Critical Manufacturing Sector Landscape

Publication: August 2019
Cybersecurity and Infrastructure Security Agency

Contents

Executive Summary

The Critical Manufacturing Sector comprises processes and products that are crucial to the economic prosperity and continuity of the United States. Among myriad roles and responsibilities, manufacturers in the sector process raw materials and primary metals; produce engines, turbines, and power transmission equipment; produce electrical equipment and components; and manufacture cars, trucks, commercial ships, aircraft, rail cars, and their supporting components. Products made by these industries are essential to many other critical infrastructure sectors; a failure or disruption in the Critical Manufacturing Sector could result in cascading disruptions to other sectors in multiple regions.

A number of factors may affect the critical infrastructure security and resilience posture of the Critical Manufacturing Sector. These factors, which influence the current operating environment and associated decision-making processes, stem from environmental, technological, human, and physical causes. With facilities, suppliers, and end users located around the globe, Critical Manufacturing Sector operations are subject to a variety of disruptions that may start at a local or regional level but have the potential to cascade across geographic regions and multiple industries.

The following are five major focus areas for Critical Manufacturing Sector security and resilience risk management planning consideration.

Supply Chain Security and Resilience: Dependence on both domestic and global supply chains to deliver raw goods, manufactured parts, and final components for assembly. Through highly interconnected supply chains of products and source materials, a major failure or disruption in the sector could significantly affect the national economy and cause lengthy disruptions that cascade across multiple infrastructure sectors or regions. For the Critical Manufacturing Sector, supply chain security and resilience issues include introduction of counterfeit parts and components, concentration or bottlenecking at coastal ports, globalization affecting the pricing and availability of products and raw materials, and the challenges of lean processes and just-in-time practices.

Natural Hazards: Adverse events caused by Earth's natural processes, such as floods, tropical cyclones, wildfires, tornadoes, earthquakes, and tsunamis. Natural hazards have the potential to cause substantial loss of life or property damage, as well as economic damage through disruption or destruction of facilities and operations. For the Critical Manufacturing Sector, the primary issues related to natural hazards are long-term physical damage to sector facilities, disruption of access to sector facilities, power and fuel losses, and disruption of the supply of raw materials and manufacturing inputs. Any natural hazard could have broad impacts on the sector because of disruptions in freight rail, highway, and maritime transportation that limit the availability of raw materials and the delivery of finished products.

Cybersecurity: Information technology attacks by sophisticated cyber threat actors and nation-states that exploit vulnerabilities to steal information and disrupt, destroy, or threaten the delivery of essential services. For the Critical Manufacturing Sector, major cybersecurity issues include impacts on operations due to targeted and opportunistic attacks (advanced persistent threats, distributed denial of service attacks, or malware and ransomware) or manipulation of industrial control systems. Vulnerabilities due to increased connectivity and disruptive digital technology and evolving tactics, techniques, and procedures can expand the potential attack surface. Cyberattacks have become a predominant method for stealing intellectual property, which is often considered a manufacturer's most valuable asset. The Critical Manufacturing Sector also relies on cyber assets to control and measure physical processes. Abuse of these control systems could potentially lead to physical damage, personnel hazards, and interrupted operations.

Criminal Activities and Terrorism: The unlawful use of violence and intimidation in the pursuit of personal or political aims. Criminal activities and terrorism can take many forms, including chemical, biological, nuclear, radiological, explosive, and vehicular attacks. These attacks can have catastrophic impacts on lives, facilities, and operations. For the Critical Manufacturing Sector, attacks such as active shooter incidents, insider threats, intellectual property theft, poisons and toxins, property damage, and suspicious activity have the potential for temporary disruptions in operations or the total loss of a facility.

Crosscutting Issues: Issues stemming from infrastructure, social, technology, and economic changes that have the potential to disrupt supply chains, increase capital expenditures, and lead to loss of sensitive security and operational information. For the Critical Manufacturing Sector, crosscutting security and resilience issues include operational dependencies on other sectors (e.g., large amounts of energy and water for manufacturing processes, communications and geospatial technology to coordinate the movement of inputs and products, financial services to conduct wide-ranging business transactions, and transportation capabilities to maintain manufacturing supply chains and deliver finished products). Other prominent issues include geopolitical issues affecting supply chains and availability of materials, workforce issues such as rebuilding long-term institutional knowledge and international skillset competition, and intrusion by unmanned aircraft systems.

This document provides a sector-specific characterization of relevant factors and decision-making drivers influencing the current operating environment and security and resilience posture of the Critical Manufacturing Sector. Government and industry partners may use this document to support identifying and addressing factors that could have adverse effects on the security or resilience of facilities, personnel, and operations. This document does not represent a compendium of vulnerabilities, nor is it a sector risk assessment. The different factors discussed in this document have been included because they influence the critical infrastructure security and resilience posture of the sector as a whole. Therefore, these factors are discussed from a sector-wide perspective and may not apply to all industry segments within the sector. As the security and resilience operating environment for the Critical Manufacturing Sector changes, this document may be updated.

Supply Chain Security and Resilience

The Critical Manufacturing Sector relies heavily on complex, effective global and domestic supply chains to deliver raw goods, manufactured parts, and final components. Important supply chain security and resilience issues for Critical Manufacturing Sector organizations include introduction of counterfeit parts and components, concentration or bottlenecking at coastal ports, globalization affecting the pricing and availability of products and raw materials, and the challenges of lean processes and just-in-time (JIT) practices.

Counterfeiting

Manufacturers are concerned about counterfeit parts or components entering the supply chain. Major disruptive events, such as natural disasters, increase the opportunity for counterfeit components to infiltrate the supply chain, as companies may have to adjust acquisition procedures to compensate for limited component availability or other supplier-based difficulties.

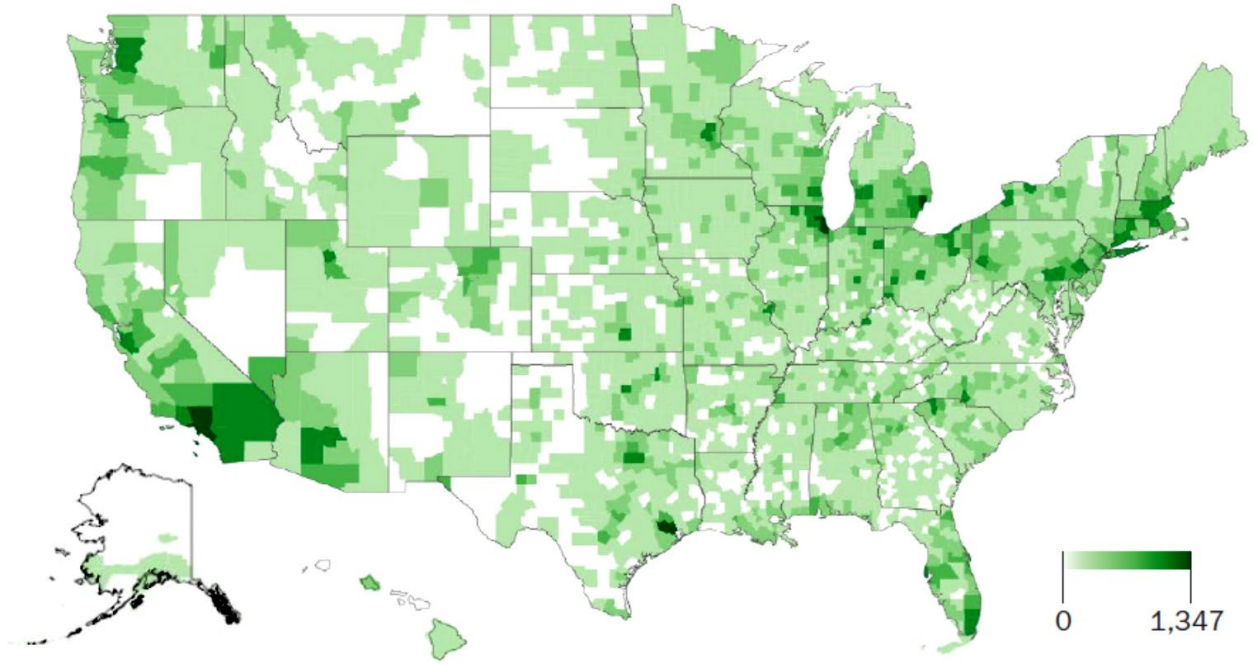
- **Diminished Product Quality and Safety:** Counterfeit components can significantly reduce the quality and safety of manufacturing products, potentially leading to accidents, lawsuits, or the loss of market share or competitiveness. In 2012, a Senate Armed Services Committee uncovered more than one million counterfeit parts in the Pentagon supply chain. The parts were found in multiple products, including missiles, aircraft, helicopters, and submarines. Although there was no impact on public safety, the same cannot be said of private-sector manufacturing.[1] Perhaps the most well-known example is the Norwegian charter aircraft that crashed off the coast of Denmark in 1989, resulting in 55 deaths. The cause of the crash was determined to be counterfeit parts that fastened the tail to the fuselage.[2]
- **Types of Counterfeit:** Identifying the type of counterfeiting threat can help to inform appropriate mitigations, such as adopting industry anti-counterfeit standards and best practices, developing a trusted supplier network, including audits in supplier contracts, and establishing documented policies and procedures for employees to follow when counterfeit is discovered. Several general types of counterfeit may be considered:
  - Adulterate: A component of the legitimate finished product is fraudulent.
  - Tamper: A legitimate product and package are used in a fraudulent way.
  - Over-run: A legitimate product is made in excess of production agreements.
  - Theft: A legitimate product is stolen and passed off as legitimately procured.
  - Diversion: A legitimate product is sold or distributed outside of intended markets.
  - Simulation: An illegitimate product is designed to look like, but not copy exactly, the legitimate product.
  - Complete counterfeit: All aspects of the fraudulent product and package are fully replicated.

