Open Access

Online Journal of
Robotics & Automation Technology

Iris Publishers

Research Article

The Cyber Vulnerability in Automation of Material Handling and Logistics Systems

MD Sarder*

Department of Engineering Technologies, Bowling Green State University, USA

***Corresponding author:** Department of Engineering Technologies, Bowling Green State University, USA

Received Date: November 19, 2019

Published Date: February 04, 2020

Abstract

The level of automation in material handling and logistics industries has increased significantly in recent years. This increase in automation and integration is driven by customer expectations, technology shifts, and pursuit for perfections among others. The material handling and logistics industries not only become effective and efficient, but also became competitive in the market Place. On the other hand, this increased automation exposes vulnerability to cyberattacks. The frequency and impact of cyberattacks on businesses doubled in the last five years and expected to triple in the next five years. Cybersecurity breach poses a dynamic challenge to businesses and threatens their smooth operations and competitive advantage. Study reveals that one in three small businesses do not have the resources in place to protect themselves. Some businesses are more vulnerable to cyberattacks that others, but none is spared from potential attacks. Businesses need to be strategic in cyber defense and create a resilient system that minimizes the impact of cyberattacks. This paper mainly focuses on challenges faced by cybersecurity and how businesses, especially the material handling and logistics should do to address those challenges.

Introduction

Cybersecurity is the ability to prevent, defend against, and recover from disruptions caused by cyber-attacks from adversaries. The cyber-attacks have been classified as passive and active attacks [1,2]. Passive attacks are difficult to detect and are mainly used on confidential data. The passive attacks have been classified as eavesdropping and traffic analysis. Active attacks are classified as masquerade, replay, message modification and denial of service. The hackers use malware to Penetrate into a system and breach the critical data like customers' payment and personal details. Cyber breaches are increasing every year affecting the confidentiality, integrity, and availability of data [2,3]. The material handling supply chain systems are becoming markedly vulnerable to cyber-attacks. Over time, material-handling devices are connected with corporate networks, so they can integrate and share information across the enterprises. This helps the companies to monitor and manage operations remotely, but it also increases the chances of cyber-attacks. When the system is broadly networked, it can be accessed by a malware. Many companies manage external vendors where information sharing and accessing is involved. This can generate vulnerabilities especially if the processes are automated. The company should take up measures like mapping the data flow in supply chain, planning a comprehensive risk assessment, aligning with emerging standards, and setting clear expectations in all supply chain contracts. Some of the impacts cyber-attacks can have on businesses are:

- Altering the installation settings can cause physical damage to the equipment.
- Changing the production settings can lead to defective products which will result in loss of profit.
- Malfunction in the installation of the equipment may lead to release of harmful pollutants in the industry site and the surroundings.
- Theft of confidential data like manufacturing secrets and customer information may be a risk to the company.

Cybersecurity has become increasingly critical for any industries including logistics and material handling. Today, the stakes are higher than ever, as most companies operate on some kind of technology [3-5]. Technology has become more than a supplement to a company's operations, and hence cybersecurity became a daily necessity.

Cybersecurity impacts for material handling and logistics based technologies should be viewed with the same level of scrutiny as a typical IT infrastructure for any organization. The fact that the focus of this technology is on IoT based devices, and often not typically associated with "sensitive" information thus is not a target of cyber criminals, is naïve. Information technology resources (hardware, software, networks, data, and people) should always be assessed to the impact of the organization with the common principle of confidentiality, integrity, and availability (also known as the CIA Triad) (Figure 1) [6-8].

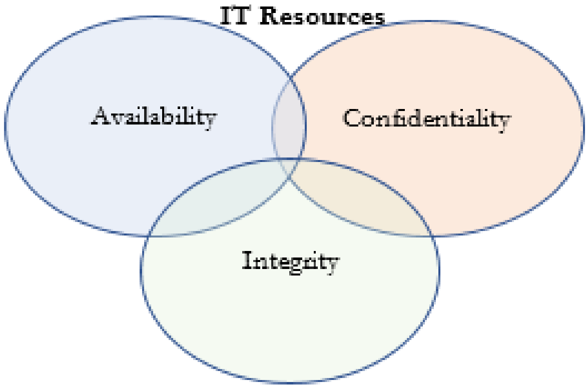

Figure 1: Common principle of confidentiality, integrity, and availability.

