Material Handling & Logistics
CONFERENCE
SPONSORED BY DEMATIC

THE BIG CONNECT

UNITING PEOPLE, PROCESS & PURPOSE

Connect Selectively and Win the War Against Security Risk

Track 5: Session 6

James W. Haile, Jr., CPM

JWH & Associates

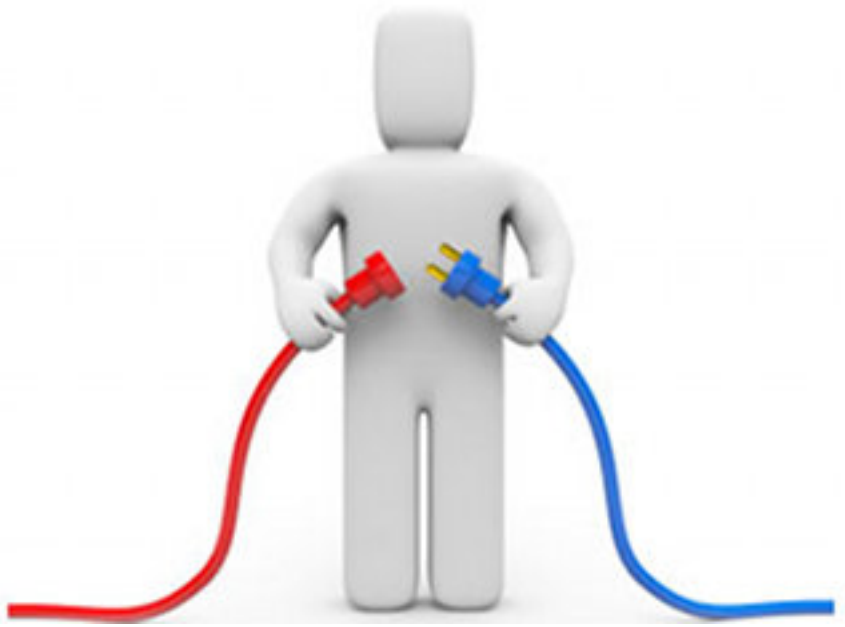
Founder

- Email: jwhaile@netzero.net
- Phone: 610-490-0470
- Linkedin: www.linkedin.com/in/james-w-haile-jr-c-p-m-97a3b52

Abstract

The Mobile Supply Chain, Internet of Things, and Big Data are fine, until somebody gets in the door and cleans out your fridge. This heads-up from the dark side comes from a one-step-ahead scientist who developed a revolutionary approach to identifying emerging classes of attacks on mobile devices, the power grid, and the Web… on which all of your Supply Chain systems depend. You will leave this discussion worried but energized to turn your vulnerabilities into actionable plans and reduce the business risk you didn't know you had.

Be Aware and Stay Alert!
Manage Your Connections!



Agenda

- Purpose
- Supply Chain
- Terms and Definitions
- Cyber Risks and Dollar Impact
- Cyber Threats and Attacks
- Manage and Protect
- Key Takeaways
- Conference Cloud
- Questions

Purpose

To generate continuous awareness and managed activities, using specific regulatory guidelines, appropriate employee behavior, business processes and solutions, to prevent and minimize Black Hat Hackers, who implement cyber threats and cyber attacks from adversely impacting our supply chains.

What is the Supply Chain?

