CYBERSECURITY AND ITS IMPLICATION ON MATERIAL HANDLING AND LOGISTICS

MHI Solutions community

CICMHE
COLLEGE-INDUSTRY COUNCIL
ON MATERIAL HANDLING EDUCATION

MD SARDER
MATTHEW HASCHAK

Cyber Security and Its Implication on Material Handling and Logistics

MD Sarder[1] and Matthew Haschak[2]
[1]Department of Engineering Technologies
[2]Information Technology Services
Bowling Green State University

February 2019

Abstract

The frequency and financial 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. Despite widespread attention to the dangers of cyberattacks, many companies are not well equipped to address the issue. 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. Various Governments and businesses are taking many measures in order to prevent these cybercrimes. Besides various measures, cybersecurity is still a very big concern to many. This paper mainly focuses on challenges faced by cybersecurity and how businesses, especially the material handling and logistics should do to address those challenges.

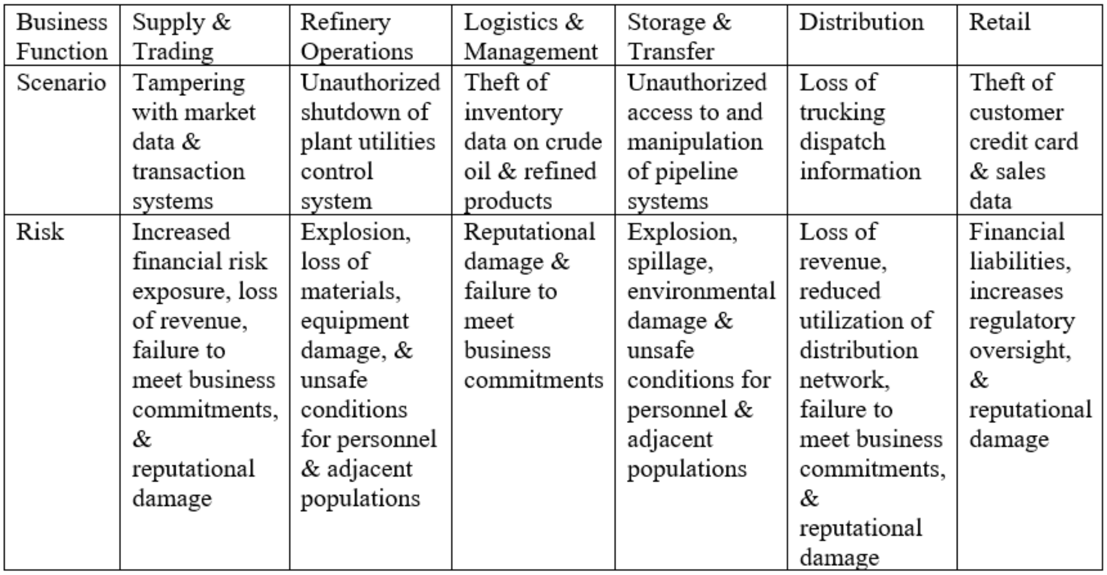
1.0 Introduction

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.

Table 1 describes some potential scenarios that can impact business functions and potential risks they carry for businesses.

Table1: Example of potential downstream cybersecurity risks through the value chain.



Business Function	Supply & Trading	Refinery Operations	Logistics & Management	Storage & Transfer	Distribution	Retail
Scenario	Tampering with market data & transaction systems	Unauthorized shutdown of plant utilities control system	Theft of inventory data on crude oil & refined products	Unauthorized access to and manipulation of pipeline systems	Loss of trucking dispatch information	Theft of customer credit card & sales data
Risk	Increased financial risk exposure, loss of revenue, failure to meet business commitments, & reputational damage	Explosion, loss of materials, equipment damage, & unsafe conditions for personnel & adjacent populations	Reputational damage & failure to meet business commitments	Explosion, spillage, environmental damage & unsafe conditions for personnel & adjacent populations	Loss of revenue, reduced utilization of distribution network, failure to meet business commitments, & reputational damage	Financial liabilities, increases regulatory oversight, & reputational damage

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 necessity like a car.

"Think of [cybersecurity] more as safety and security in roads and cars. The car hasn't really changed in the last 30 years, but a lot of security is built in, and it's not sexy until the moment it saves your life. You've got bits that are hidden – airbags – and bits there to remind you to be safe like seatbelts…Some of it is about good behaviour and good attitude, some of it is about physical security to remind you there is a risk, and some of it is baked in to save you."
– Sian John, Senior Cybersecurity Strategist at Symantec

Cybersecurity impacts for material handling/supply chain-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].