Geographical Concentration

Concentration of Critical Manufacturing Sector assets, facilities, and suppliers around coastal ports could magnify geographic issues and the effects of local disasters and labor disruptions. Significant delays or closures at a single port can have widespread consequences, and labor disputes or bilateral policy issues can involve more than one site. Figure 1 provides a map of the distribution of Critical Manufacturing Sector facilities in the United States.[3]

- **Labor Disruptions to Supply Chains:** Labor strikes, poor equipment handling, or inadequate equipment can create a supply chain bottleneck with significant impacts. One large-scale example is the 2002 U.S. West Coast port lockout, which led to several manufacturers slowing or stopping production. Another example is the 2013 40-day labor strike at Hong Kong's Kwai Tsing container terminal, which resulted in significant shipping delays and cascading effects throughout the global supply chain.[4]
- **Local Disasters Affecting Supply Chains:** Disasters specific to one location or region can cause cascading impacts across the world, especially if major international ports are compromised. The August 2015 explosions in the port city of Tianjin, China, killed 173 people, caused extensive infrastructure damage, and disrupted automotive, machinery, and electronics supply chains for months.[5] The collective business losses due to this break in the supply chain were estimated at $9 billion.[6]

Figure 1. *Number of U.S. Critical Manufacturing Facilities by County*
Source: Critical Manufacturing Sector-Specific Plan



Globalization

International events could have significant and unpredictable impacts on domestic manufacturing, including pricing, availability, and delivery of products and raw source materials. The Crosscutting Issues chapter provides additional information related to geopolitical issues.

- **International Suppliers:** Rare earth elements are used in a range of modern technologies and national security applications. The United States imports 100% of these materials for manufacturing use, while China dominates the market. In 2010–2012, China significantly reduced its export quotas, leading to escalating costs and supply deficits. The prices plummeted in succeeding years but then leapt again in 2017, indicating potential for continued volatility in the market.[7] Such volatility could have an impact on Critical Manufacturing Sector products (especially large engines and power generators). Rare earth metal producers other than China, such as Australia, would likely be important during a rare earth metals shortage crisis, as would reinvigorated domestic production.

- **Effects of Government Policy on Supply Chains:** Policies and administrative procedures are interwoven with the supply chain in a complex manner. For example, the events of September 11, 2001, prompted restrictions on air travel and tighter security at U.S. customs checkpoints, thereby disrupting international shipments of parts and components. As a result, one major auto manufacturer had to shut down five of its U.S. plants. Policy can affect not only trade routes and customs clearance processes but also the ability to invest in facilities, international movement of businesspersons, information exchange, and technology access.[8]

Lean Processes, Just-in-Time Practices, and Inventory Management

The trade-off in time and cost efficiencies versus robust and resilient supply chains, coupled with narrow margins for error, can lead to unexpected supply chain disruptions. These inventory approaches, while seen as necessary for a competitive edge, increase the supply chain's importance while simultaneously heightening its susceptibility to outside forces.

- **Increased Dependence on the Supply Chain:** Japanese manufacturers proved JIT inventory methods to be a highly efficient, competitive approach—qualities progressively necessary in increasingly fast-paced markets. However, these same businesses showed the supply chain's fragility in the wake of the earthquake and tsunami disaster in Fukushima, Japan. The JIT approach makes companies inflexibly reliant on suppliers that provide inventory when needed—not earlier, not later. Deviations in highly synchronized JIT supply chains can present manufacturing challenges. For example, unexpected increases in orders can cause backups or rushes in production, compromising smooth workflows, quality assurance, and safety.
- **Global Supply Chains and Uncertainty:** The global supply chain is a recent and evolving phenomenon, making it challenging for industry to control. The supply chain involves many disparate parts that are difficult to predict and monitor, and a disruption to any one of them causes a disruption to the chain as a whole. At the same time, current supply chains are subject to greater hazards: weather events are increasing in both severity and frequency, events such as terrorist attacks across the world show the rising likelihood of manmade effects on supply chains, and emerging virtual technologies are under threat from cyberattack.

Supply Chain Cybersecurity

Critical Manufacturing Sector assets and networks are susceptible to compromised vendor communications associated with the supply chain. Email phishing attempts from presumed trusted vendor email accounts are becoming more frequent. Successful phishing attempts could allow attackers remote access to enterprise networks and the opportunity to escalate attacks to operations infrastructure. Trusted contractors and vendors may have legitimate remote access to provide services; however, this access could become a vulnerability if the contractor or vendor is compromised. The supply chain for software itself represents another cybersecurity concern, as compromised software introduced along the supply chain could be used to attack Critical Manufacturing Sector networks. Cyber threats to the supply chain can also affect physical security.

- **Software Supply Chain:** In 2017, software supply chain attacks increased dramatically across all sectors.[9] By attacking software providers, attackers can replace legitimate business software with maliciously modified versions, unbeknownst to end users. For example, Critical Manufacturing Sector entities may try to install the latest version of previously trusted software, unwittingly downloading a malicious version instead.
- **Cyber and Physical Security Convergence:** Supply chain impacts to cybersecurity can also affect physical security. The converse is also true: physical security supply chain impacts can affect cybersecurity. For example, compromised software used in an industrial control system (ICS) could

cause ICS network vulnerability or instability and lead to failure of physical operations of the ICS. Counterfeit hardware introduced into physical control systems—such as electronic door locks or security cameras—could render a facility vulnerable to specific cyberattacks.

- **Third-Party Attacks:** Attackers have targeted critical infrastructure subcontractors' networks to abuse access the subcontractor might have to the target organization. This abuse of trust in software suppliers and subcontractors can affect even well-protected organizations.

Transportation Industry Trends

The transportation industry continues to adapt to an evolving global supply chain. As changing transportation market pressures encourage global and domestic transportation companies to consolidate and/or lead to their failure, Critical Manufacturing Sector operations may be disrupted. Major recent examples of transportation industry changes include consolidations of large trucking companies from 2015–2017 and the largest-ever bankruptcy of a shipping company in 2016. Transportation consolidations and bankruptcy absorptions disrupt JIT supply chains as companies restructure and evolve.

- **Trucking Consolidations:** Mergers and consolidation in the trucking industry have been occurring in North America and Europe at a rapid rate in the recent past. Many billion-dollar mergers occurred from 2015–2017. Numerous smaller mergers and consolidations also took place, with hundreds of smaller companies being purchased by larger ones.[10] Such large-scale consolidation can decrease competition and lead to many smaller companies failing. This volatility can cause unforeseen disruptions in the Critical Manufacturing Sector, such as the sudden loss of trucking contracts, increased trucking costs, or a decrease in available trucking options when supply chains change.
- **Major Shipping Bankruptcy:** In 2016, a South Korean company became the largest container shipping company in history to file for bankruptcy. At the time of its bankruptcy, it accounted for approximately 4 percent of global maritime container shipping volume, including 5 percent of U.S. container imports. The sudden cessation of its operations caused substantial delays in container shipping times, significant increases in shipping costs, and a shortage of trailer chassis around the major ports of Los Angeles and Long Beach.[11] Such major changes in container shipping can affect the supply and value chains of the Critical Manufacturing Sector by slowing production, increasing operating costs, and reducing product value.

Case Study: Supply Chain Information Sharing

Several major international aerospace and defense manufacturers established a joint venture in 2000 to continuously monitor, measure, and mitigate security risks throughout multi-tier supply chains. What began as a supply chain portal to bring buyers and sellers together in the aerospace industry has evolved into a cloud-based, online platform to ensure secure connections across the global aerospace and defense supply chain ecosystem.

The original portal was slated for upgrading and enhancement in 2007 when the aerospace companies convened to discuss an emerging concern at the U.S. Department of Defense (DoD)—leaks of critical company and product data through the supply chain. Such leaks of sensitive information are significant threats to both industry and government. On the industry side, the loss of intellectual property affected both jobs and the companies' bottom lines. On the DoD side, that loss of proprietary information had the potential to affect the Nation's military posture.

In response to the threat, the aerospace and defense companies collaborated to jointly develop and deploy a number of tools to manage information-sharing processes more securely and to protect information throughout the supply chain ecosystem. One set of tools was designed to secure supplier portals by strengthening access controls and identity management systems. The resultant identity and access management platform allows more than 100,000 organizations to share information securely and seamlessly across partner networks, thus creating a "do it once—share to many" model.

A second tool was developed by an industry working group over an 18-month period to ensure that suppliers were capable of protecting critical information assets and network connections. The tool establishes common cyber security definitions and standards for aerospace industry suppliers—setting minimum thresholds of compliance for every supplier. The value of the tool extends beyond the buy side to the supply side. Partners working with multiple organizations need only complete a questionnaire once, thus easing the administrative burden, eliminating redundancy and inconsistency, and delivering the information that leads to improvements in their overall vulnerability.

Natural Hazards

Natural hazards are major adverse events caused by Earth's natural processes and include floods, tropical cyclones, wildfires, tornadoes, earthquakes, and tsunamis. Natural hazards can cause disasters that result in loss of life or property damage as well as economic damage through disrupting or destroying facilities and operations. The severity of a natural disaster is measured in terms of lives lost, economic disruption, and the affected population's ability to rebuild.