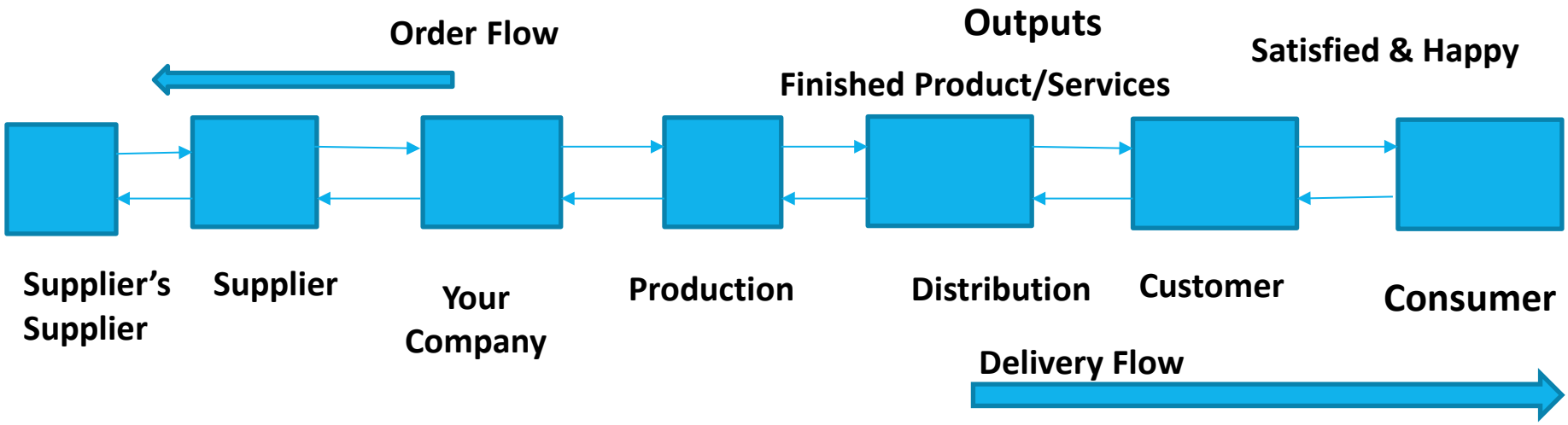
- **The Supply Chain is a process where the sum total of resources (i.e. material, equipment, labor and capital dollars) are transformed into a product or service which is sold to a customer and then resold to the final consumer.**

- **They have major inputs and outputs that affect specific businesses, industries and their employees.**

- **Supply Chains shape the economic opportunity of businesses**

The Supply Chain

Inputs: raw materials, equipment, people and capital

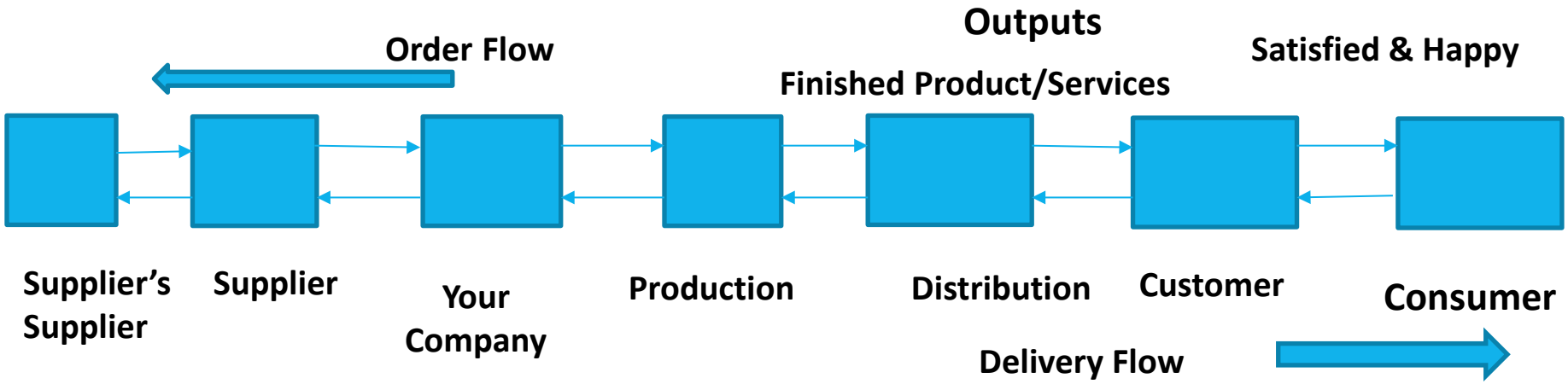


The Internet of Things (IoT): Embedded Technology/Internet connections

Cars Production Equipment Smart TVs Toys
Refrigerators Thermostats Drones Lighting
Security Systems Industrial Controllers Driverless Agricultural Tractors
Medical Devices (e.g. wireless heart monitors or insulin dispensers)

