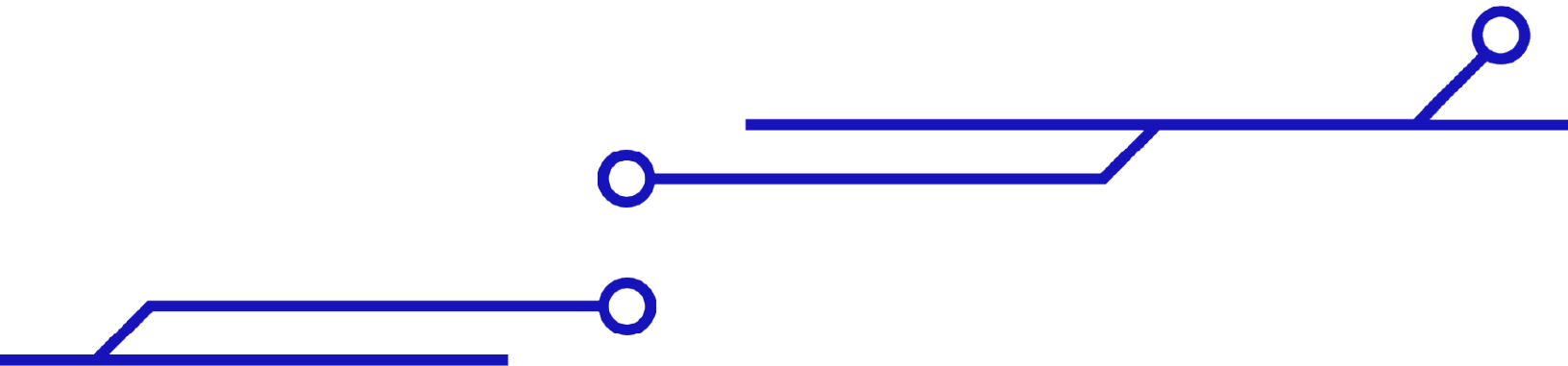
MITIGATING GOVERNMENT TECHNOLOGY RISKS

Ensuring the secure deployment of AMRs in government operations requires a multi-layered approach that covers cyber and physical security, as well as procurement practices:

- **Network Isolation and Secure Architecture:** Government agencies should segment AMRs on dedicated networks that are isolated from general IT and public networks. For instance, a city's sanitation robots should communicate only on a secure channel specific to the waste management system, not on the city hall office network. Use VPNs or private cellular networks for communications rather than public Wi-Fi. If robots connect to cloud services, ensure those cloud environments are FedRAMP-authorized (for federal use) or meet equivalent security benchmarks. Essentially, treat the robot network as a sensitive operational network, similar to SCADA for utilities, with strict access controls and monitoring at its ingress and egress points.
- **Strict Access Controls and Identity Management:** Implement strong authentication for any commands or data access related to AMRs. Law enforcement or emergency response robots should have command systems secured with multi-factor authentication (MFA) and digital certificates, ensuring that only verified personnel can operate or modify them. Introduce digital identity verification for the robots themselves – each device should have a unique cryptographic identity. This prevents scenarios where an attacker could introduce a fake robot or simulate one; the system would reject commands or data from an entity that isn't recognized and authenticated. Role-based access is crucial: a transit department official shouldn't have access to police robot controls, for example, and within a police department, only specific roles should be able to access a robot's evidence data.
- **Real-Time Monitoring and Incident Response:** Deploy continuous monitoring tuned explicitly for the behaviors of government AMRs. For example, geo-fence the operational areas and set alerts if a robot leaves its designated zone, which could indicate theft or hijacking. Monitor for abnormal telemetry, such as a robot transmitting large video files to an unknown server (potentially indicating data exfiltration) or repeated deviations from its typical movement path, which could suggest someone physically pushing it off course or a malfunction. Given the high risk, an automated response is valuable. If a public safety robot is suspected of being compromised, it should automatically shut down or revert to a safe mode and alert backup teams. Government SOC's (Security Operations Centers) should incorporate these robots into their drills – for example, by practicing scenarios involving hacked city robots and coordinating responses between cyber teams and field operators.
- **Supply Chain Security and Procurement Standards:** Governments should incorporate cybersecurity requirements into their Requests for Proposals (RFPs) and contracts for Autonomous Mobile Robots. This means requiring vendors to follow secure development practices and provide evidence of testing, such as penetration test results or code audit reports. Compliance with standards like NIST SP 800-53, FedRAMP (for cloud components), or CMMC (for DoD suppliers) should be mandated where applicable. Additionally, require that vendors deliver devices with the latest security patches and with any default credentials changed. Consider performing acceptance testing on delivered units – essentially a mini penetration test – to catch any issues before the robots go operational. By asserting these requirements up front, agencies can avoid the scenario of deploying insecure devices and then scrambling to fix them later.