Major security and resilience issues for the Critical Manufacturing Sector regarding natural hazards include earthquakes in the Western and Central United States, flooding along the Gulf Coast and in the Central United States, hurricanes along the Atlantic Coast and Gulf Coast, and tornadoes in the Midwest and South. Disruptions caused by natural hazards in surface, rail, barge, and pipeline transportation are also of great concern. Recognizing and addressing these concerns could help to mitigate the financial, operational, and human impacts of natural hazards.

Costly Impacts of Natural Hazards

Recent billion-dollar-loss natural disaster events in the United States include Atlantic and Gulf Coast hurricanes, northeastern winter storms, flooding along the Gulf Coast and in central and western states, freezing in southeastern states, tornadoes and hail storms in central states, and fires and drought in western states. In 2017, the United States experienced 16 separate billion-dollar disasters, with total damage costs exceeding $300 billion. The total number of these disasters ties the annual record from 2011, and the total damage cost is a new annual record. Figure 2 provides a map of these events.[12] Such large-scale events have cascading impacts across sectors and regions, with the potential to cause significant disruptions to Critical Manufacturing Sector facilities and companies (e.g., long-term physical damage, disruption of access, and power, fuel, and raw material loss).

Figure 2. *2017 U.S. Billion-Dollar-Loss Natural Disaster Events*
Source: National Oceanic and Atmospheric Administration (NOAA)

- **Long-Term Physical Damage:** Physical damage to Critical Manufacturing Sector facilities from such large natural hazards can be catastrophic, with recovery times extending for months or years. Such long-term disruption of manufacturing operations could cause negative operational and economic impacts along supply chains to other manufacturers or sectors.
- **Disruption of Access:** Major natural hazards often damage roads or bridges leading to Critical Manufacturing Sector facilities affected by the event, cutting off or drastically restricting access. This hinders response and recovery efforts, limiting the ability of owners, operators, and response personnel to assess conditions and begin mitigation activities. Secondary disasters such as explosions or environmental contamination (depending on the facility) could also occur if limited access is prolonged.
- **Power and Fuel Loss:** Power outages and the disruption of the fuel supply chain (for backup power) are expected during large-scale natural hazard events. Dependence on the Energy Sector to supply power and fuel and respond to their disruption renders the Critical Manufacturing Sector susceptible to cascading failures (i.e., if a facility is otherwise unimpaired by a natural disaster, it is still vulnerable to Energy Sector disruptions). For example, Hurricane Harvey caused weekly refinery inputs in the Gulf Coast region to drop 34 percent from the previous week. Major pipelines were without fuel to transport, and the lower Atlantic region in particular drew upon inventories of motor gasoline to make up for shortfalls, which caused a spike in fuel prices.[13]
- **Raw Material Loss:** Natural disasters can limit access and disrupt transportation to Critical Manufacturing Sector facilities, which can result in the loss of raw materials needed for manufacturing. The flow of raw materials may halt as a direct result of a disaster, or the event may reduce personnel or affect systems that manage material input. Either way, raw material loss can cause significant disruptions, resulting in economic losses and hindering the flow of products to and from manufacturing facilities.

Earthquakes

Major earthquakes are a significant threat to the Critical Manufacturing Sector. A strong earthquake in the Cascadia seismic zone in the Pacific Northwest, the San Andreas Fault in California, or the New Madrid seismic zone in the Central United States could cause significant manufacturing industry disruptions.

- **Cascadia Seismic Zone:** A major earthquake in the Cascadia seismic zone would severely disrupt critical infrastructure in the Pacific Northwest, including major manufacturers in Oregon, Washington, and British Columbia. Manufacturing in the region greatly depends on the transportation of products to market and access to raw materials for production. Such an event could cause transportation system devastation (including major port and barge disruptions from an earthquake-triggered tsunami) and lead to several hundred billion dollars in losses for the region.[14]
- **San Andreas Fault:** A major earthquake along the San Andreas Fault in southern California would have drastic impacts on critical infrastructure in the region, including over $200 billion in damage with long-lasting economic impacts. Not only would Critical Manufacturing Sector facilities in the region experience major disruptions directly, the impacts to transportation systems (especially for the critical port of Long Beach) would cripple critical infrastructure supply chains for weeks. Water and power infrastructure could be similarly disrupted in the region.[15]
- **New Madrid Seismic Zone:** A major earthquake in the New Madrid seismic zone (similar to the earthquake that occurred in the region in 1895) would have devastating impacts on the Central United States, including eight states (Alabama, Arkansas, Illinois, Indiana, Kentucky, Mississippi, Missouri, and Tennessee) and the metropolitan areas of Memphis and St. Louis. The area includes more than 40 million citizens and major critical infrastructure facilities of the Chemical, Communications, Critical Manufacturing, Energy, and Transportation Systems Sectors along the

Mississippi River. Total estimated economic loss for such an event could reach several hundred billion dollars.[16]

Flooding

Increased likelihood of flooding along the Gulf Coast and in the North Central and Western United States increases risk to manufacturing facilities in those regions. Past major events have threatened Critical Manufacturing Sector operations at locations along the Gulf Coast and major rivers of the Central and Western United States (e.g., Hurricane Harvey and flooding in California and of the Mississippi River in 2017). Flooding in international manufacturing regions or trade routes can also affect manufacturing operations and suppliers in the United States. The primary concern with a flood event's disruption of manufacturing facilities is the interruption of the inbound and outbound supply chain of products and materials. Facilities that depend upon barge deliveries as their primary resupply mechanism will likely suffer a greater impact than facilities that rely on roads and rail for the transportation of materials. Flooding could also potentially damage production facilities and storage mechanisms.

- **Electrical Damage:** Flooding of electrical equipment can lead to short-circuiting and power blackouts, which could result in the failure of manufacturing processes and safety systems.
- **Flood Path Debris:** The impact of floating debris dragged along with floodwaters poses a threat to facilities or equipment and can lead to the release of hazardous substances or trigger explosions.
- **Hazmat:** Flood impact can release hazardous materials that react with the floodwaters to generate toxic or flammable mixtures, which pose a secondary threat.
- **Cascading Impacts:** Floods usually affect a wide swath of land and can carry released substances over significant distances. Therefore, the risk of cascading effects in a densely industrialized area is elevated.

Tornadoes

The potential for tornado disasters in the Central United States, the Midwest, and the South increases the risk to manufacturing facilities in these regions. Storms that produce tornadoes can also produce damaging hail and potentially disrupt Critical Manufacturing Sector operations and suppliers in the United States, Canada, and Mexico.

- **Manufacturing and Tornado Alley:** The areas of the United States in which tornadoes frequently occur are collectively referred to as Tornado Alley. These areas include several states in the Central United States, the Midwest, and the South. Manufacturing hubs in these states have increased susceptibility to damages, losses, and cascading impacts from tornadoes. Past prominent examples of tornado impact in the sector include the February 2008 damage to a key parts factory for a major heavy equipment manufacturer in Oxford, Mississippi; the April 2012 damage to multiple aircraft and aerospace manufacturing facilities in Wichita, Kansas; and the February 2017 damage to a NASA manufacturing facility in New Orleans, Louisiana.
- **Hail Storms:** Storms with the potential to generate tornadoes also have the potential to produce hail that can significantly damage property. Hail is an important concern for automotive and aerospace manufacturers that may have open areas of finished products exposed to such storms. Some major automotive manufacturing facilities in the U.S. South and in Mexico have incorporated hail mitigating strategies (e.g., hail nets in vehicle yards) to prevent hail damage.

Transportation Disruptions

Any natural hazard can lead to significant Critical Manufacturing Sector impacts from disruptions in transportation systems. Critical Manufacturing Sector operations and facilities rely on the secure flow of raw materials and finished products across transportation modes. Natural hazards that compromise the freight rail, highway, and maritime modes can have significant impacts on Critical Manufacturing Sector operations as well as cascading impacts on other interdependent sectors.

- **Freight Rail:** Trains ship manufacturing products in shipping containers, usually on a path to exportation. During normal conditions, railways often become clogged in metropolitan areas. If a natural hazard affects rail service, these delays can become debilitating to Critical Manufacturing Sector companies relying on bulk transportation, as delivery times cannot be guaranteed or readily estimated.
- **Highway:** A significant number of domestic Critical Manufacturing Sector shipments are conveyed with trucks on highways and roads. When natural hazards affect surface transportation in areas essential to Critical Manufacturing Sector supply chains, major delays and losses can occur.
- **Maritime:** International shipping across oceans is vital to Critical Manufacturing Sector operations. By necessity of their locations, major international ports are subject to coastal natural hazards, such as tropical cyclones and flooding. In addition, flooding and drought from natural hazards can severely hinder waterway transportation inland from ports and contribute to Critical Manufacturing Sector losses.

Tropical Cyclones

Tropical cyclones are large, powerful, low-pressure storm systems that typically form over large bodies of warm water. Tropical cyclones include tropical storms, hurricanes, and typhoons. The Atlantic hurricane season has been disastrous for the United States in the recent past. As shown in Figure 2, three large hurricanes impacted the United States in 2017, each resulting in more than one billion dollars in losses. Other historical hurricane events such as Hurricanes Katrina, Rita, Ike, Sandy, and Matthew have also shown how devastating these events can be for all sectors, and the Critical Manufacturing Sector may be more prone to damages in the regions along the East and Gulf Coasts where tropical cyclones tend to strike.