Confidentiality does not mean that all data within an organization needs the highest level of protection. It is up to each organization to determine the value of the data and have it classified. Data that is required to be protected by law or is valuable to the competitive advantage of an organization, such as intellectual property, should have proper controls in place to protect them from unauthorized disclosure. The integrity of the data is the assurance that only those authorized to add or modify the data can do so. Of course, every organization would want their data to be accurate, but certain functions within an organization are more critical than others to ensure they are accurate. IT resource availability is critical, especially in manufacturing when the process is halted, and product cannot be produced. The reliability of systems for some processes may be more important than others and understanding the risks and developing redundancy is important.

The primary focus in this paper is to identify cybersecurity challenges and how companies, especially the material handling and logistics companies should do to address those challenges. In addition, this paper discusses cybersecurity in general, cyber security framework, potential impact of cybersecurity breaches, and implications of cybersecurity on material handling.

Significance of Cybersecurity

Because it hurts their bottom-line. The frequency of cyberattacks and costs associated with cyberattacks are increasing at a higher pace. According to a recent survey of 254 companies, the average cost of a data breach in 2017 is $11.7 million [9]. The cost went up from $7.2 million in 2013 Figure 2. Costs include everything from detection, containment, and recovery to business disruption, revenue loss, and equipment damage. A cyber breach can also ruin a company's reputation or customer goodwill. The cost of cyber-crime varies by country, organizational size, industry, type of cyber-attack, and maturity and effectiveness of an organization's security posture. The frequency of attacks also influences the cost of cyber-crime. It can be observed without statistics that cybersecurity incidents have exploded. 23 Million security breaches were recorded globally in 2011 and by 2013 it hiked to 30 million, a 12.8% annual growth [9]. It has been reported that every year the cost of cyber-crimes is increasing at the rate of 23% per year. On an average it is costing the industries US $11.7 million. The number of successful breaches per company each year has risen to 27% which is approximately 102 to 130 [9]. There has been an increase in ransomware attacks from 13% to 27% [9]. Information theft is the most expensive consequence of cyber-crime. There has been a rise in the cost component of information theft of 35% in 2015 to 43% in 2017. The average cost of malware attack costs around $24 million [9]. It has been analyzed that companies spend most on detection and recovery. It usually takes approximately 50 days to resolve a malicious insiders attack and 23 days to resolve ransomware attack [9] (Figure 2).

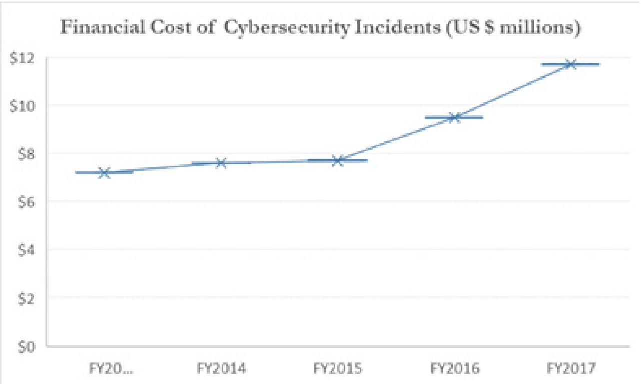

Figure 2: Financial Cost of Cybersecurity Incidents (US $ millions).

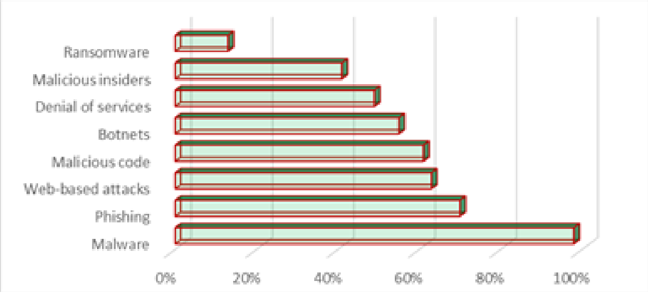

Figure 3: Types of cyber-attacks experienced by companies.