- **Privacy and Data Handling Policies:** For any AMR that collects or stores citizen data (such as video footage, facial recognition data, and license plates), ensure that strict data management policies are in place. Data should be encrypted, access should be logged and audited, and retention policies must be enforced (i.e., data should be retained only as long as necessary). If a robot is compromised, having limited data on it (and that data encrypted) will minimize fallout. Additionally, perform Privacy Impact Assessments when introducing such systems to identify and mitigate privacy risks proactively.

By implementing these safeguards, government agencies can more confidently integrate AMRs into public services, law enforcement, and smart-city initiatives without increasing risk. It is about taking a “security-first” approach: assuming these systems will be targeted and planning defenses and responses accordingly. As a positive outcome, a securely deployed AMR can enhance public safety (e.g., keeping officers out of harm’s way) and improve city services (more efficient maintenance and cleaning) while maintaining public trust. The key for leadership is to ensure that innovation in the public sector is matched with rigorous risk management, so that the benefits of autonomous systems are realized safely.





03 | AMR CYBERSECURITY GOVERNANCE FACTORS

Ensuring robust cybersecurity for Autonomous Mobile Robots (AMRs) requires a comprehensive approach that integrates human awareness, proactive monitoring, and effective measurement of security performance. This governance framework encompasses training personnel, implementing sophisticated monitoring systems, and continuously evaluating cybersecurity effectiveness to adapt to evolving threats. By unifying these elements, organizations can establish a resilient and responsive security posture that safeguards AMR operations.



ADDRESSING HUMAN CONSIDERATIONS

No cybersecurity strategy is complete without considering the people who interact with technology. Human factors play a critical role in securing AMR systems. Employees, contractors, and third-party technicians can either enhance security or introduce vulnerabilities. Therefore, building a security-conscious workforce is essential to complement technical measures.

Training programs should educate personnel on recognizing anomalies in robot behavior, safeguarding credentials, and adhering to proper maintenance procedures. For example, if a robot suddenly deviates from its usual route or enters a restricted area without authorization, it could signal tampering or malware. Rather than assuming someone else reprogrammed it, employees should report such incidents to security or IT immediately. Every employee should act as a sensor within the security network, detecting issues that technology might miss.

Physical inspections of robots should be part of routine operations. Warehouse workers who swap batteries or load items should visually inspect the AMRs for unusual devices, unfamiliar wires, or signs of tampering. In hospital settings, a nurse or technician might notice a piece of tape covering a sensor or an unexpected device attached to a robot. Integrating these inspections into daily workflows through checklists that include security points can significantly enhance overall security awareness.

Insider threats, whether intentional or accidental, also pose a risk. Even well-meaning employees can create vulnerabilities, such as plugging unsecured USB drives into a robot's port to charge personal devices. This could introduce malware or provide unauthorized access. Clear policies must prohibit such practices, and role-based access control (RBAC) should ensure that employees have access only to the resources necessary for their roles. For example, a maintenance contractor's account should only be active during their scheduled work period, limiting exposure if credentials are later compromised.