- **Tropical Cyclone Preparedness:** Critical Manufacturing Sector emergency plans for tropical cyclones involve many actions taken in advance of storms. Depending on the severity of the storm, these actions may include complete shutdown of facilities following strict safety and operating procedures, evacuating personnel, preparing backup power generators, physically securing equipment, and removing unnecessary vehicles and other equipment.
- **Tropical Cyclone Impacts:** As major storms such as Harvey, Irma, Katrina, and Rita have demonstrated, the impact of tropical cyclones can extend well beyond the potential threat to employees and physical damage to facilities and their communities. While most Critical Manufacturing Sector facilities did not suffer major structural damage and were operational within days following the disasters, many were unable to resume normal production because of external consequences of the storms. Extensive damage to local infrastructure blocked the flow of key supplies, such as electricity, natural gas, and raw materials, while damaged roads and rail lines prevented the delivery of products to customers.

Case Study: Fukushima Earthquake and the Global Supply Chain

In 2011, Japan experienced the most powerful earthquake in the country's recorded history. The 9.0-magnitude quake triggered a powerful tsunami with 100-foot waves that traveled up to 6 miles inland. The losses, in terms of human casualties and displacement, were staggering. The event had a significant economic impact as well, attributable in part to disruptions to the global supply chain.

Fukushima is home to a number of manufacturing facilities integral to the automotive industry, from vehicle assembly plants to component manufacturers to electronics producers. Many of these facilities closed, leading to shortages that had widespread affects across all countries linked to the production networks.

In the days and weeks immediately following the quake, major international automakers took several strategic actions to minimize the disruption. Executives sought ways to re-engineer the supply chain in the short term, such as issuing temporary contracts to operational vendors and working with competitors to help suppliers get back into production.

Manufacturing organizations in Japan worked toward making supply chains more resilient following the disaster. Many had adopted JIT production systems to increase efficiency, yet this approach provides little cushion for emergencies. After the tsunami, businesses had to balance the benefits of JIT against the potential losses. Some decided to keep more inventory, although many concluded that carrying excessive stock would be detrimental to a company's bottom line. Instead, some companies standardized parts and created alternative production capabilities for use during emergencies. A major international automotive manufacturer built redundancy into its supply chain, identifying one key producer and two backup vendors whose production can be ramped up if needed. The company also implemented a new database that stores information for over 650,000 supplier sites, allowing quick identification of options if a supplier goes offline.

Cybersecurity

The Critical Manufacturing Sector is subject to a wide range of risks stemming from cyber threats and hazards. Sophisticated cyber threat actors and nation-states exploit vulnerabilities to steal information and disrupt, destroy, or threaten the delivery of essential services. As information technology (IT) becomes increasingly integrated with physical infrastructure operations, risk of wide-scale or high-consequence events increases.

Issues of higher cybersecurity risk for the Critical Manufacturing Sector include advanced persistent threat (APT) attacks, distributed denial of service (DDoS) attacks, vulnerable ICSs, increased connectivity and complexity of communications technology, the Internet of Things (IoT), malware, and ransomware. Recognizing and mitigating these issues could help to limit cyber intrusions.

Advanced Persistent Threat

APTs are typically nation-state or nation-state-sponsored cybersecurity threats. Coordinated, long-term cyber campaigns by motivated cyber threat actors pose significant risk to the Critical Manufacturing Sector. Opportunities for long-term cyberattacks will likely always exist in both cyber assets and the personnel who use them, and APTs can exploit these opportunities, given enough time and resources. APTs may be able to establish a foothold in a manufacturer's network and move laterally or probe deeper into internal networks undetected to attack ICSs. Developing attacks on ICSs takes time, knowledge, and expertise in the unique operating environments of the target manufacturer. APTs therefore take advantage of vulnerabilities at multiple stages to gather information and develop and validate their attacks.

VPNFilter, Dragonfly, and Hatman are three recent notable examples of malware whose sophistication indicates that it originated with an APT group, and all three targeted or had the ability to target critical infrastructure. These types of intrusions can lead to cyber threat actors taking full control of network infrastructure, allowing for further attacks on connected infrastructure (e.g., data theft, espionage, denial of service, or decreased productivity/functionality). Cyber threat actors with persistent access to network devices can move laterally and reattack after they have been ejected from previously exploited hosts.

- **VPNFilter:** In May 2018, Cicso's Talos Intelligence Group announced its research into a modular malware system named VPNFilter, which had infected more than 500,000 devices. The malware uses vulnerabilities in a range of network devices—primarily internet routers—to install a persistent foothold in the targeted devices, which can be used to deploy further modular malware on the device. Parts of the code used in this platform overlap with the BlackEnergy malware used to target Ukrainian electric utilities in 2015, and modules exist that extend the malware's capabilities to monitor for Modbus network traffic, a common protocol used in ICSs.[17]
- **Dragonfly:** Russian government cyber threat actors have been targeting U.S. critical infrastructure sectors since at least March 2016 in a coordinated campaign of malware attacks collectively named Dragonfly. The threat actors used a combination of spear-phishing (highly targeted emails with malicious attachments) and watering hole attacks (introducing malware through well-known industry trade publications' websites) to collect user credentials. The threat actors were able to establish footholds in the target networks and conduct network reconnaissance, move laterally, and collect information pertaining to ICSs.
- **Hatman (also known as TRITON and TRISIS):** This attack platform targets safety controllers manufactured by a major international ICS provider. Safety controllers play an essential role in ICS environments to ensure the safe and predictable shutdown of operational equipment. Hatman malware was specifically designed to allow changes to the safety controller to introduce new

functionality that would likely degrade the safety controller's ability to shut down unsafe equipment safely.

Distributed Denial of Service Attacks

DDoS attacks are a growing threat. They use many Internet-connected devices to generate immense bandwidth loads to the point of disruption or creation of openings for malware to be deployed. As the Critical Manufacturing Sector introduces more Internet-connected devices into its processes (see Internet of Things below), the risk DDoS attacks also increases. Common security devices that use high-bandwidth connections, such as security cameras and digital video recorders in Critical Manufacturing Sector facilities, are of particular concern in terms of DDoS attacks because they can suddenly consume large volumes of Internet traffic and are commonly deployed in large batches.

- **Botnets:** Botnets are collections of Internet-connected devices that have been infected with malware to respond to specific requests from a command and control entity. Potential devices range from home computers to IoT devices. Botnets can be used to generate massive amounts of Internet traffic to a specific target with the intention of disrupting essential services. A recent high-profile example was the Mirai botnet, which was used in October 2016 in a DDoS attack on a major domain name system (DNS) service provider. The attack flooded 1.2 terabits per second (Tbps) of Internet traffic (at the time, the highest volume of DDoS traffic ever recorded) managed by the DNS provider and shut down many well-known websites. At the height of the attack, millions of users were denied Internet services in North America and Europe. Similar to a previous September 2016 Mirai attack, the DNS attack employed millions of compromised Internet-connected security cameras to conduct the attack simultaneously.[18]
- **Amplification:** Amplification refers to a technique in which a cyber threat actor abuses Internet-connected devices such that they respond to a small amount of data sent from the threat actor by sending large packets of data to a target as part of a DDoS attack. The effect amplifies the bandwidth sent by the threat actor, resulting in much larger amounts of data flooding the target. Unlike with botnets, the threat actor does not necessarily need control of the device. Instead, the threat actor abuses the devices' intended functionality to respond to requests and causes the responses to flood a target's servers. Memcached DDoS attacks, a specific type of amplification attack, resulted in 1.3 Tbps and 1.7 Tbps of Internet traffic in separate attacks in March 2018, though no critical services were disrupted.[19]

Increased Connectivity and Disruptive Digital Technology

Critical Manufacturing Sector organizations are integrating IT and automation to streamline operations and promote growth in the manufacturing industry. This convergence of operational technology (OT) and IT can lead to increased points of access through which malicious code could be introduced or data could be stolen, a broadening landscape of cyber threats from cloud services, and cascading failures between devices due to interconnectivity.

- **Increased Points of Access:** An expanding footprint of networked devices introduces more points of potential targets for cyberattack in the network. This includes both physical (e.g., locations for input or display devices) and cyber (e.g., network ports) points of access that could be exploited.
- **Cloud Services:** Critical Manufacturing Sector organizations are increasingly incorporating cloud services into their business operations. Cloud software-as-a-service (SaaS) is leveraged to enhance business functions in the areas of IT, human resources, marketing, and supply chain. Although cloud services offer benefits, such as scalability, high availability, advanced data analysis and storage, and decreased ownership cost, new cybersecurity concerns are associated with those benefits. Cloud services and physical IT share many of the same cybersecurity issues (e.g., denial of service, APT,

stolen credentials, and phishing) yet are also susceptible to novel attacks, including malicious control of virtual machines and attacks on systems running virtual processes.

- **Cascading Failures:** Automated systems that are dependent on interconnected devices may be subject to cascading failures that result from disruptions along the network of devices. Similarly, production process flow disruption or alteration (whether intentional or accidental) within a chain of interconnected devices can have drastic cascading effects on facility safety and product integrity, assurance, and quality.

Industrial Control Systems

ICSs are vital to the efficient and safe operation of many Critical Manufacturing Sector facilities. As the Critical Manufacturing Sector advances in technical complexity, increased ICS automation and connectivity introduce new cybersecurity issues. Cyberattacks on ICSs are advancing in complexity, sophistication, and volume, leading to new methods of infiltration and disruption. The number of known cyber vulnerabilities of ICSs across all sectors has steadily increased since 2010.[20] Common high-risk ICS cyber issues include deferred security updates, unverified device firmware, buffer overflows, use of default credentials, and cross-site scripting.