With each year there is a significant amount of increase in number of security breaches that happen globally. The large number of attacks may put companies in risk with sensitive information and data, but also can put companies at risk for increased costs from the attacks or even preventative measures. According to the average increase per year percentage of security breaches, by the year 2021, the number of attacks will nearly be reaching 70 million. Organizations must acknowledge that their core operations whether they are logistics or material handling are the equivalent to any other IT systems for any organization. It runs on hardware, software, operating systems, databases, and networks. Thus, it requires the same, if not greater attention and resources that critical systems in other organizations receive. Malware and Web-based attacks are the two most costly attack types [9] (Figure 3).

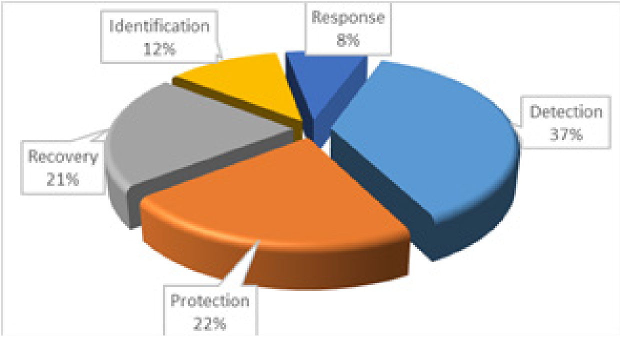

Figure 4: Percentage of efforts dedicated to different phases of cybersecurity.

Information security principles need to be assessed with all systems. This starts with senior management of the organization supporting the resources to ensuring security. Establishing policy and a risk governance structure to these systems. Once this has been created, a formalized program following a commonly accepted risk framework such as NIST or ISO will provide the guideline necessary to securing any systems. Cybercrime detection and recovery activities account for 55 percent of total internal activity cost (35 percent plus 20 percent), as shown in (Figure 4) [9].

Implications of Cybersecurity on Material Handing and Logistics Industries

Study reveals that financial sector is the top target for cyberattacks followed by utilities, aerospace and defense, and technology sectors. Manufacturing, logistics, and transportation sectors attract medium cyberattacks while communications, education, and hospitability sectors are least vulnerable to cyberattacks. Figure 5 shows the cost of cyberattacks by industry sectors in 2017 [9] (Figure 5).

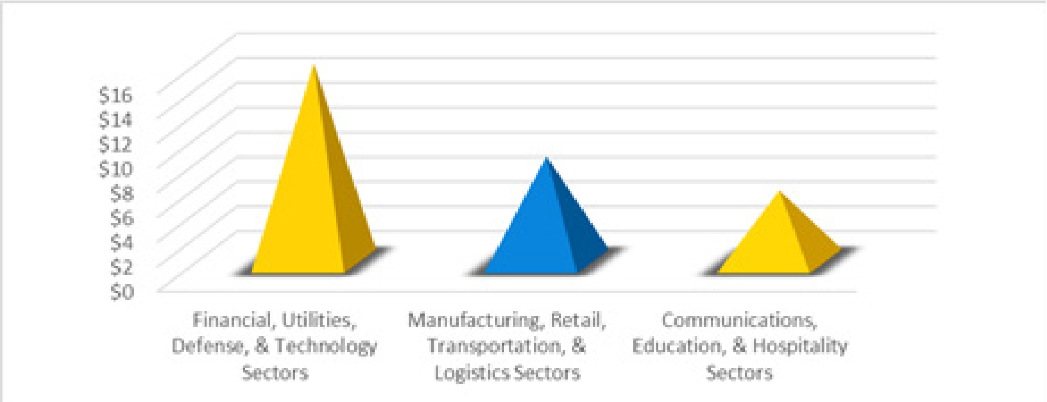

Figure 5: Cost of cyberattacks by industry sectors (US $ millions).