The Supply Chain

Inputs: raw materials, equipment, people and capital



Potential Devices and Internet Connections to your Company's Supply Chain

-Employees BYOD's (e.g. smartphones, apps, tablets, laptops, etc.)
-Your mobile Employees (Travel expense system, P-cards, corporate credit card, etc.)
-Employees Working at Home
-Electronic management systems (e.g. billing, supply systems, databases, BOMs, scheduling systems, contract mgmt., etc.)
-Your Major Supplier, Your supplier's supplier and Your major Customers
-3-D Printing (Additive Manufacturing)
-Design/Collaborative Systems

Terms and Definitions

- **Hacker Hats:**
  - Black Hat Hackers violate computer security for personal gain (such as stealing credit card numbers or harvesting personal data for sale to identity thieves) or for pure maliciousness.
  - White Hats are “ethical hackers,” experts in compromising computer security systems who use their abilities for good, ethical, and legal purposes.
  - Gray Hats don’t work for their own personal gain or to cause carnage, but they may technically commit crimes and do arguably unethical things.
- **Nation-State: The government of countries who actively act as Black Hat Hackers who breach the cyber security of other governments and or key businesses to steal military secrets, conduct industrial espionage, disrupt operations or to terrorize.**

Terms and Definitions

- **Malware: malicious software is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.**

- **Darkode.com: This is a criminal marketplace where hackers can buy or sell malware or advertise for help to design malware**
- **Social Engineering: psychological manipulation of people into performing actions or divulging confidential information.**

Example: Drop memory sticks/thumb drives in the parking lot. Who will pick them up and plug them in their work or home PC?

- **Spear-phishing or Phishing: the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.**

Terms and Definitions

- **Internet of Things (IoT): the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to collect and exchange data (medical devices, manufacturing equipment, watches, automobiles, televisions, refrigerators, security systems, digital cameras, toys, etc.).**

- **Cloud: a shared pool of computing resources (networks, servers, storage, applications, and services).**

Terms and Definitions

- **Consent Decree:**
  - A settlement of a lawsuit or criminal case in which a person or company agrees to take specific actions without admitting fault or guilt for the situation that led to the lawsuit.
- **Ransomware:**
  - A type of malware that restricts access to a computer system that it infects in some way and demands that the user pay a ransom to the operators of the malware to remove the restriction.
- **BYOD (Bring Your Own Device):**
  - Personal devices such as smartphones, laptops, tablets, digital cameras and other devices that you may bring to work to use on your job.
- **CYOD (Choose Your Own Device):**
  - All of the above devices, but provided to the employees by their employers who have loaded the devices with company approved security software and protocols.

Cyber Risks and Dollar Impact

- **The International Maritime Bureau's (IMB), a Division of the International Chamber of Commerce, is calling the global supply chain "the next playground for hackers"!**
- **Events in 2014 showed that systems managing the movement of goods needed to be strengthened against the threat of cyber-attacks by criminals targeting carriers, ports, terminals and other transport operators.**
- **Criminal's were actually installing spyware within the operator's IT network by targeting individuals' personal devices where cybersecurity is less adequate.**

Cyber Risks and Dollar Impact

- **Hackers often make use of social networks to target truck drivers and operational personnel who travel extensively to ascertain routing and overnight parking patterns.**
- **The criminals were looking to extract information such as release codes for containers from terminal facilities or passwords to discover delivery instructions.**
- **In 2016, both the U.S. and Canada have recently issued advisories on “ransomware” attacks within the shipping industry.**

Cyber Risks and Dollar Impact

- **Many companies, including manufacturing, do not seem to be raising this topic to an urgent and critical level.**
- **The recent Manufacturing Leadership Council survey indicate:**
  - 62% believe that IT is responsible for Cyber Security
  - 37% provide Cyber Security training
  - 34% have a budget for Cyber Security
  - 35% have a formal plan and strategy
- **Cyber Security is not just IT's job!**
- **Cyber Security threats and attacks affect "Cost Containment" and "Insuring Continuity of Supply" of your business!**
- **It is a great portion of your "Business Continuity Planning" strategy!**