- **Deferred Security Updates:** ICSs are purpose-built and can remain in operation, unmodified, for decades. Some owners and operators may believe that ICSs are safe from cyberattacks and choose to defer available ICS software and firmware updates. As a result, some ICS devices may be vulnerable to attack or be entirely unsupported.
- **Unverified Firmware:** Many ICS devices permit firmware updates through a communications interface but do not have the capability to verify that the new firmware is authentic and working properly. This can allow cyber threat actors to remotely install corrupt firmware that may go unnoticed.
- **Buffer Overflows:** Software programming errors may allow data writing buffers to extend beyond their boundaries and overwrite adjacent memory blocks. These overflows can corrupt data, crash software, or allow for the execution of malicious code. ICS components subject to buffer overflows include supervisory control and data acquisition (SCADA) systems, distributed control systems, human–machine interfaces (HMIs), and programmable logic controllers (PLCs). Some buffer overflow attacks can be conducted remotely by a cyber threat actor.
- **Default Credentials:** Manufacturers of ICS devices often provide default username and password values to allow customer access to configure the devices. Failure to replace the default credentials leaves devices open to attackers who know the default values, which are usually found in instruction manuals. Hard-coded credentials that are built into devices—with no ability to change them—pose a more serious threat. These static passwords and access keys in ICS components allow an attacker to bypass authentication configurations and requirements, gaining malicious control of HMIs, PLCs, or other networked ICS devices. Such credentialing attacks are commonly conducted remotely.
- **Cross-Site Scripting:** This attack method allows malicious scripts to be embedded into web pages. The scripts enable the cyber threat actor to steal user authentication data remotely (from web browser cookies), conduct social engineering attacks (e.g., to collect sensitive information or credentials), or spread malware. Known cross-site scripting ICS issues are found mostly in SCADA systems.

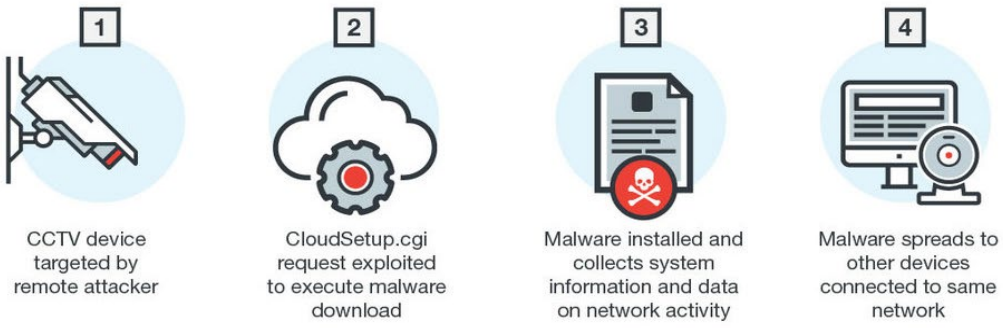
Internet of Things

Internet-connected devices, commonly referred to as IoT, are becoming more generally used in the Critical Manufacturing Sector for monitoring and controlling manufacturing processes. IoT sensors and analyzers

monitor and optimize product production, share real-time data among devices, and send alerts for faults or deficiencies. Smart packaging with radio frequency identification (RFID) optimizes supply chains and reduces operating costs. Autonomous vehicles within manufacturing facilities work on a 24-hour cycle to conduct production tasks and move or deliver components and products. IoT devices can be procured and installed in manufacturing environments with little understanding of their network activities or impact. The rising use of IoT in the sector, as well as all over the world, leads to increasing cybersecurity issues, such as more opportunities for sector devices to be attacked, increased likelihood that unrelated consumer-level devices will be used against sector infrastructure, and business operations susceptibility to DDoS attacks.

- **Multitude of Devices:** Increasing the number of IoT devices in use by Critical Manufacturing Sector operations increases the number of ways sector organizations can be attacked. Wireless communication between IoT devices in sector facilities often transmits proprietary or confidential information on processes or business operations. This information could be stolen in reconnaissance operations, or this connectivity could be abused to move within a network or to spread malware—whether remotely, internally through an insider, or in proximity to the facility. Figure 3 provides an example of IoT malware delivery.[21]
- **Critical Manufacturing Operations as a Target:** Cyber threat actors seeking to harm or exploit Critical Manufacturing Sector organizations may employ many external IoT devices in coordinated attacks for economic espionage, disruption of operations, or destruction of property. RFID applications may be exploited to deliver or trigger malware within manufacturing operations.
- **DDoS Attacks:** As described above, IoT devices can be exploited to carry out DDoS attacks. The malware saps network bandwidth and can compromise the performance of the infected devices and network.

Figure 3. *Example Infection Pathway of IoT Malware*
Source: Trend Micro



Malware and Ransomware

Malware and ransomware are common means of attack on all business IT networks and can infect Critical Manufacturing Sector organizations as well. Ransomware is a type of malware that cyber threat actors use to deny access to systems or data by encrypting the files and data on the infected computer. Typically, the threat actor requests a ransom in exchange for decrypting the data and returning functionality. Ransomware attacks have increased across all sectors, and industry IT systems are at an increased risk of attack. During 2017, the monthly rate of ransomware attacks on businesses in the United States increased tenfold, and the number of ransomware detections by a major cybersecurity vendor increased by 90 percent.[22] Also in 2017, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center received 1,783 complaints identified as ransomware with adjusted losses of over $2.3 million.[23] The prevalence of ransomware has led to some manufacturers purchasing insurance just for this kind of threat. Major examples of large-scale ransomware attacks include the May 2017 “WannaCry” attack and the April 2016 attack of a U.S. utility company.

- **WannaCry:** In May 2017, WannaCry ransomware infected organizations all over the world, encrypting and paralyzing the systems. WannaCry exploited security vulnerabilities in Windows computer systems. Information about the Windows code flaw was released in leaked National Security Agency documents, and although a patch was developed to eliminate the security vulnerability, many organizations did not download the upgrade before the attack. Although the ransomware affected mostly business control systems, the malware mechanism used could be adapted to disrupt process control systems or ICSs, which could have catastrophic effects for critical infrastructure.
- **U.S. Utility Attack:** A municipal water and power company announced its corporate network had been compromised by ransomware in April 2016. The attack was carried out through an infected email attachment opened by an employee. In response, the company disclosed the attack (the first of its kind reported in the United States), shut down its corporate network, ensured that plant operations and ICSs were not compromised, and worked on developing a solution. Ultimately, the company paid the ransom to decrypt its email and accounting systems.
- **Social Media:** Highly publicized cyber incidents such as the two described above often involve information sharing through social media. Social media can drive awareness, disseminate information, and prompt response during a cyber incident. It can allow customers and stakeholders to quickly and publicly report issues and express concerns. Organizations can use social media to their advantage to identify affected customers, directly engage, and provide guidance. However, such virtual platforms can also be used to spread misinformation (knowingly or unknowingly) and serve as a mechanism to promote an adversary's agenda.

Tactics, Techniques, and Procedures

Many cyber threat actor tactics, techniques, and procedures (TTPs) are openly available, travel rapidly across the Internet, and are globally adopted. Critical Manufacturing Sector networks and advanced products are subject to the quickly evolving landscape (and marketplace) of cyber TTPs. Potent tools to support TTPs have become widely available to cyber threat actors—for example, through the Shadow Brokers release and the availability of search tools for Internet-connected devices. As incentives change, TTPs change; for example, there is a growing focus on cryptocurrency mining using vulnerable devices. Similarly, as defenses improve, TTPs evolve to better reach well-defended targets. Advanced attack methods such as the CrashOverride malware demonstrate the increasing sophistication with which cyberattacks target critical infrastructure.

- **Shadow Brokers:** In August 2016, a group known as Shadow Brokers publicly released a large number of files, including exploitation tools for both old and newly exposed vulnerabilities. Some of the tools, such as EternalBlue, have been adapted and incorporated into new TTPs, allowing attackers to spread malware more easily with "off-the-shelf" tools.
- **Shodan:** Attackers may use openly available Internet search tools such as Shodan to identify Internet-facing devices used in manufacturing that have potentially insecure mechanisms for authentication and authorization.
- **Cryptocurrency Mining:** Criminals have developed new TTPs to steal computing power from vulnerable machines to mine cryptocurrencies. With Internet scanning tools, known vulnerabilities, and techniques to exploit them, attackers can opportunistically install cryptocurrency mining software, which can slow critical devices, cause overheating, or prevent critical functions from running.
- **CrashOverride**: CrashOverride is an advanced modular malware specifically designed to disrupt physical industrial processes, especially ICSs. While the known capabilities do not appear to be U.S.-focused, the general TTPs used in CrashOverride could be leveraged with modified technical implementations to affect U.S.-based critical infrastructure. Features of the malware's design

indicate that it was developed by a well-funded team—including experts in industrial control protocols—and that its creators intend to use this framework for future attacks. [24]

Case Study: Steel Mill Cyberattack

In late 2014, cyber threat actors successfully infiltrated a steel mill in Germany. The attack involved sending spear-phishing emails—fraudulent emails that appear to come from legitimate sources—to the facility's industrial operators. At least one recipient opened the email file attachment, which hosted malicious code. The code targeted a system vulnerability, opening a remote connection point and allowing cyber threat actors access to the corporate network. Through this opening, the threat actors could then access the plant network, penetrating the facility's production management software and gaining control of many plant systems.