Fostering a culture of cybersecurity awareness is both crucial and challenging. Leadership must communicate that security is a priority by providing regular updates, recognizing employees who report issues, and integrating security awareness into performance metrics. Organizations may also implement periodic phishing simulations or "rogue robot drills" to test staff awareness of unusual robot behavior. These exercises are not intended to deceive employees, but rather to keep them engaged and reinforce their responsibility in safeguarding AMR systems.

In conclusion, human factors can either strengthen or undermine AMR security. By effective training, empowering, and occasionally testing personnel, organizations add a vital layer of defense that complements their technical safeguards. A vigilant and prepared workforce can detect issues that automated systems miss and prevent mistakes that attackers could exploit.

WHAT THE EXPERTS SAY



Shaun Flaharty: As automation increases, we can't forget about our people. The factories of the future will have more robots and autonomous systems, but that doesn't mean people go away — their roles just change. Instead of manual labor, they'll be managing processes and overseeing systems. That means companies need to invest in upskilling their workforce. In my mind, the future of manufacturing is people working with automation. It's not about robots replacing people; it's about people and robots working together to do more. So training operators and staff to handle advanced tech securely is crucial. And through it all, safety is still number one. You can add all the robots you want, but you have to ensure none of it compromises safety. A hacker making your automated systems unsafe is the worst-case scenario — it puts your people, your brand, and your whole company at risk. Safety and security have to go hand in hand.

PROACTIVE LOGGING, MONITORING, AND ALERTING

Effective cybersecurity begins with visibility. You cannot protect what you cannot see, and you cannot respond to incidents you never detect. That's why logging, monitoring, and alerting are foundational components of a proactive security posture for AMR systems.

Comprehensive Logging: Every interaction between AMRs and enterprise systems should be logged to create a detailed audit trail. This includes both successful and failed login attempts to the AMR control console, commands issued to robots, movements and tasks completed, data accessed or transferred, and any system events (such as sensor errors or communication drops). Centralizing these logs is equally important, as it involves consolidating them into a Security Information and Event Management (SIEM) system or a centralized logging server. Centralization enables correlation; for example, if one robot experiences a login failure and shortly after another robot on the other side of the facility also has a strange event, you might connect the dots as a coordinated attack. Logs provide the forensic evidence needed to investigate incidents, but they also provide operational insights to fine-tune systems and detect anomalies.

Real-time Monitoring: With logs and data in place, continuous monitoring can take over. Modern monitoring systems, often powered by AI and machine learning, can analyze patterns in log data and robot telemetry in real time. For instance, machine learning can determine that a particular AMR typically transfers ~5 MB of data per hour during working hours. If suddenly 50 MB of data is sent at 2 AM, an anomaly is flagged. Another example: monitoring can detect if a robot that usually operates on weekdays is active on a Sunday, which might indicate unauthorized use. These systems essentially create a behavioral baseline for what's "normal", and then alert on deviations that might signify a security issue (or even a safety or maintenance issue – e.g., a motor drawing unusually high current could indicate a mechanical problem).

Alerting and Response: It's not enough to detect; the system must quickly alert the proper personnel. Alerts should be configured to prioritize critical issues, such as the detection of a known malware signature on an AMR or multiple robots repeatedly failing authentication, which could indicate a brute-force attack. These alerts may be routed to the SOC, the on-call engineer, or even trigger automated containment actions.

WHAT THE EXPERTS SAY



Don Capener: Jeremy, you consult with many manufacturers. How do you help them manage that balance between security and operational efficiency?



Jeremy Smyth: I tend not to use the word "balance" because you really can't compromise on security. Like Josh said, you need empathy for what the manufacturer is good at. Most of these companies are excellent at making their product — whether it's paper towels or chocolate bars — but cybersecurity isn't their area. That's why they bring in experts like us. Instead of balancing, I focus on control. You either have control over your systems or you don't; you're either protected or you're not. I'll give you an example: a client told me, "Our production machines aren't on the internet; they're on an internal network only." But when I connected to their Wi-Fi, I could actually see those machines. Clearly, they were exposed in ways they didn't realize. The lesson is that manufacturers should stick to what they do best, and ensure they have the right controls and expert help to secure the rest. There's really no middle ground on security.