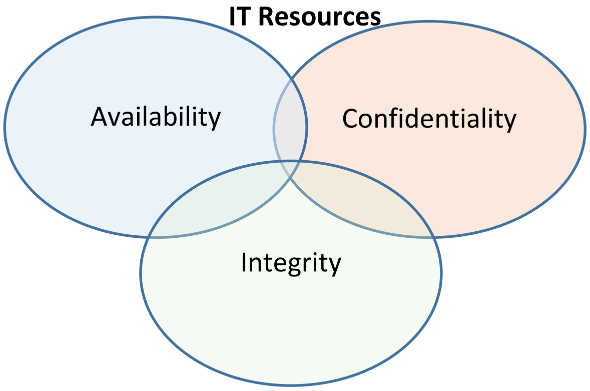


Figure 1: Common principle of confidentiality, integrity, and availability

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 when cost effective is important

In addition to the common principles, it is imperative that it is clear that life safety is the absolute priority. Any system that had a direct impact on the protection or saving of lives or could result in the injuring or taking of a life takes the highest level of precedence in terms of cyber security protections. Once the risk assessment has occurred utilizing the CIA triad principles, an action plan to address the proper level of controls needs to be developed. Organizations will address these control options using commonly available frameworks such as the ISO 27001 or the NIST Cybersecurity Framework, explained in Figure 2 [4].

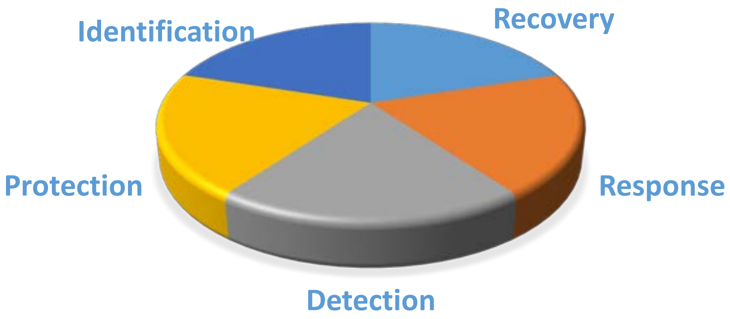


Figure 2: NIST Cybersecurity Framework

The primary focus in this white 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 white paper discusses cybersecurity in general, NIST cyber security framework, potential impact of cybersecurity breaches, implications of cybersecurity on material handling, and how to build a resilient cybersecurity system that addresses various aspects of cyber security framework.

2.0 Why do Companies Need to Worry about 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 3). 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].

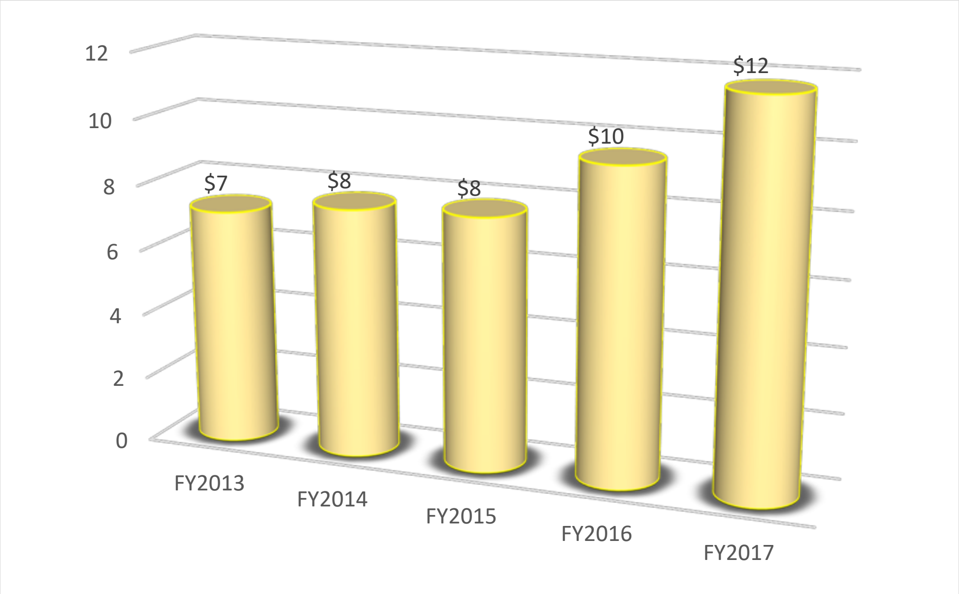


Figure 3: Financial Cost of Cybersecurity Incidents (US $ millions)