The cyber threat actors caused the malfunction of critical process components, such as centralized controls, alarm systems, and HMIs. From this point, it was a simple matter to stop a blast furnace from shutting down, resulting in serious damage to the infrastructure.

The steel mill incident demonstrates the need for cyber defenses against just this type of attack. The highly connected systems prevalent in industry today allow for easy movement from the corporate system to the plant network, creating a door that is easy for an experienced cyber threat actor to enter. Therefore, systems architecture should include extreme regulation of connections between networks, as well as network security monitoring that allows analysts to track network communications and identify anomalies. As this incident indicates, it is also imperative that facility staff members receive cybersecurity training relative to their roles. Finally, plants should have plans, both cybersecurity strategies to prevent infiltration and incident response plans to minimize damage, should an attack succeed.

Criminal Activities and Terrorism

Criminal activities and terrorism affecting critical infrastructure make headlines around the world almost every day. Terrorism, which can be described as the unlawful use of violence and intimidation in the pursuit of ideological aims, can take many forms, including chemical, biological, nuclear, radiological, and explosive attacks.

In the Critical Manufacturing Sector, security and resilience issues regarding criminal activities and terrorism include active shooter incidents, the threat of malicious insiders, intellectual property theft, poisons and toxins introduced into supply chains, property damage from vehicle attacks and vandalism (including arson), and suspicious activities. Recognizing and mitigating these issues could help to limit the financial, operational, and human impacts of deliberate attacks and terrorism.

Active Shooter

The frequency of active shooter incidents in workplace environments across many sectors has increased in recent years. From 2000–2017, 250 active shooter incidents occurred in the United States, with the average annual number of incidents increasing from 7 (2000–2008) to 20 (2009–2017).[25] Injury and loss of life are the obvious impacts of such incidents. Critical Manufacturing Sector facility operations can also be affected through the loss of employee hours and downtime from compromised equipment or facilities caused by an active shooter incident.

- **Incident Management:** Active shooter situations are dynamic and quickly evolve. Often, the immediate deployment of law enforcement is required to stop the aggressive action of a shooter to mitigate harm to potential victims. However, because active shooter situations are also frequently over prior to the arrival of law enforcement, Critical Manufacturing Sector organizations must be prepared both mentally and physically to deal with an active shooter situation prior to law enforcement arrival.
- **Operational Impacts:** Facilities and equipment may be damaged from shots fired and removed from service for repairs. Operations may be halted because of the need to investigate a crime scene, which could last for weeks. Employees may not be able to return to work for an extended time because of injuries, psychological impacts, and/or the closure of a facility.

Insider Threats

The insider threat can be described as an insider using his or her authorized access, wittingly or unwittingly, to do harm to the organization's resources, personnel, facilities, information, equipment, networks, or systems. Insiders may be employees, former employees, business partners, contractors, consultants, temporary personnel, interns, or vendors. Critical Manufacturing Sector organizations should be familiar with how to identify behavioral indicators of potential insider malicious acts; implement insider threat mitigation best practices; vet personnel thoroughly before hiring; and recognize, monitor, and report on suspicious activities.

- **Behavioral Indicators:** Behavior traits that may indicate an employee may act or is acting against the employer include disgruntlement; dissatisfaction; and persistent anger, anxiety, or negative attitude. Although insiders intent on doing harm to others or themselves in the workplace may show some visible signs of discomfort or being disgruntled, they may also take steps to avoid drawing any attention to themselves, knowing that behavioral indicators may lead to detection.

- **Mitigation Actions:** Best practices for insider threat mitigation include determining behaviors and suspicious activities to monitor, developing clear reporting and investigating mechanisms, and training employees on recognition and reporting. Detecting and mitigating insider threats will almost always rely on the identification of concerning workplace behaviors in combination with select types of suspicious activity. Organizations should develop clear standard mechanisms for reporting and investigating possible insider threats, including provisions for confidential reporting to enable the protection of legitimate whistleblowers. In addition, well-informed and -trained employees are the most effective resource to prevent, identify, deter, and respond to insider threats.
- **Personnel Vetting:** Thoroughly examining and identifying the potential for malicious insider activity is imperative to reducing vulnerability to insider threat. This examination should start during an organization's hiring process and continue after the hiring process concludes. Important considerations for vetting potential personnel (employees as well as contractors and subcontractors) include procedures to properly evaluate personnel and contractor information (e.g., background checks), compliance assessments of personnel regarding insider threat policies and procedures, and a process to facilitate sharing information from human resources, law enforcement, and other pertinent sources to recognize the presence of an insider threat.
- **Suspicious Activities:** Certain activities may indicate an insider threat if they are unrelated to an individual's job duties: collecting excessive information or data (especially of a sensitive nature), frequent unexplained travel, or working uncommon hours without approval.

Intellectual Property Theft

Intellectual property is often considered a manufacturer's most valuable asset. Intellectual property can include proprietary manufacturing processes, operations data, product plans, or trade secrets. The highly competitive, global environment in which the Critical Manufacturing Sector operates is prone to intellectual property theft for illicit gain. Intellectual property may be stolen through cyberattacks, surveillance and espionage, illegal actions by current or former employees, or physical attacks.

- **Prevalence:** In a recent study by a manufacturing trade association, over a third of manufacturing executives interviewed believed intellectual property theft was the primary motive for cyberattacks experienced by their companies in the past year.[26] International supply chains often have limited remote oversight of intellectual property, which increases the potential for theft.
- **Targets:** Manufacturing firms invest a significant amount of money in research and development (R&D), with these efforts and their findings generating a competitive advantage for manufacturers. As a result, unethical competitors and organizations new to the market may endeavor to steal such intellectual property. According to a recent cybersecurity report of a major communications and IT provider, R&D intellectual property represented 90% of manufacturing data stolen in 2017.[27]
- **Methods:** Cyberattacks on manufacturers' systems and networks is a predominant method of intellectual property theft in the sector. In addition, malicious insiders can improperly access, copy, email, share, or print intellectual property—often without an audit trail. Physical attacks with the intent to steal specific intellectual property may also be used, such as breaching security barriers and controls to access a specific target (see vehicle attacks below). Surveillance by photography or through the use of unmanned aircraft systems (UASs) is another method of concern for the sector regarding intellectual property theft. See the Crosscutting Issues section for more information on UASs.

Poisons and Toxins

Harmful substances (such as ricin, botulinum, or chemical reaction precursors) maliciously introduced into the supply chains of manufacturers could have disastrous effects on sector companies, products, suppliers, or customers. Violent extremists continue to circulate how-to instructions for producing and disseminating poisons, crude biological toxins, and toxic industrial chemicals that in many cases are commercially available and easy to obtain (fortunately, these instructions are often ineffective or misleading).

- **Botulinum Toxin:** An odorless and colorless potent neurotoxin produced by *Clostridium* bacteria, botulinum toxin may be sought after by terrorists because of its toxicity in low doses. It can be used for small-scale attacks using contaminated shipping packaging or containers. Indicators of nefarious use or production of botulinum toxin include an unusual interest in, or possession of, botulinum toxin production literature or instructions; attempts to purchase *Clostridium* bacterial species or the toxin directly; theft of equipment or materials that may be used in the preparation or dispersal of chemicals or poison; and loitering or strange behaviors near shipping containers or packaging with no reasonable explanation.
- **Ricin:** This deadly toxin is easily extracted from the seeds of the castor bean plant using household items and basic chemical extraction techniques. Castor beans are used in several industries—most notably the commercial production of castor oil—and readily available for legal purchase from garden stores or through the Internet. Indicators of nefarious use or production of ricin include increased theft or purchases of castor beans from manufacturers or industrial retailers; collection or possession of castor seeds in excess of botanical requirements; unusual interest in or possession of ricin production literature or instructions; and loitering or strange behaviors with no reasonable explanation in areas where Critical Manufacturing personnel store food or gather for meals.

Property Damage

Malicious actors may attempt to cause harm to Critical Manufacturing Sector organizations through property damage to sector buildings, equipment, or other infrastructure. Vehicle attacks, vandalism, and arson are potential methods that attackers may use to cause harm. The use of vehicles as attack vectors for terror or criminal attacks has increased in recent years. Though such attacks have focused mostly on harming people in crowds, Critical Manufacturing Sector facilities may be targeted for vehicle attacks for theft of products or sensitive information or for impacts causing industrial disasters. In addition, attackers may use vandalism and arson to cause direct harm to specific manufacturers because of individual grievances or ideological protests.

- **Vehicle Attacks:** Attackers may use vehicles to directly ram and destroy perimeter barriers, fences, or facility walls with the intent of stealing specific high-value property or information. Such vehicle breaches may also be used to create an opening for attackers to carry out a secondary attack inside the facility, such as with improvised explosive devices or firearms. Vehicle impact damage could severely disrupt manufacturing facilities operations. An attacker intent on causing harm to a specific manufacturer could use a vehicle to physically destroy the machines, equipment, or supply lines critical to a particular manufacturing process, halting that facility's operations. Depending on the target and its significance in manufacturing supply chains, the ramifications of disruption could be widely detrimental to the Critical Manufacturing Sector. A vehicle attack could be used to trigger a much larger disaster than disrupting a single manufacturing facility. Manufacturing facilities may contain storage of hazardous materials used or produced in facility processes, such as large tanks of methane or propane, or heavy metal and organic waste byproducts. A direct vehicle impact on such storage equipment could trigger large explosions or cause a widespread environmental disaster.