Material handling and logistics industry groups include Automated Storage/Retrieval Systems, Automated Guided Vehicle System, Conveyors and Sortation, Cranes, Electrification and Controls, Hoists, Lifts, Loading Dock Equipment, and Software Systems [10]. Almost all these systems relate to a bigger system when in real time operation. For example, an Automated Storage and Retrieval System (AS/RS) is a combination of equipment and controls that handle, store and retrieve materials as needed with precision, accuracy and speed under a defined degree of automation. This AS/RS system can be an extremely large, computer-controlled storage/retrieval systems totally integrated into a manufacturing and distribution process. In general, AS/RS consists of a variety of computer-controlled methods for automatically depositing and retrieving loads to and from defined storage locations [10]. AS/RS system includes Horizontal Carousels, Vertical Carousels, Vertical Lift Modules, and/or Fixed Aisle (F/A) Storage and Retrieval Systems, the latter utilizing special storage retrieval machines to do the work needed to insert, extract and deliver loads to designated input/output locations within the aisles being served.

Another example of material handling system is Automated Guided Vehicle (AGV). An AGV consists of one or more computer-controlled wheel-based load carriers that runs on the plant floor without the need for an onboard operator or driver. AGVs have defined paths or areas within which or over which they can navigate. Navigation is achieved by any one of several means, including following a path defined by buried inductive wires, surface mounted magnetic or optical strips or alternatively by way of inertial or laser guidance.

The AGVs or any other devices within material handling and logistics industries are smart devices and can be connected through Internet of Technologies (IoT) into an integrated system. Any parts of this interconnected systems is vulnerable to cyberattacks. Cyber criminals can exploit this vulnerability and take control of individual device, part of a system, or the whole system and create substantial damage including service disruptions, data loss, equipment damage, other property loss, or injury to people. No one should take the risk of cybersecurity on material handling systems lightly.

Current Challenges and How to Address Those Challenges

Companies are facing ever-increasing challenges of cyberattacks. In many cases, they are struggling to cope up with those challenges as they are adopting new technologies, operating on web-based applications, working with multi-level constituents, and operating in a competitive environment. Other challenges include lack of skilled manpower, lack of awareness of cybersecurity, lack of readiness due to financial commitment. Following sections highlight some critical challenges and how to respond those challenges.

Dependence on mobile and web-based technologies

Among others customer expectations, efficiency of operations, supply chain visibility, and convenience are driving companies to rely on increasing use of web-based and mobile technologies. This dependence creates vulnerable online targets. Due to a growing number of online targets, hacking has become easier than ever. In customer transaction, usage of mobile devices and apps have exploded. According to a 2014 Bain & Company study, mobile is the most-used banking channel in 13 of 22 countries and comprises 30% of all interactions globally [11]. In addition, customers have adopted online/mobile payment systems, which is vulnerable to cyberattacks.

Enacting a multi-layered defense strategy can reduce vulnerability. This ensures that it covers the entire enterprise, all endpoints, mobile devices, applications, and data. Where possible, companies should utilize encryption and two- or three-factor authentication for network and data access. Some institutions are utilizing advanced authentication to confront these added security risks, allowing customers to access their accounts via voice and facial recognition. Companies invest the most on network layer (online/mobile) protection compared to protection of any other layers. Figure 6 shows the percentage of 2017 spending [9] of companies to protect various layers of security vulnerability (Figure 6).

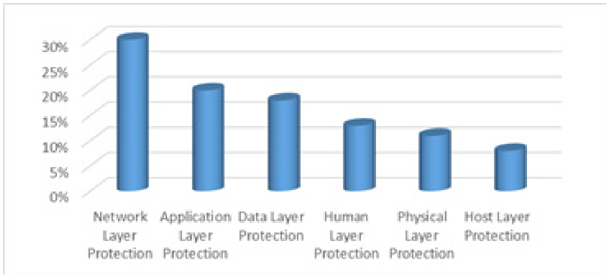

Figure 6: Percentage of spending by companies to protect their security in 2017.