The key is to minimize alert fatigue: tune the system so that alerts are meaningful by reducing false positives through refined rules. Regularly review and adjust alert thresholds and logic based on experience.

Routine Log Reviews: In addition to real-time monitoring, organizations should establish procedures for regularly reviewing logs and security events. Sometimes, slow, subtle attacks or policy violations may not trigger loud alerts, but they can be spotted in logs by a savvy analyst. For instance, reviewing weekly logs may reveal that a specific service account accessed the AMR system from an IP address that doesn't match known facilities – a possible indication of credential misuse. These periodic audits serve as a safety net to catch what automated systems might not flag as urgent.

Integration with Incident Response: Logging and monitoring systems should be seamlessly integrated into the incident response plan to enable swift, decisive action. When an alert is triggered, such as an “AMR deviating from route” or transmitting an unusually large amount of data, teams must know how to verify the issue and respond appropriately. This could involve anything from contacting local staff for verification to automatically isolating a robot from the network if a breach is suspected.

For instance, if a monitoring system detects an AMR transmitting excessive data to an unknown server during off-hours, the system should immediately flag the anomaly and alert a security engineer. Prompt intervention, such as remotely shutting down the compromised AMR and dispatching personnel to secure it, can prevent data exfiltration from escalating. The key is ensuring that monitoring outputs are directly linked to clear, predefined actions, allowing threats to be contained before they cause significant damage.

In conclusion, visibility is a powerful tool in cybersecurity. By diligently logging and intelligently monitoring AMR systems, organizations gain the power to detect intrusions or failures at the earliest moment and respond decisively. It shifts security from reactive (finding out after damage is done) to proactive (acting when signs first appear), which is crucial for minimizing the impact of any threat.



MEASURING AND MONITORING CYBERSECURITY EFFECTIVENESS

To ensure the ongoing success of cybersecurity strategies for AMR deployments, organizations should establish measurable indicators that track performance and highlight areas for improvement. Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) provide a structured approach to assessing the effectiveness of the security program and identifying residual risks.

Key Performance Indicators (KPIs) focus on achieving positive security outcomes and optimizing process efficiency. For AMR security, important KPIs include:

- **Incident Response Time:** How quickly can the team detect and respond to a security incident involving an AMR? A faster response time, measured from initial alert to containment actions, reduces the potential impact of an incident. Executives might set a KPI, such as “All high-severity AMR incidents are responded to within 30 minutes.” Continuous monitoring and clear runbooks help drive this metric down.
- **System Uptime:** This measures the availability of AMR systems, essentially determining the amount of operational time lost due to security issues. If applying security controls causes frequent downtime or if incidents lead to robots being offline, that’s a problem. A strong security program will maintain high uptime (e.g., “AMR fleet operational $\geq 99.5\%$ of the time”). Tracking uptime can reveal whether security measures are too onerous, resulting in false positives that shut things down unnecessarily, or, conversely, if incidents are causing unacceptable downtime.
- **Threat Detection Rate:** This metric measures the percentage of real or simulated threats successfully identified by the security monitoring system. For example, during drills or red-team exercises, it is essential to determine whether most attempted breaches are detected. A high detection rate indicates that monitoring and alerting mechanisms are functioning effectively. Conversely, a low detection rate suggests potential blind spots that need addressing. Just as AI-based monitoring systems continuously learn and adapt, this KPI should improve over time, reflecting a progressively stronger ability to detect and respond to attacks.

WHAT THE EXPERTS SAY



Don Capener: Shaun, you’ve managed massive projects and CAPEX budgets. How do you justify or incorporate the cost of cybersecurity when you’re projecting at the bottom line? For example, when you’re presenting a new project to a CFO or calculating ROI, how do you factor in investing in cybersecurity measures versus the risk?