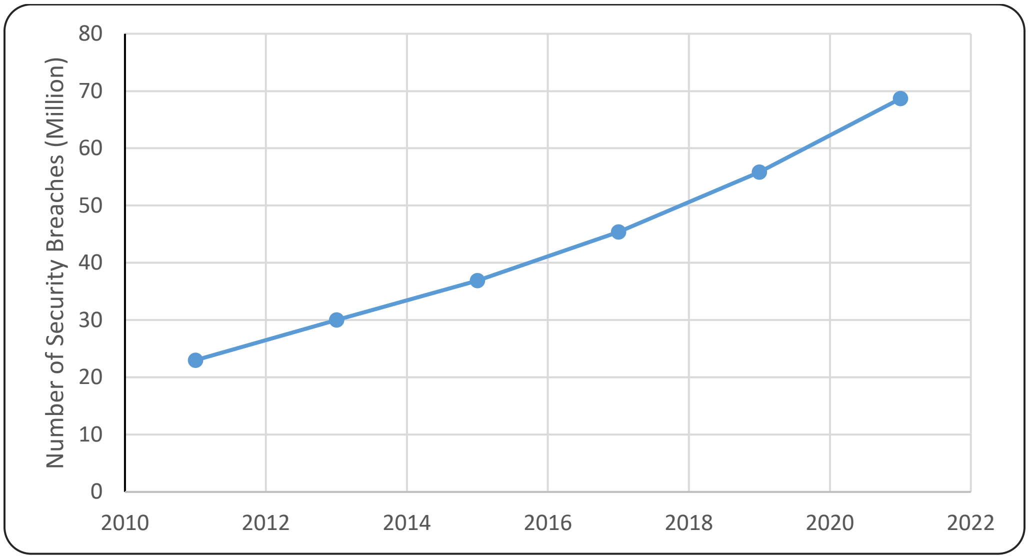


Figure 4: Annual Security Breaches Global Estimate

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 (Figure 4). 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 (Figure 5) [9].

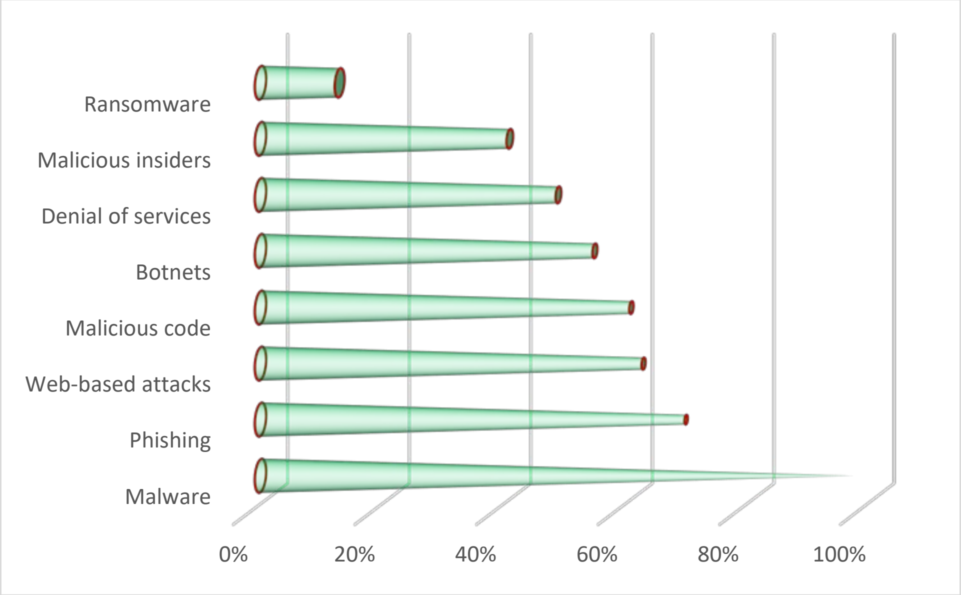


Figure 5: Types of cyber-attacks experienced by companies

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 6 [9].

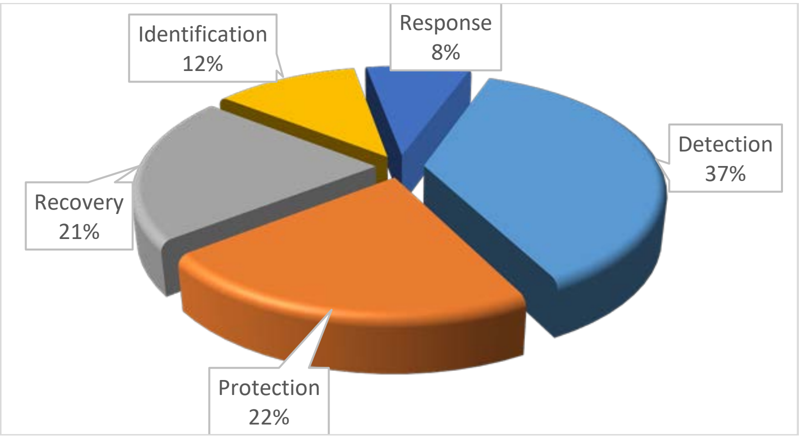


Figure 6: Percentage of efforts dedicated to different phases of cybersecurity

3.0 Implications of Cybersecurity on Material Handing

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 7 shows the cost of cyberattacks by industry sectors in 2017 [9].