Proliferation of internet of things (IoT)

Internet of things (IoT) is a concept of integrated network where a wide array of devices, including appliances, equipment, automated guided vehicles, software systems, and even buildings, can be interconnected primarily through internet connections. Due to IoT, all these components become smart and subject to cyberattacks. One of the recent MHI articles [12] on "Truck Takeovers?" highlighted the vulnerability of devices when they are connected with other systems. IoT revolves around machine-to-machine communication; it's mobile, virtual, and offers instantaneous connections. There are over one billion IoT devices in use today, a number expected to be over 50 billion by 2020 [11]. The problem with wide network of interconnected devices is that many cheaper smart devices often lack proper security infrastructure and creates multitude of access points. When each technology has high risk, the risk grows exponentially when combined. Multiple access points also increase the vulnerability of cyberattacks. Again, enacting a multi-layered defense strategy that protect the entire enterprise, all endpoints, mobile devices, applications, and data is necessary.

Systems vs individual security

No companies are working in isolation. They interact with suppliers/vendors, investors, third party logistics providers, freight forwarders, insurance providers, and many other stakeholders. Figure 7 shows a simplified Cloud based vendor-managed system where a system of companies are sharing information with each other. If any of these parties is hacked, the individual company is at risk of losing business data or compromising employee information. For example, the 2013 Target data [11,13] breach that compromised 40 million customer accounts was the result of network credentials being stolen from a third-party heating and air conditioning vendor. A 2013 study indicated [13] that 63% of that year's data breach investigations were linked to a third-party component. Transportation vehicles and their monitoring system was hacked in 2015. About 1.4 million vehicles were impacted by the cyber security related recalls [14] (Figure 7).

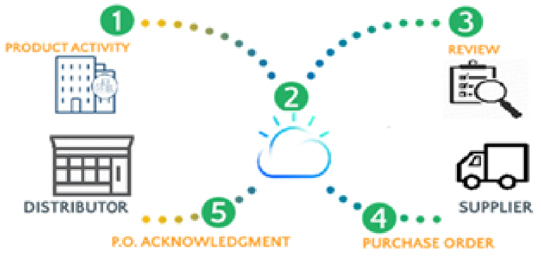

Figure 7: Cloud based vendor-managed inventory.

The paramount priority is to ensure the security of whole system alliance instead of focusing on individual company. Performing a third-party vendor assessment or creating service-level agreements with third parties can significantly reduce the vulnerability of the whole system. Companies can implement a "least privilege" policy regarding who and what others can access and create a policy to review the use of credentials with third parties. Companies could even take it a step further with a service level agreement (SLA), which contractually obligates that third parties comply with company's security policies. The SLA should give the company the right to audit the third party's compliance.

Information loss and theft

Critical information such as trade secrets, operation data, tools & techniques, and customer data provides competitive advantage. Loss or theft of sensitive and confidential information as a result of a cyber-attack is detrimental to the companies. Such information includes trade secrets, intellectual properties (including source code), operational data, customer information and employee records. The loss or theft of this data not only incurs direct costs, but also involves dealing with lost business opportunities and business disruption.

Companies should deploy extensive data encryption techniques and continuously backing-up data. This can help to safeguard against ransomware, which freezes computer files until the victim meets the monetary demands. Backing up data can prove critical if computers or servers are locked for various reasons. In addition to backing up data, companies should patch and whitelist software frequently. A software patch is a code update in existing software. They are often temporary fixes between full releases of software. A patch may fix a software bug, address new security vulnerability, address software stability issues, or install new drivers. Application whitelisting would prevent computers from installing non-approved software, which are usually used to steal data.

Lack of cybersecurity awareness and readiness to address

Despite major headlines around cybersecurity and its threats, there remains a gap between companies' awareness of cybersecurity, potential consequence of cyberattacks, and company readiness to address it. In the last year, hackers have breached half of all U.S. small businesses. According to the phenomenon Institute's 2013 survey [11], 75% of respondents indicated that they did not have a formal cybersecurity incident response plan. Sixty-six (66%) percent of respondents were not confident in their organization's ability to recover from a cyberattack. Further, a 2017 survey [13] from cybersecurity firm Manta indicated that one in three small businesses do not have the resources (skilled manpower, security system, tools, and money) in place to protect themselves. As mentioned earlier in this report, that most of the cyber-attacks are targeted to financial companies, but manufacturing, logistics, and service companies are not spared from these attacks. According to the same study, in 2013, 88% of the attacks initiated against financial companies are successful in less than a day. However, only 21% of these are discovered within a day, and in the post-discovery period, only 40% of them are restored within a one-day timeframe [13].