Shaun Flaharty: It can be a tough sell at first, but we’ve learned you have to bake cybersecurity in from the start. We try to include security infrastructure in the upfront design of new facilities or systems. I haven’t personally used the kind of continuous monitoring Josh mentioned yet — that might be the next step — but even on day one, we build as much protection as we can. Yes, it adds cost upfront, but that cost is really about ensuring business continuity. If we ever get hacked badly, production stops and no product goes out the door — that’s a far bigger cost. So I’d call cybersecurity spending a cost of doing business now, like insurance.

We also follow through as we expand or upgrade systems: every time we add something, we stick to those security standards. It only works if you keep it consistent. In the end, it’s much cheaper than a major disruption. We’ve all seen the news; it’s happened too often to both big and small companies. Just last year, it felt like every month another manufacturer got hit and had to shut down operations for days. The C-suite has become very sensitive to this issue.

These KPIs provide insight into the efficacy and responsiveness of the security program. They should be reported to management through a dashboard that displays, for example, the average incident response time for this quarter compared to last quarter, the number of incidents detected, and other relevant metrics. Trends can indicate improvement or the need for additional resources.

Key Risk Indicators (KRIs), on the other hand, focus on the presence of risk factors and potential vulnerabilities. They act as early warning signs of issues that could lead to an incident if not addressed. For AMRs, useful KRIs include:

- **Unauthorized Access Attempts:** This refers to the count of failed login attempts to AMR control systems or instances of unauthorized physical access to a robot, as recorded by tamper sensors or access control systems. A spike in unauthorized access attempts might indicate an active attack or probing. For example, “Failed login attempts to the robot management portal exceeding 5 per day” could be a KRI threshold that triggers an investigation.
- **Suspicious Outbound Data Transfers:** Monitor the frequency and volume of data leaving the AMR network to external destinations. If you notice unusual patterns, such as data being sent to an unrecognized IP address or volumes significantly exceeding expected levels, that’s a strong indicator of a breach. You might set a KRI, such as “No more than one anomalous data transfer event per quarter.” If you exceed this threshold, the risk is trending upward, and you should act, such as conducting a security assessment or tightening controls.
- **Bandwidth Usage or Network Congestion:** In shared network setups, track bandwidth utilization and the frequency of AMR communications experiencing latency or congestion issues.

If bandwidth use is increasing or you see frequent network saturation alarms, it could indicate either more devices sharing the network (possibly due to someone adding an unauthorized device) or an ongoing attack, such as a slow DoS. Either way, it’s an indicator that your network may need upgrades, or that unknown devices are present.

By actively monitoring these KPIs and KRIs, organizations gain valuable insight into the effectiveness of their cybersecurity measures. For example, if incident response times—a key performance indicator—are not improving quarter over quarter, it may indicate a need for better training or additional staff. If unauthorized access attempts (a KRI) suddenly increase, it suggests an emerging threat that warrants a closer examination of system vulnerabilities or a review of access policies.

Regularly analyzing these indicators enables data-driven decision making for security. Leadership can allocate budget and resources where the metrics show weaknesses – perhaps investing in better monitoring tools if detection rates are low, or in network upgrades if bandwidth issues are rising. It also provides accountability, as security teams can report to the C-suite and board on concrete metrics, demonstrating progress or highlighting challenges in a quantifiable manner.

In essence, KPIs and KRIs for AMR security create a feedback loop for continuous improvement. They make the abstract goal of “secure our robots” into something tangible and trackable. Over time, an organization should aim to consistently meet KPI targets (e.g., responding quickly enough and maintaining minimal downtime due to security issues) and keep KRIs within acceptable ranges, with no persistent, unexplained anomalies. When those conditions are met, it indicates a robust security posture that can be sustained even as threats evolve.