Cyber Risks and Dollar Impact

- **The average time between intrusion and detection is 205 days.**
- **The Ponemon Institute states that the average cost of a data breach in the US is $3.79 million for investigations, notifications and responding to the event which is an increase of 23 percent over the past two years.**
- **This above does not include the added costs for lost intellectual property, lost sales, reputations tarnished, inevitable lawsuits from angry customers, financial institutions and partners as well as any regulatory fines/punitive actions. These total costs can be upwards of billions of dollars.**

Cyber Risks and Dollar Impact

- **In the spring of 2014, SEC Commissioner Luis Aguilar publicly stated that Board members are responsible for the cyber security posture of their organizations. Corporate and personal liability penalties could be handed out by not implementing protective activities in areas when knowing about cyber weaknesses.**
- **A European car firm implemented a security patch that affected 2.4 million cars that kept hackers from automatically unlocking the car door.**
- **A television manufacturer uses voice recognition technology to enable voice command meaning it hears conversations and hackers can hear transmissions.**

Cyber Risks and Dollar Impact

- **In the past year, security patches were provided to consumers because hackers could remotely turn on the TVs' built-in cameras. While you're watching TV, a hacker could have been watching you.**
- **A toy doll can connect to the internet via Wi-Fi and has a microphone to record children and send that information off to third-parties for processing before responding with natural language responses.**
- **It was discovered that when connected to Wi-Fi the doll was vulnerable to hacking, allowing easy access to the doll’s system information, account information, stored audio files and direct access to the microphone.**

Cyber Risks and Dollar Impact

- **Forklifts embedded with technology today are equipped with wireless connectivity, data storage, and sensors that allow them to collect information from their own internal systems as well as from their environment and then transmit this data to management systems.**
- **They are mobile data centers.**
- **How secure are they?**

Cyber Attacks

Cyber Attacks

- **Stuxnet, a virus most likely created by a nation-state, was used to attack a manufacturing plant that was making nuclear weapons in an Iranian nuclear enrichment facility.**
- **The virus caused the control layer of the machine to destroy itself by operating outside of normal/safe parameters.**
- **Duqu is another nation-state intelligence weapon that looks for data which can be useful for attacking industrial control systems (ICS).**
- **The above cyber weapons are no longer weapons for nations, but they are now available for use by the domestic masses.**

Cyber Attacks

- **Hackers attacked an Ohio-based chemicals company through industrial control systems (ICS) to steal intellectual property causing substantial financial damage.**
- **In December 2014, it was reported in Germany that hackers had hit a steel mill by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down resulting in serious physical damage.**
- **In 2013, financial and business information was stolen from several robotics manufacturers and some shipping and logistics firms by malware hiding in inventory scanners manufactured by a Chinese company. The supply chain attack, dubbed "Zombie Zero," infiltrated the companies' ERP systems collecting data for over a year.**

Cyber Attacks

- e-cigarettes manufactured in China spread malicious software through the USB connection used to charge the device via an executive's computer used at work.

- A Carnegie Mellon University student pleaded guilty to creating and selling malware that allowed others to remotely control Android smartphones, including using the phone to spy on their owners.

- A Sheriff's office in Tennessee was held hostage to a hacker named "Nimrod Gruber". This person extorted $572 from the county by locking up sensitive data with "ransomware" known nationally as "CryptoWall." They paid the ransom by using Western Union and got their data freed.

Cyber Attacks

- **Two White Hat Hackers remotely took control of a vehicle while it was driving on a highway.**
- **A voluntary recall of nearly 1.4 million automobiles for a software update on their Uconnect system. The carmaker, along with entertainment system provider now faces a class-action lawsuit.**
- **Between 12/2013 and 1/2014, smart refrigerators infected with "thingbots," or robotic programs that can be remotely installed on digital devices, sent out malicious emails across the USA to individuals and enterprises just to be disruptive.**

Cyber Attacks

- **A company specializing in car breathalyzer technology, has become an extortion target, after a hacker uploaded what appears to be internal confidential documents (e.g. spreadsheets, manuals, product schematics) and source code onto an online hacking forum.**
- **Installation of adware known as “Superfish” in notebooks cannot be detected by end users because it is already embedded. This results in bad websites masquerading as major bank.**
- **A major healthcare provider was a victim of ransomware in April 2016**