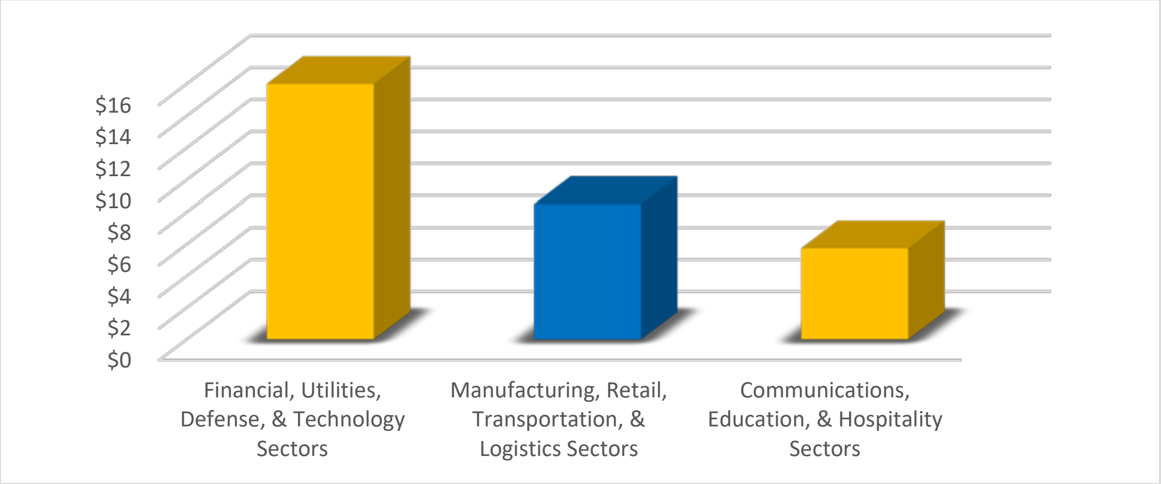


Figure 7: Cost of cyberattacks by industry sectors (US $ millions)

Solutions Groups bring MHI members together with equipment and systems users to collaborate and address common challenges and opportunities in manufacturing and the supply chains in a “safe harbor” environment. MHI’s 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 of these systems are connected with 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. Figure 8 shows some examples of AGVs [10].