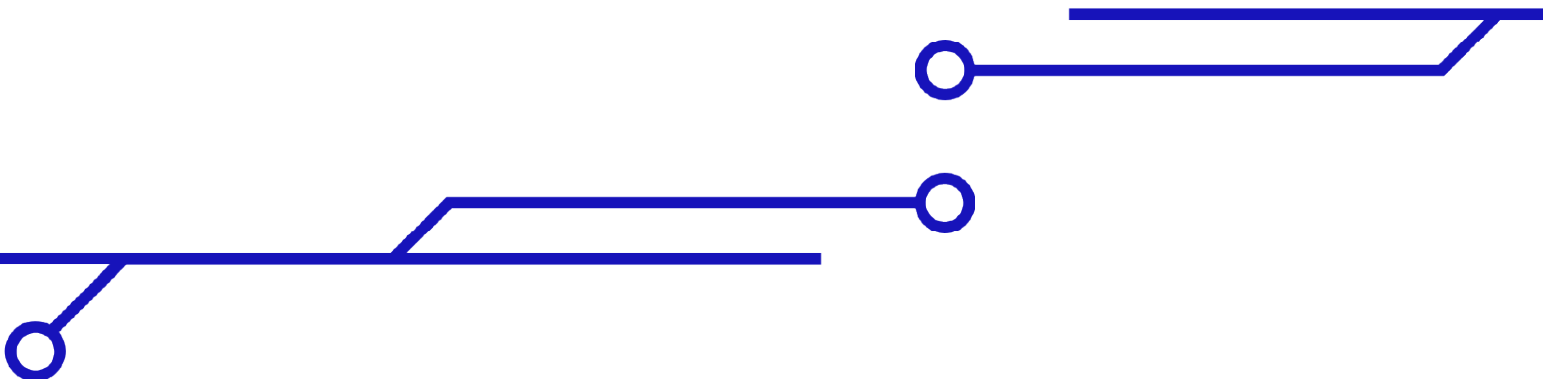
04 | CONCLUSION

The adoption of Autonomous Mobile Robots is revolutionizing industries by unlocking new efficiencies, enabling continuous operations, and redefining the potential of automation. However, with this transformation comes the responsibility to embed cybersecurity into every phase of AMR strategy—from planning and procurement to daily operations and maintenance.

By proactively addressing cybersecurity, companies can enhance their resilience and drive long-term innovation. Adequate security measures are not just about risk mitigation; they empower organizations to scale automation confidently, ensuring productivity, safety, and trust remain intact.

A well-rounded approach to AMR security focuses on these key areas: Industry-Specific Adaptation, Network Segmentation, Supply Chain Integrity, Physical Security, Integration Security, Incident Response, Zero Trust, Workforce Training, and Continuous Improvement. By addressing each of these focus areas, organizations can establish a solid cybersecurity framework that protects AMR operations and enables them to achieve aggressive automation and digital transformation goals.

Ultimately, organizations that prioritize cybersecurity will transform AMRs from potential vulnerabilities into valuable assets, enabling innovation while safeguarding their data, systems, and personnel. This confidence, built on robust security practices, becomes a critical competitive advantage in an increasingly connected world.



This research paper was prepared with the assistance of OpenAI's ChatGPT (March 2025 Version), a large language model developed by OpenAI. The tool was used to generate text, assist with brainstorming, enhance clarity, and improve the manuscript's structure. While portions of the text were generated with AI assistance, all final content was thoroughly reviewed, edited, and approved by the author.

[01] OpenAI. (2025). ChatGPT (March 2025 Version). Retrieved from <https://openai.com>.

[02] Cyngn – Warehouse Automation Trends 2024: Thompson, E. (April 22, 2024). “16 Warehouse Automation Trends for 2024.” Cyngn. (Amazon operated over 750,000 robots in its warehouses by 2023, a 40% increase from 2022; 52% of warehouse managers plan to increase automation spending.)

a. <https://www.cyngn.com/blog/16-warehouse-automation-trends-for-2024#:~:text=Smart%20warehouses%2C%20powered%20by%20IoT,from%202022%27s%2052%20%2C000%20robots>

b. <https://www.cyngn.com/blog/16-warehouse-automation-trends-for-2024#:~:text=52,the%20demand%20for%20intelligent%20automation>

[03] TechTarget – Cybersecurity Statistics 2020: Pryor, J. (January 10, 2025). “35 Cybersecurity Statistics to Lose Sleep Over in 2025.” TechTarget. (Reported a 107% surge in IoT malware attacks in 2023).