Real-time intelligence is a powerful tool for preventing and containing cyberattacks. The longer it takes to identify a hack, the more costly its consequences. To gain real time intelligence, companies must invest in enabling security technologies including the following:

- Security intelligence systems
- Advanced identity & access governance
- Automation, orchestration & machine learning
- Extensive use of cyber analytics & user behavior analytics
- Extensive deployment of encryption technologies
- Automated policy management
- Innovative systems such as block chain

Innovative technologies are Evolving and their full benefits are still unknown, but companies should be on the forefront of adopting new technologies. As the application and utility of block chain in a cybersecurity context emerges, there will be a healthy tension but also complementary integrations with traditional, proven, cybersecurity approaches [15]. Companies are targeting a range of use cases that the block chain helps enable from data management, to decentralized access control, to identity management.

Conclusion

Cybersecurity has become an essential part of business life. It poses a dynamic challenge to companies and threatens their smooth operations and competitive advantage. The increasing attention to the dangers of cyberattacks is on the rise, but unfortunately majority of the companies are not well equipped to address the issue. Despite increased attention around cybersecurity and its threats, there remains a gap between companies' awareness of cybersecurity, potential consequence of cyberattacks, and company readiness to address it. High magnitude of potential financial impact of cybersecurity continually compelling companies to be resilient, invest in security defense, and address this from a system perspective rather than an individual company perspective.

Among others, companies face critical cybersecurity challenges as they are adopting new technologies, operating on web-based and mobile applications, working with internal and external partners, and operating in a competitive environment. Other challenges include lack of skilled manpower, lack of awareness of cybersecurity, lack of readiness due to financial commitment. While these challenges are difficult, companies can minimize the impact by deploying tactical and strategic initiatives including enacting a multi-layered defense strategy, extensive encryption techniques, securing access points, creating service-level agreements with third parties, and invest in security technologies. Addressing cybersecurity challenges not only prevent business disruptions, but also improves competitive advantages.

Acknowledgement

None.

Conflicts of Interest

No conflict of interest.

References

1. Borghesi P (2018) Guarding Against Cyber Threats.
2. Ezrati M (2018) Cybersecurity: A Major Concern and a Great Business Opportunity.
3. Polatidis N, Pavlidis M, Mouratidis H (2018) Cyber-attack path discovery in a dynamic supply chain maritime risk management system. Computer Standards & Interfaces 56: 74-82.

4. Windelberg M (2016) Objectives for managing cyber supply chain risk. International Journal of Critical Infrastructure Protection 12: 4-11.

5. Yağdereli E, Gemci C, Aktaş AZ (2015) A study on cyber-security of autonomous and unmanned vehicles. The Journal of Defense Modeling and Simulation: Applications Methodology Technology 12(4): 369-381.

6. Gay C, Horowitz B, Elshaw J, Bobko P, Kim I (2017) Operator Suspicion and Decision Responses to Cyber-Attacks on Unmanned Ground Vehicle Systems. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 61(1): 226-230.

7. Cybersecurity in the Age of Smart Manufacturing.

8. (2017) Industrial systems: What are the potential impacts of cyberattacks?

9. (2017) Cost of Cyber Crime Study.

10. MHI Industry Groups.

11. Melissa Lin (2018) Cybersecurity: What Every CEO and CFO Should Know.

12. Soltes F (2018) Truck Takeovers?

13. Bernard Marr (2017) The Future of the Transport Industry - IoT, Big Data, AI and Autonomous Vehicles.

14. National Highway Traffic Safety Administration report on Vehicle Cybersecurity.

15. Arman Jabbari A Kaminsky P (2018) Blockchain and Supply Chain Management. MHI Whitepaper.