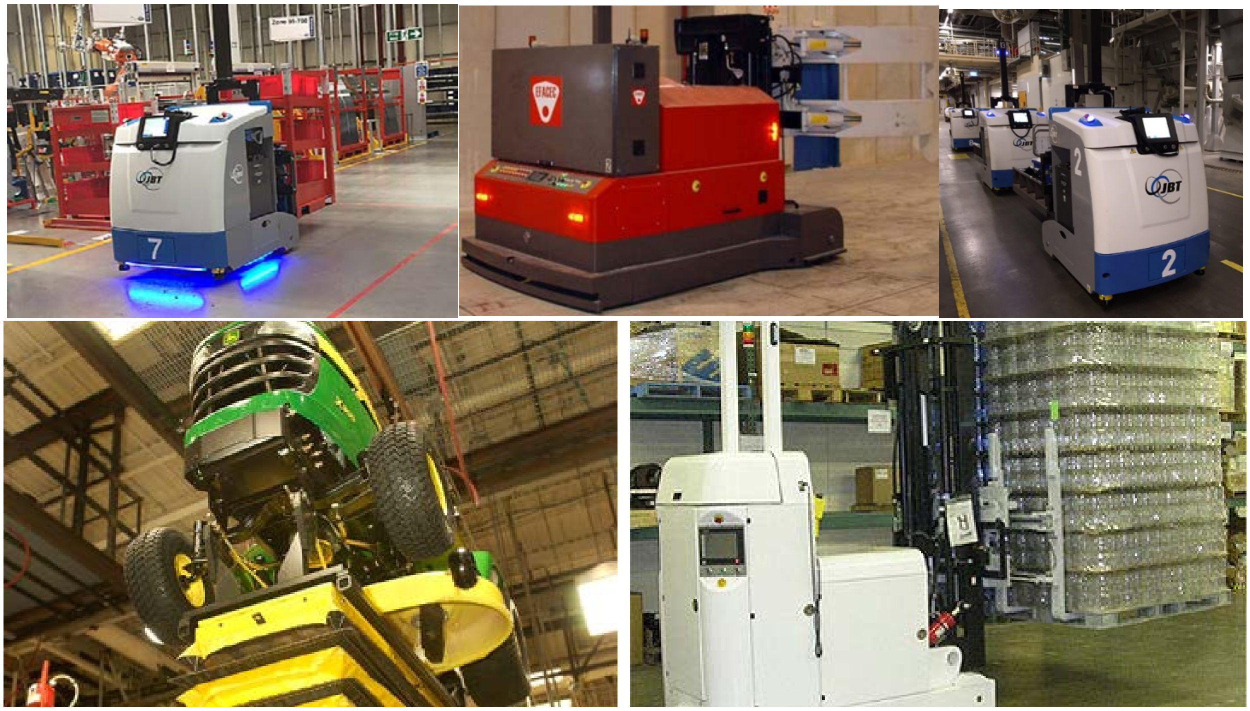


Figure 8: Automatic Guided Vehicle Systems [10]

Above AGVs or any other devices within any industry groups of MHI 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. There is a need to create a resilient material handling system.

4.0 Building Resilient Cybersecurity Systems

Material handling and logistics systems comprise of various equipment, devices, software, etc. Most of these are connected with the computer system and internet, and hence are a part of Industry 4.0. Industry 4.0, also known as smart manufacturing, is customized with products and services made with advanced technologies like internet of things (loT), analytics, robotics, artificial intelligence (AI), advanced materials, and augmented reality. Cyber risk become potentially further reaching and greater when supply chain, factories, customers, and operations are connected. Digital supply networks, smart factories, and connected devices are an integrated cybersecurity plan to mitigate the cyber risks. Digital supply network (DSN) is the merger of digital and physical production and distribution methods. The idea behind DSN is to combine the dispersed supply chains, integrated marketing, product development, manufacturing and distribution, and collecting data and feeding back into the system. DSN helps to improve the management and flow of materials, and efficient use of resources and supplies to improve customer satisfaction. The organizations must understand what data needs to be shared and how to protect the data that should not be shared. During expansion of the organization, broader network of vendors is added in the process. The new partners get their own vendors. Safe policies and guidelines must be developed to track and protect the data from unlawful vendors. Industrial control systems (ICS) rely mostly on automation, which are controlled through connected systems like ERP, manufacturing execution, supervisory control and data acquisition. They may make the process easy and smooth, but the huge network could be exposure points that could be misused or manipulated which in turn results in financial loss, lowered product quality or other cybercrimes. Some of the guidelines the organization could follow is to prevent the cybercrimes are to have an integrated approach like built in security and safeguard sensitive data. The following is a systematic framework (Table 2) to assess the risk for AGVs as an example.

Table 2: Security Framework Assessment for AGVs (*example)

Identify	
Asset Management	• A physical inventory of all AGVS should be documented and maintained • An inventory of all software and systems used to maintain the AGVS is needed • Data mapping and system flows for communicating within the AGVS • All human resource roles that are involved in the procurement, maintenance, operation or support of the AGVS needs to be listed
Business Environment	• How critical is the function of AGVS for the organization

Governance	• Organization policy of securing AGVS • Any legal or regulatory requirements on the security of AGVS • Program around regular risk management of AGVS
Risk Assessment	• Known vulnerabilities of all software, hardware and systems used to maintain AGVS is needed • Involvement in information sharing organizations/lists should be enacted • Business impact analysis on availability of AGVS • Prioritizing risks and responses
Risk Management	• Establish risk management processes and agreement from stakeholders • Establish organizational risk tolerance levels as pertains to AGVS
Supply Chain Risk Management	• Establish risk management measures as it pertains to third party supplier to support of AGVS