<https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020#:~:text=7,in%20IoT%20malware>

[04] Ivanti Blog – 5 New Aethon TUG Robot Vulnerabilities: Feldstein, S. (April 19, 2022). “5 New Aethon TUG Robot Vulnerabilities Expose Healthcare Facilities to IoMT Hackers.” Ivanti. (Summary of zero-day flaws in Aethon TUG healthcare robots and their potential impacts)

a. <https://www.ivanti.com/blog/5-new-aethon-tug-robot-vulnerabilities-expose-healthcare-facilities-to-iomt-hackers#:~:text=Some%20of%20the%20IoMT%20vulnerabilities,robots%20could%20allow%20hackers%20to>

b. <https://www.ivanti.com/blog/5-new-aethon-tug-robot-vulnerabilities-expose-healthcare-facilities-to-iomt-hackers#:~:text=1,in%20the%20robots%E2%80%9999%20online%20portal>

[05] TechTarget – Cybersecurity Statistics 2025: Pryor, J. (Jan 10, 2025). “35 Cybersecurity Statistics to Lose Sleep Over in 2025.” TechTarget. (Includes Gartner prediction: 45% of orgs will experience supply chain attack by 2025, and SonicWall report of 107% increase in IoT malware attacks in 2023)

a. <https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020#:~:text=1,from%20Skybox%20Security>

b. <https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020#:~:text=7,in%20IoT%20malware>

[06] NIST – Guide to Industrial Control Systems (ICS) Security: Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (June 2022). “Guide to Industrial Control Systems (ICS) Security” (NIST SP 800-82 Rev. 3). National Institute of Standards and Technology. (Recommends dividing OT networks into isolated segments with strong access controls as part of a defense-in-depth strategy).

<https://nvlpubs.nist.gov>

[07] Darktrace – DETECT/OT Product Brief: Darktrace. (n.d.). “DETECT/OT Product Brief.” Darktrace. (Describes AI-driven monitoring solutions that learn normal device behavior to autonomously detect anomalies, such as unusual communication times or abnormal data volumes in industrial environments). darktrace.com

[08] Cybersecurity Dive – Blue Yonder Ransomware Recovery: Jones, D. (Dec 2, 2024). “Blue Yonder moves closer to full recovery after November ransomware attack.” Cybersecurity Dive. (Attack on supply chain software Blue Yonder impacted major companies like Starbucks and Morrisons with operational disruptions)

a. <https://www.cybersecuritydive.com/news/blue-yonder-recovery-ransomware/734275/#:~:text=The%20Arizona,in%20connection%20with%20the%20attack>

b. <https://www.cybersecuritydive.com/news/blue-yonder-recovery-ransomware/734275/#:~:text=Morrisons%2C%20which%20has%20about%20500,the%20situation%20has%20significantly%20improved>

[09] CISA – Autonomous Ground Vehicle Security Guidance: Cybersecurity and Infrastructure Security Agency (2022).

“Autonomous Ground Vehicles Security Guide – Transportation Systems Sector.” (CISA guidance emphasizing converged physical and cyber security for autonomous systems; notes that resilience relies on a combined approach)

<https://www.cisa.gov/sites/default/files/publications/Autonomous%2520Ground%2520Vehicles%2520Security%2520Guide.pdf#:~:text=to%20the%20enterprise%2C%20such%20as,in>

[10] Omron Automation. “AMR Safety Assessment.” Omron Industrial Automation Europe. Accessed March 26, 2025.

<https://industrial.omron.eu/en/services-support/services/safety-service/machine-safety-services/amr-safety-assessment>

[11] MOV.AI. “Autonomous Mobile Robot Cybersecurity: Threats and Mitigation.” MOV.AI Blog. Accessed March 26, 2025.

<https://www.mov.ai/blog/autonomous-mobile-robot-cybersecurity-threats-and-mitigation>