- **Vandalism and Arson:** Vandalism is the willful or malicious destruction or defacement of public or private property. Typically, vandalism involves relatively minor destructive crimes (e.g., damaging perimeter barriers, breaking windows, tampering with security cameras, or external defacing of buildings or walls). However, vandalism could be severe enough to cause major destruction of facility property. The act could also be an indicator of intent for more serious malicious activity against Critical Manufacturing Sector facilities. Arson is the malicious burning of personal or real property with fraudulent or criminal intent. Arson can be considered a more serious form of vandalism in which fire could severely damage or completely destroy major assets. Arson at a Critical Manufacturing Sector facility could halt operations, cause explosions, and threaten the safety of personnel and adjacent communities.

Case Study: Theft of Wind Turbine Trade Secrets

In 2011, a major wind turbine manufacturer based in China stole trade secrets from a U.S. wind energy technology firm, a partner of the Chinese manufacturer for several years. The Chinese manufacturer built turbines, and the U.S. firm developed technology and software to control them.

At the time of the theft, the Chinese manufacturer had contracted with the U.S. firm for more than $800 million in products and services to be used for the wind turbines that the manufacturer produced, sold, and serviced. Rather than pay the U.S. firm under the contract, the Chinese manufacturer paid a former employee of the U.S. firm to steal proprietary controlling software code and develop a counterfeit software system to use for its turbines. The manufacturer then commissioned three wind turbines to be built in the United States incorporating the counterfeit software, presumably to test its effectiveness.

The U.S. firm suffered severe financial hardship because of the theft. It lost more than $1 billion in shareholder equity and almost 700 jobs, over half its global workforce. The U.S. Department of Justice filed a criminal complaint against the Chinese manufacturer in 2013, after receiving reports of intellectual property theft from the U.S. firm and the builders who installed the three turbines in the United States. This ultimately led to the conviction and fining of the Chinese manufacturer for conspiring to commit and committing theft of trade secrets and wire fraud.

The U.S. firm could have been more effective in identifying the activities of the Chinese manufacturer if a data loss prevention capability was employed in the U.S. firm's IT infrastructure. However, the firm's data logs and data storage were supportive in reconstructing events surrounding the theft to aid the criminal investigation.

Crosscutting Issues

The Critical Manufacturing Sector is subject to several crosscutting issues that stem from infrastructure, social, technology, and economic changes. These include aging transportation infrastructure, dependencies on other critical infrastructure sectors, geopolitical issues such as crime and conflict zones, workforce issues and readiness, and intrusion by UASs. These issues could disrupt supply chains, increase capital expenditures, lead to loss of sensitive security and operational information, and have other serious impacts. Recognizing and mitigating these issues could help to limit their impacts.

Aging Transportation Infrastructure

Age and disrepair of transportation systems render most critical infrastructure vulnerable to disruptions. The Critical Manufacturing Sector requires secure transportation to operate effectively. The American Society of Civil Engineers 2017 Infrastructure Report Card rates U.S. infrastructure as a whole at D+. Of that, roads received a D; bridges, a C+; ports, a C+; rail, a B; and inland waterways, a D. This section highlights issues for these transportation modes.[28]

- **Roads:** The Nation's roads and highways are commonly overcrowded, in disrepair, and significantly underfunded. In 2014, over $160 billion was wasted in time and fuel owing to traffic delays and congestion. Approximately 20 percent of highways are in poor condition, causing increased costs of vehicle maintenance and repairs. An approximate backlog of over $700 billion in projects awaits funding to repair existing highways, make strategic expansions, and update the highway system (e.g., for safety, operational, and environmental improvements).
- **Bridges:** In the United States, most highway bridges are designed for a life span of approximately 50 years. Of the more than 600,000 bridges in the United States, approximately 40 percent are 50 years old or older, and 9 percent are structurally deficient. Although bridge conditions have improved in recent years, funding for bridges may be inadequate to maintain or improve current capacities. An estimated $123 billion is needed to eliminate the Nation's bridge upgrade backlog.
- **Ports:** The vast majority of the Nation's international trade—99 percent—flows through its ports, accounting for approximately 26 percent of its economy. As the ships carrying this cargo continue to increase in size and capacity, U.S. ports become more congested and less able to accommodate the largest ships. Ports are expected to spend approximately $155 billion from 2016–2020 to expand, modernize, and repair in response to demands of international trade. Connected infrastructure (land, rail, and inland waterway connections to ports) requires commensurate aid, yet funding for these improvements and repairs is lacking.
- **Rail:** The freight rail industry has made important investments and repairs in the past several years to improve its systems and meet future needs. Short rail lines are in need of upgrading and maintenance funding—more so than long-distance lines—to advance in freight car size capacity and repair and replace bridges.
- **Inland Waterways:** A total of 50,000 miles of canals, locks, and dams comprise the U.S. inland waterways system, the majority of which is older than the original 50-year design life of its components. An important part of freight transportation, these waterways connect ocean ports with inland transportation hubs and account for approximately 14 percent of domestic freight. Age and disrepair with lack of funding result in frequent delays for hours at a time, contributing to economic losses. Although investments have been increasing in recent years, repair and upgrade projects can take decades to complete.

Dependencies on Other Sectors

Critical Manufacturing Sector facilities and processes are energy- and water-intensive. Critical Manufacturing is also very reliant on the Communications, Information Technology, Financial Services, and Transportation Systems Sectors. Incidents and disruptions affecting these sectors can have negative impacts on the Critical Manufacturing Sector.

- **Communications:** Communications networks underpin the coordination of supply chain movements and control system processes. The global positioning system is vital for navigation and timing along supply chains and is subject to disruption and tampering ("spoofing" of location and time). Owners and operators rely on the Communications Sector for telecommunications access for operations and logistics. The Critical Manufacturing Sector also relies on Communications Sector services for emergency notification and response.
- **Energy:** Manufacturers require large amounts of uninterrupted energy—including electricity, natural gas, diesel, and other forms or fuels—for all critical operations. Backup generation equipment is a major component of energy security in manufacturing.
- **Financial Services:** Secure and functioning financial services are vital to the business operations of the Critical Manufacturing Sector. Global manufacturing industries are complex, involving fluctuating international markets, numerous currencies, and large business transactions among multinational corporations.
- **Information Technology:** Critical Manufacturing Sector facilities rely heavily on IT for their manufacturing operations, global transit, business operations, quality control systems, critical processes, facility security, and cybersecurity.
- **Transportation Systems:** The Transportation Systems Sector enables the global movement of large and specialized materials and products on strict timelines. Manufacturers depend on multiple modes of transportation (e.g., aviation, freight rail, highway, and maritime) for the secure movement of raw materials and finished products.
- **Water and Wastewater Systems:** Many manufacturing processes depend on continuous clean water supply and wastewater services.

Geopolitical Issues

Availability of materials may be affected by geopolitical disturbances (e.g., materials originating from conflict zones of the world) or regional/global scarcity. Critical Manufacturing operations and supply chains are susceptible to geopolitical disruptions and areas of heightened crime.

- **Conflict Zones:** Areas of the world considered conflict zones include areas in a state of armed conflict, areas in a fragile post-conflict state, areas with inadequate or without governance and security (e.g., failed states), and areas with widespread violations of international law, including human rights abuses. Delivery of raw materials originating from such areas is subject to disruption by conflict and regulation. As conflict zones change over time, manufacturers may be subject to unexpected disruptions or regulatory requirements, often with little warning.
- **Crime:** Areas of heightened crime throughout the world can affect the security and resilience of the Critical Manufacturing Sector. Crime-afflicted areas that coincide with major manufacturing contribute additional risk to sector operations and supply chains. Current examples include corruption, organized crime, and violence associated with the illegal drug trade, affecting manufacturing in Mexico and Brazil. Some manufacturers in these regions have invested in armored

vehicles to protect their assets and supply chain from hijacking and theft. Manufacturers can incur significant losses in production, employment, and profit in areas of heightened crime.

- **Political Impacts on Costs:** Political issues endemic to specific countries or regions can greatly influence the cost of doing business in those areas. Issues of concern that can influence manufacturing costs include governmental price manipulations of scarce materials, hostile governments taking control of private manufacturing companies, changing trade agreements, restriction of import and export mechanisms, and local labor force strikes. Impacts on costs from such issues could include decreased availability/increased cost of labor, increased commodity prices, decreased access to products and transport, and increased shipping and border-crossing costs.

Workforce Issues

Workforce issues that can affect Critical Manufacturing Sector security and resilience include an aging workforce that will need to be replaced, the skills gap between manufacturers' expectations of future demand and potential employees' skills, heightened international competition for labor skillsets, and the opioid crisis's affecting workforce readiness.

- **Aging Workforce:** Many Critical Manufacturing Sector organizations are concerned that as the average age of its workforce continues to increase and highly skilled and experienced employees retire, replacing such institutional knowledge and expertise will be challenging. In 2000, the median age of the U.S. manufacturing workforce was 40.5, which is 1.1 years above the median age of the total U.S. workforce. In 2017, the median age in manufacturing was 44.5 years, versus 42.2 years for the total workforce.[29] The median manufacturing workforce age is rising disproportionately to that of other industries, and employers will need to address the potential for labor shortages due to retirement.
- **Gaps in Skill Demand:** Coupled with the concern regarding an aging workforce, manufacturers are also challenged with filling the gap between the demand of skills consistent with strategic goals and the pool of potential new hires that employers find in the current labor market. Skilled manufacturing workers are more difficult to locate and hire than in the past.
- **International Workforce Competition:** The international labor market for specific skills in manufacturing has led to competition challenges. As more areas of the world develop highly skilled manufacturing workforces, global manufacturers relocate operations to those areas in which the labor cost per level of skill is less than in historical centers of highly skilled labor (i.e., developing nations competing with developed nations).
- **Opioid Crisis:** The opioid crisis in the United States is rapidly expanding. Drug overdose deaths and opioid-involved deaths continue to increase. The majority of drug overdose deaths (more than six out of ten) involve an opioid. Since 1999, the number of overdose deaths involving opioids (including prescription opioids and heroin) has more than quadrupled.[30] Illegal production and distribution of opioids has led to increased concentrations of stronger opioids (especially fentanyl) included with illicit and counterfeit drugs. This greatly increases the risk of overdose and death. As more of the U.S. population confronts opioid addiction and death, the potential for the crisis to affect Critical Manufacturing organizations and operations increases.