Protect	
Identity, Authentication and Access Control	• How to manage the provisioning and deprovisioning of accounts for users with access to the maintenance, configuration, and IT operation of the AGVS systems • Restrict physical access to those systems • Restrict and monitor remote access to those systems • Restricted access on principle of least privilege and separation of duties to those systems • Based on criticality, implement a segmented network for AGVS from rest of organizational LAN • Implement controls to ensure access lines up to roles • Authenticate users appropriately to systems within the AGVS (MFA, password controls etc.)
Awareness/Training	• Train all users in AGV systems to understand responsibilities commensurate to their role and involvement • Train third parties as well • Make executives aware of their roles and responsibilities • Cyber and physical security staff trained on roles and responsibilities
Data Security	• Entire data life cycle as it pertains the AGVS should be documented and protected (data at rest, in transit, storage, disposal) For example, when decommissioning an AGVS, all data should be wiped from hard drive and memory before repurposing • Backups of data and configurations of AGVS • Given the importance of integrity with AGVS, validation of data and instructions must be verified
Information Protection Processes and Procedures	• Baseline configuration of AGV systems maintained and secured • Systems Development Life Cycle (SDLC) of all AGV systems • Change control for modifications to AGV systems • Proper backup of AGV systems with integrity checking and testing • Policies established • Data is properly retained and destroyed based on retention schedule • Metrics established for protection effectiveness • Testing of response and recovery plans • Vulnerability management plan established
Maintenance	• Regular maintenance schedule established for AGV systems • Controls around remote maintenance established and monitored

Protective Technology	• Audit logs are created, maintained and reviewed • Any remote media involved with AGVS is restricted • Redundancy built in (manual override, backup network, key components to achieve resiliency based on criticality of availability of AGVS

Detect	
Anomalies and Events	• Establish a baseline of normal AGVS activity • Identify how to detect anomalous behavior • Correlate the behavior with other systems • Understand impact levels of different behavior • Understand alert thresholds/false positives
Security Continuous Monitoring	• Monitor all components of the AGVS environment o Physical o OS o Software o Network o Personnel • Conduct vulnerability scans against AGVS environment
Detection Process	• Establish roles for those responsible for detection to ensure accountability • Ensure processes are tested, communicated and improved

Respond	
Response Planning	• Ensure response plan is executed based on policy
Communication	• Members of response plan know their roles and responsibilities • Proper reporting of incidents in the AGVS environment
Analysis	• Proper response per notifications are investigated • Impact to the AGVS is understood • Forensic performed if necessary • Incident properly categorized • Processes established based on category and impact
Mitigation	• Contain and mitigate incident • Document newly discovered and develop plan
Improvements	• Lessoned learned from incident • Update response plan

Recover	
Recovery Planning	• Ensure a recovery plan is executed after incident within the AGV system
Improvements	• Incorporate lessons learned • Update recovery strategies
Communication	• Manage communication including public message if applicable • Manage reputation • Ensure all relevant parties are updated regarding incident in AGV system

** Note: These are just some subcategories within the NIST Cybersecurity framework and are provided as guidance questions to conducting the analysis of AGVS and not intended to be a comprehensive list of questions. Each organization will need to adjust based on their environment.*

One of the major and important steps in the cybersecurity framework is to protect the company and its information. If proper preventative steps are taken, those companies may be less susceptible to a cyber-attack. Some companies take several measures in order to prevent or protect their data from being intruded. These steps could be a firewall in order to block the attacks, intrusion detection to alert the company of the attack, antivirus to help stop the attacks that were able to access the data, and encryption of the data and information in case it had been tampered with or stolen. These measures are significant in the framework of cybersecurity in order to prevent the process of having to recover and the costs that accompany that recovery.

Throughout any supply chain organization, there are a considerable number of systems, networks, people, data, and applications. Providing a completely secure environment is not attainable. It ultimately comes down to risk management. There are countless threats and vulnerabilities out there and a limited number of resources to prevent them from being exploited. As a result, an organization needs to be able to allocate resources effectively to mitigate the risk to the organization. **Function**: Identify **Category:** Risk Assessment of the NIST Cybersecurity Framework is a critical component to helping an organization determine where to focus their resources. Risk is calculated with the following formula:

Risk = Threats x Vulnerability x Impact ……………………………………………………………… (1)

The values assigned are subjective but are typically assigned by a cross functional group of subject matter experts that can provide relative values based on experience, organizational knowledge, and the familiarity with the current information security threat landscape.

The following is a high-level template (Table 3) to guide the risk assessment process for AGVS (note: this is a ***fictional scenario*** used as an example):

Table 3: Risk Assessment Charts

Threat Description	**1 2 3 4 5 6 7 8 9 10**
Automated Guided Vehicle Systems are used throughout the organizations manufacturing facilities to deliver products and materials to and from the manufacturing floor. Reports from trusted third parties indicated that a software vulnerability can be remotely executed over Transmission Control Protocol (TCP) Port 22 that can alter the navigation of the device including being remotely controlled by the threat agent.	