Cyber Attacks

- **On Nov. 14, 2015, hackers accessed an Asian toy company's customer data**
- **The stolen information includes children's name, age, parent's name, home address, email addresses and from chat logs, personal information that only a trusted adult would know, such as a child's favorite toy and the names of their siblings.**
- **The educational toymaker suspended trading on the Hong Kong stock exchange after admitting a hack that contained the information of nearly five million people, including more than 200,000 children, had been committed.**

Cyber Attacks

- **CNBC TV in Houston reported that someone hacked into a couple's baby monitor so that the intruder not only could see into their sleeping 2-year-old daughter's room, but used profanity at her. This is not the first such incident involving wireless baby monitors across the USA.**

- **In 2014 the Dragonfly/Energetic Bear hack of U.S. and European energy companies began with a spear-phishing campaign against senior employees in energy sector companies. Those senior employees took the bait and enabled the hackers to compromise legitimate software used by industrial control system (ICS) manufacturers, inserting malware into software updates sent from the ICS manufacturers to their clients.**

Cyber Attacks

- **Jay Radcliffe, a medical device cybersecurity researcher at Rapid7, a data security analytics firm based in Boston, hacked his own insulin pump, revealing the potential life-threatening nature of poor security practices within the medical device arena.**
- **The Healthcare industry is saddled with old un-secured medical devices and is behind other industries in terms of the evolving cyber security landscape.**

Manage and Protect

Manage and Protect

- **The National Counterintelligence and Security Agency is planning to provide information including classified threat reports to companies about the risks of hacking and other crimes tied to the supplies and services they buy.**
- **They want to raise awareness that vulnerable supply chains give China, Russia and other governments -- as well as criminals, hackers and disgruntled employees -- the opportunity to steal sensitive information or disrupt operations.**

Manage and Protect

Office of the Director of National Intelligence

Know the Risk - Raise Your Shield: Supply Chain Risk Management

- https://www.youtube.com/watch?v=X0ySVjZu3-0

Manage and Protect

- **The Federal Trade Commission (FTC) on June 30, 2015 released its "Start with Security" initiative and guidance document aimed towards helping businesses protect their consumers' information in a world where sensitive data is often at risk. The initiative provides 10 steps developed from lessons learned from 54 FTC data security cases.**

- **Start with security.**
- **Control access to data sensibly.**
- **Require secure passwords and authentication.**

Manage and Protect

- Store sensitive personal information securely and protect it during transmission.
- Segment your network and monitor who's trying to get in and out.
- Secure remote access to your network.
- Apply sound security practices when developing new products.
- Make sure your service providers implement reasonable security measures.
- Put procedures in place to keep your security current and address vulnerabilities that may arise.
- Secure paper, physical media, and devices.

Manage and Protect

- **Use the Framework for Improving Critical Infrastructure Cybersecurity provided by the National Institute of Standards and Technology (NIST).**
- **The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities.**
- **https://www.nist.gov/cyberframework/**

Manage and Protect

- **Make sure that everybody adheres to the company's IT Security policies and is trained.**
- **Employee Behavior and Culture from top to bottom must be created and aligned to manage and protect the business!**
- **Educate and keep employees aware of any IT system intrusions or "Social Engineering" attempts re the supply chain. This is a year round function, not a once a year event.**
- **Insure that employees adhere to company policies re BYOD (Bring Your Own Devices) and if there is no policy create one.**

Manage and Protect

- **Train employees from clicking “links or attachments” that they are not suppose to click.**
- **Do Not plug any non-authorized company devices into your work computer’s USB port.**
- **Protect yourself with appropriate language re cyber security with critical contract manufacturers and critical equipment/services acquisitions.**
- **Buy Equipment from well known suppliers.**
- **Make sure IT security supports the vetting of internet related software, systems and devices that will be connected to the supply chain.**