Vulnerability Description	**1 2 3 4 5 6 7 8 9 10**
TCP Port 22 is the Secure Shell (SSH) service used to remotely access the core operating system of the AGVS. This is a required service and disabling the service is not an option if we want to allow IT staff from corporate offices to provide software updates to the AGVS. The AGVS software engineers are working on a patch, but it has not yet been fully developed and tested. *(see protective control description section)*	

Impact Description	**1 2 3 4 5 6 7 8 9 10**
If the intruder is able to access the AGVS via the SSH vulnerability, they have the ability to change the navigation of the device that could result in death, injury, damage to property and lost productivity	

Protective Controls Description		
Control	**Description**	**Comment**
Access Control Lists	The AGVS only allow certain IP addresses to connect to it via port 22	Our AGVS lists currently consist of 13 static IP v4 addresses allocated to authorized staff
Border Firewall	Port 22 is blocked by our Internet based firewall which would only allow non-LAN connection via the Virtual Private Network (VPN)	This would effectively stop a hacker from spoofing one of the authorized IP addresses
Certificate Based Authentication	Any connection via TCP will only be allowed to proceed based on a valid certificate on the connecting host	The certificate is a self-signed certificate installed on most corporate issued laptops, thus the intruder would need to compromise one our systems to attack the AGVS

Risk	=	Threat	X	Vulnerability	X	Impact
210		7	X	3	X	10

This exercise would be conducted across the all the systems within the organizations portfolio. Based upon the score, an organization will be able to determine and justify which systems provided the greatest risk to the organization and thus how to allocate resources to mitigate.

5.0 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.

5.1 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. Following figures shows the percentage of 2017 spending [9] of companies to protect various layers of security vulnerability.

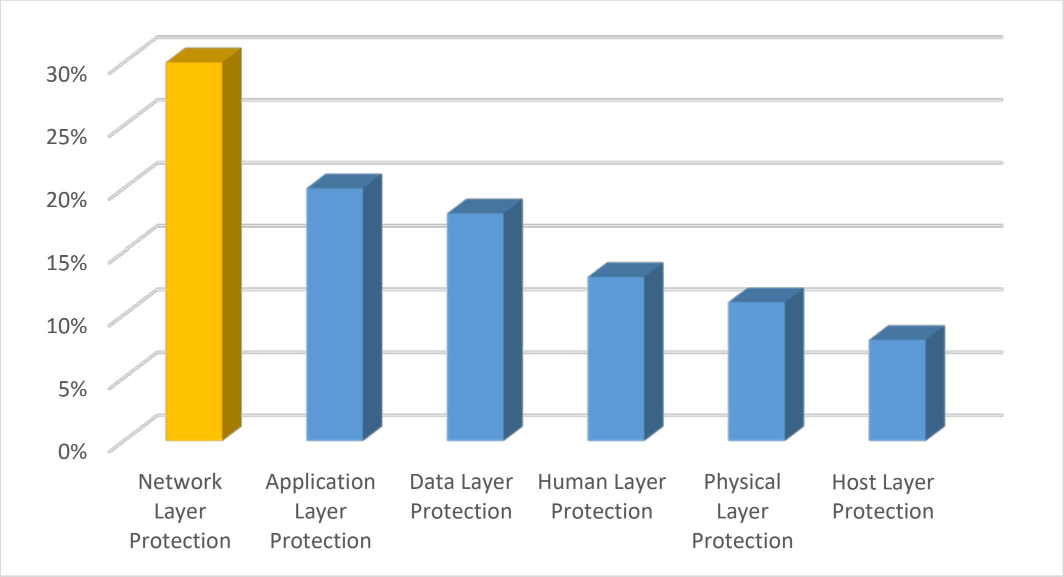


Figure 9: Percentage of spending by companies to protect their security in 2017

5.2 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.

5.3 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 10 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.

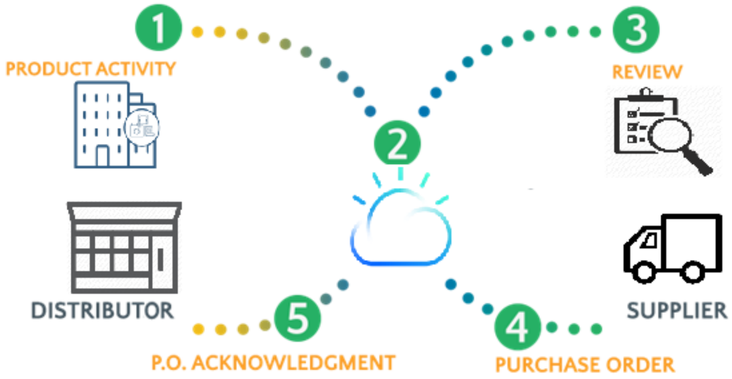


Figure 10: Cloud based vendor-managed inventory

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.

5.4 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.