Manage and Protect

- **Understand where your company's and your key supplier's "Cloud" is geographically located, how it is protected and what is the back-up plan. If located out of the country, what are the local laws for e-Discovery and for claiming ownership of your company's information?**
- **Implement an e- Discovery workshop for employees using in-house legal resources?**
- **When a breach occurs, insure that all supplier/customer contracts are immediately reviewed and appropriate communications are implemented.**
- **Share information between IT Security and Supply Chain twice a year to understand emerging information re IT security issues, national trends, what to do in terms of a breach, identify weaknesses re connections and discuss potential purchases to upgrade supply management systems.**

Manage and Protect

- **Process Map your Supply Chain to identify weakness and risk!**
- **Use outside firms to audit your systems and to run “breach simulations” to grow capability and experience for your employees.**
- **Supplier selection criteria should include strong IT evaluations of potential suppliers by including the internal IT security professionals and or third party IT security experts as part of your evaluation team.**
- **Visit your critical supplier’s site annually, communicate quarterly and include cyber security as a topic on the agenda.**

Manage and Protect

- **Use a “two-factor authentication” process for all third parties using remote network access to a company’s network.**
- **Supply Management professionals must take a more active role in corporate merger/acquisition activities during the due diligence process re supplier contracts, internal/external risk management evaluations and supply chain IT security weaknesses.**

Manage and Protect

- **Mitigating Risk through Cyber Insurance**
  - Costs of those cybercrimes can add up from things like direct financial loss, notification requirements, extra staff hours, legal fees, credit monitoring, fixing vulnerabilities, lost customers and brand damage.

Manage and Protect

- **There are four main types of cyber liability insurance coverage.**
  1. Data breach and privacy management coverage – covers costs associated with managing and recovering from data breaches, including investigation, data subject notification, credit monitoring, and associated legal fees.
  2. Multimedia liability coverage – covers defacement of websites, media, and intellectual property rights.
  3. Extortion liability coverage – covers damage incurred from extortion. This could be used in the case of DDoS or attacks that demand ransoms, for example.
  4. Network security liability – covers costs associated with denial-of-service attacks and third-party data theft.

Key Takeaways

- **Cyber Threats and Cyber Attacks will continue as technology advances and is integrated more and more in the Supply Chain and the total business.**
- **Cyber Security is the fastest growing occupation in the US today and will continue to grow by 36.5% (27,200 jobs) by 2022 as predicted by the US Labor Department.**
- **Create a relationship with the National Counterintelligence and Security Agency to obtain the classified cybersecurity threat reports**
- **Understand and Adhere to the Federal Trade Commission (FTC) “Start with Security” initiative**

Key Takeaways

- **Use the National Institute of Standards and Technology (NIST) Cybersecurity supply chain audit tool.**
- **Create and Manage a robust “Cyber Security Program” with a budget that is driven by Senior Leadership.**
- **Build a company “Cyber Security Team” consisting of Supply Management, IT Security, Legal and Human Resources with Senior Leadership oversight to manage the program.**
- **Keep senior management informed re risks, threats and attacks that are cyber related to the supply chain in order to gain their support and to elevate priority.**

Key Takeaways

- **Understand your risks and weaknesses in your Supply Chain by Process Mapping, Audits and Breach Simulations periodically.**
- **Train and Inform all Employees year round and treat it as a “Marketing Campaign”!**
- **Supplier selection and total supplier management will be more important Now and into the Future.**
- **BE AWARE and STAY ALERT!**
- **Manage Your Connections Wisely!**

Conference Cloud

Additional Resources

- **Federal Trade Commission (FTC): "Start with Security" initiative**
  https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

- **Five ways to avoid or defeat a ransomware infection**
  https://www.carbonite.com/en/cloud-backup/business/resources/carbonite-blog/five-ways-to-avoid-or-defeat-a-ransonware-infection/?utm_campaign=10392&utm_source=linkedin&utm_medium=paid-social&utm_content=2595&catid=214877&c3placement=2595&c3ch=Likedin&c3nid=Five_Ways_to_Avoid_or_Defeat_a_Ransomware_Infection

Material Handling & Logistics
CONFERENCE
SPONSORED BY DEMATIC

THE BIG CONNECT

UNITING PEOPLE, PROCESS & PURPOSE

Questions?