5.5 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 Ponemon 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

Companies are already investing in these technologies. A recent survey reveals that companies receive highest return on investment when they invest in security intelligence systems followed by advanced identity & access governance and automation, orchestration & machine learning. Following figure shows the average cost savings from deploying enabling technologies (US $ millions) by 254 companies in 2017 [9].

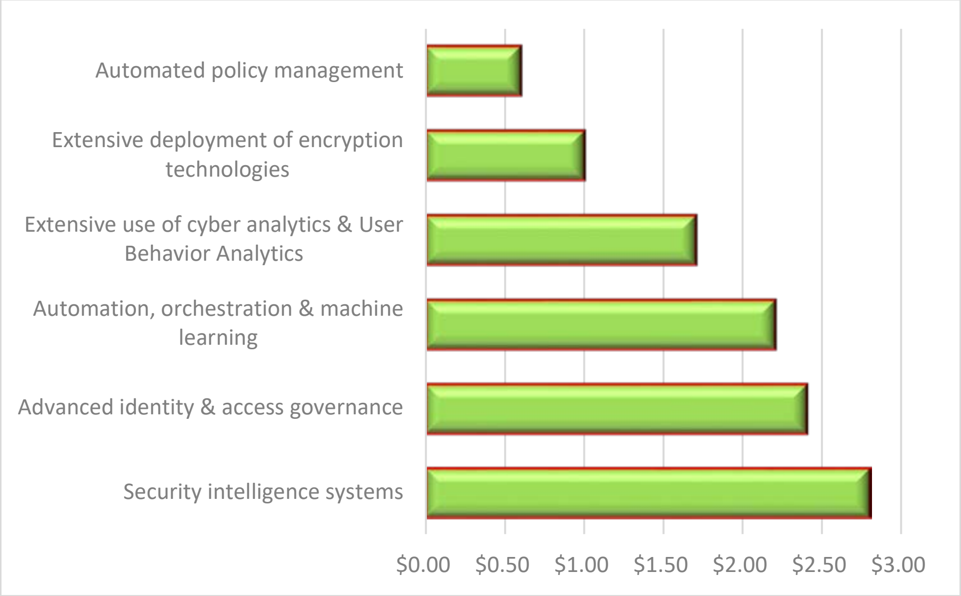


Figure 11: Cost savings from deploying enabling technologies (US $ millions)

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 [14]. Companies are targeting a range of use cases that the block chain helps enable from data management, to decentralized access control, to identity management.

6.0 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.

7.0 Acknowledgement

This research was funded by a grant from the Solutions Community and the College Industry Council on Material Handling Education (CICMHE).

References:

(1) Borghesi, P. (2018, January 30). Guarding Against Cyber Threats. Retrieved from https://www.mmh.com/article/guarding_against_cyber_threats

(2) Ezrati, M. (2018, September 06). Cybersecurity: A Major Concern and a Great Business Opportunity. Retrieved from https://www.forbes.com/sites/miltonezrati/2018/09/05/cyber-security-a-major-concern-and-a-great-business-opportunity/#49b5d09d3e26

(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. doi:10.1016/j.csi.2017.09.006

(4) Windelberg, M. (2016). Objectives for managing cyber supply chain risk. International Journal of Critical Infrastructure Protection, 12, 4-11. doi:10.1016/j.ijcip.2015.11.003

(5) Yağdereli, E., Gemci, C., & Aktaş, A. Z. (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. doi:10.1177/1548512915575803

(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. doi:10.1177/1541931213601540

(7) Cybersecurity in the Age of Smart Manufacturing. (n.d.). Retrieved from https://deloitte.wsj.com/cio/2018/02/27/cybersecurity-in-the-age-of-smart-manufacturing/

(8) Industrial systems: What are the potential impacts of cyberattacks? (2017, November 09). Retrieved from https://www.sentryo.net/industrial-systems-potential-impacts-cyberattacks/

(9) Cost of Cyber Crime Study. (2017). Retrieved from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

(10) MHI Industry Groups. http://www.mhi.org/industrygroups

(11) Lin, M. (2018, December 2018). Cybersecurity: What Every CEO and CFO Should Know. Retrieved from https://www.toptal.com/finance/finance-directors/cyber-security

(12) Soltes, F. (2018). Truck Takeovers? Retrieved from https://www.mhisolutionsmag.com/index.php/2018/09/13/truck-takeovers/

(13) Marr, B. (2017). The Future of the Transport Industry - IoT, Big Data, AI and Autonomous Vehicles. Retrieved from https://www.forbes.com/sites/bernardmarr/2017/11/06/the-future-of-the-transport-industry-iot-big-data-ai-and-autonomous-vehicles/#530f77831137

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