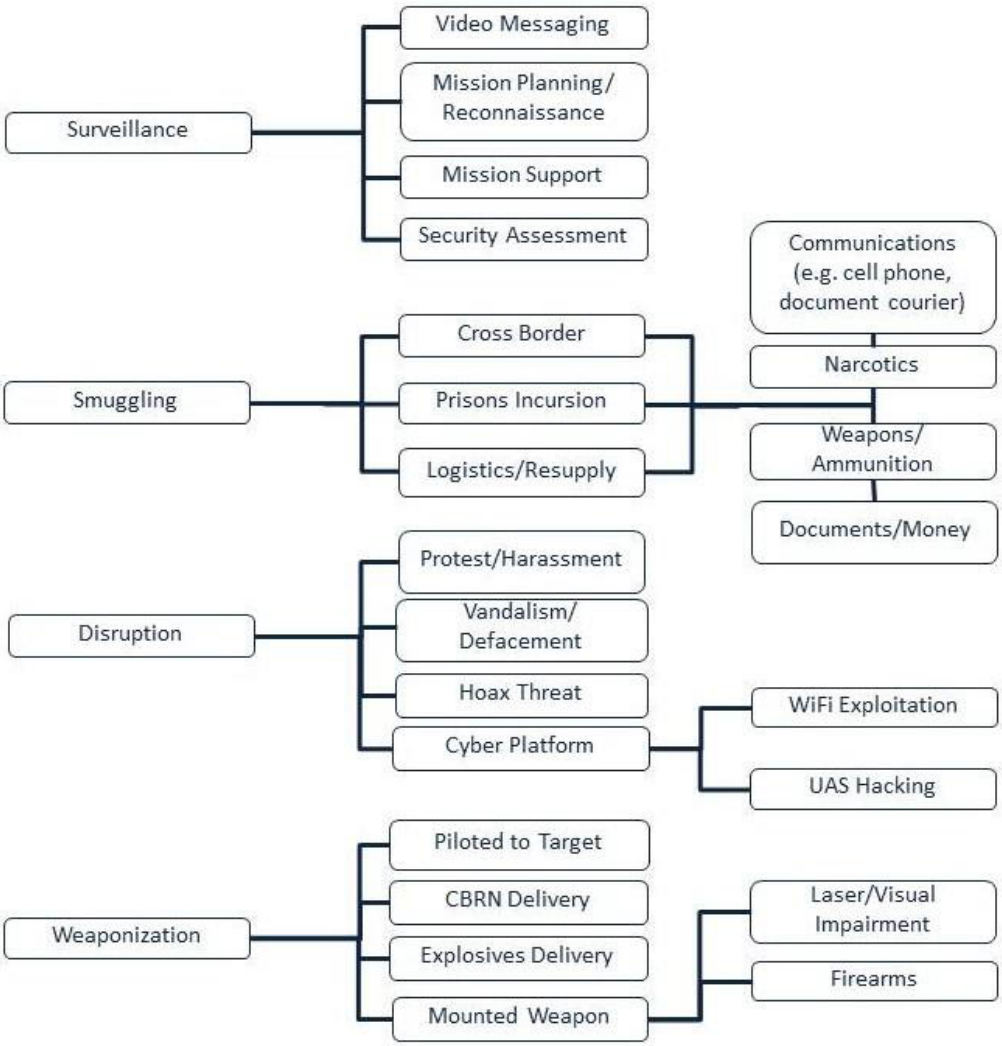
Unmanned Aircraft Systems

The Federal Aviation Administration (FAA) estimates that the number of consumer UASs will increase from 1.9 million in 2016 to approximately 4.3 million by the end of 2020.[31] Recent known malicious use of UASs includes intrusions on large public gatherings, power infrastructure damage and outages, and radiological

material delivery. Critical Manufacturing Sector facilities with traditionally distinct access pathways and perimeter security are susceptible to UAS intrusion because the facility security was likely not designed to address small, remotely controlled, or autonomous aircraft. Malicious UAS activity (see Figure 4) typically may be categorized as relating to surveillance, smuggling, disruption, or weaponization.[32]

- **Surveillance:** Adversaries can use UAS video capabilities for preoperational planning to monitor and assess security operations at sensitive sites, large-scale events, and law enforcement and emergency response operations.
- **Smuggling:** UAS payload capabilities can be exploited to deliver illicit or contraband materials to bypass security barriers.
- **Disruption:** Adversaries can direct UASs close to a facility to access, monitor, or attack computer networks and/or monitor or interfere with radio frequency communications. UAS use in proximity to a facility, whether intentional or unintentional, can harass, hinder, or inhibit security operations.
- **Weaponization:** UASs can be central to an attack intended to cause casualties or physical damage. Actions can include disrupting air traffic, deliberately crashing, and delivering a hazardous payload (e.g., an explosive device or a chemical, biological, or radiological weapon).

Figure 4. *Categories and Examples of Malicious UAS Activity*
Source: DHS I&A



Case Study: Supply Chain Consequences from Bridge Disruption

The City of Memphis plays a critical role in the regional, national, and global supply chain, enabled by a robust and diverse transportation system. Memphis is home to the second-busiest freight cargo airport in the world, third-busiest trucking corridor in the nation, third-largest national rail center, and fourth-largest inland port. Colloquially known as "America's Distribution Center," Memphis' transportation systems, particularly highway and rail, depend on direct passage across the Mississippi River for goods to reach their ultimate destination. Four bridges serve this function. In 2017, the U.S. Department of Homeland Security (DHS) conducted an infrastructure impact assessment based on a scenario in which these major bridges are shut down for two to four weeks.

DHS assessed that supply chains utilizing freight rail most likely would experience regional-level impacts from a bridge disruption. Without bridge connectivity, freight trains would be forced to reroute to other comparably suitable facilities in the region, most likely Chicago and Kansas City. These facilities are routinely operating at or near capacity, and a resulting inflow of unanticipated trains would generate significant congestion within intermodal and non-intermodal facilities, while simultaneously saturating alternative routes with traffic. Rail congestion would cause significant delays throughout the region.

DHS assessed that supply chains that rely on highway Mississippi River bridges would likely experience disruptions limited to the local level if these bridges were closed temporarily. Trucks transiting either of the central highway arteries would be forced to divert to the next available bridge. Delayed shipments and increased fuel consumption would increase operator costs temporarily, but deliveries would still be able to reach their destination only a few hours later than intended. Long-haul trucks would adjust their routing to accommodate a disruption, minimizing the impact to supply chains outside of the Memphis metropolitan area.

In contrast to rail and highway supply chains, DHS assessed that little to no impact to supply chains utilizing maritime systems or aviation would be felt from a bridge disruption. Mississippi River shipping would not experience any interruption beyond workers from West Memphis arriving late for their shifts. Supply chains utilizing river shipping would still have access to the Memphis Port terminals. Air freight systems would likely not experience any interruptions in operations.

Endnotes

[1] Defense Systems Information Analysis Center, Combating Counterfeit Components in the DoD Supply Chain (March 2015)
[2] Flight Safety Australia, For the want of a genuine part… (April 2015)
[3] DHS, Critical Manufacturing Sector-Specific Plan (May 2016)
[4] The Asian Journal of Shipping and Logistics, Cost Consequences of a Port-Related Supply Chain Disruption (September 2015)
[5] DHL, A Look Back at 2015: The Top 10 Supply Chain Disruptions (January 2016)
[6] Resilinc, EventWatch 2015 Annual Report (January 2016)
[7] Reuters, Boom, bust and boom again for rare earths? (September 2017)
[8] World Economic Forum, Enabling Trade: Valuing Growth Opportunities (February 2013)
[9] Symantec, Internet Security Threat Report (April 2018)
[10] Trucks.com, Torrid Rate of Trucking Mergers Pauses, but More Consolidation Expected (September 2016)
[11] DHS Office of Cyber and Infrastructure Analysis (OCIA), Consequences to Critical Infrastructure from Container Shipping Disruptions (April 2017)
[12] National Oceanic and Atmospheric Administration, Billion-Dollar Weather and Climate Disasters, January 2018
[13] Energy Information Administration, Hurricane Harvey caused U.S. Gulf Coast refinery runs to drop, gasoline prices to rise (September 2017)
[14] OCIA, Columbia River Basin Petroleum and Refined-Product Supplies: Disruptions and Mitigations Under Cascadia Subduction Zone Earthquake Scenario (July 2016)
[15] San Gabriel Valley Tribune, What a major earthquake would do to Southern California's economy (March 2016)
[16] Central United States Earthquake Consortium, After-Action Report (September 2014)
[17] Talos, New VPNFilter malware targets at least 500K networking devices worldwide (May 2018)
[18] McAfee Labs, Threats Report, (April 2017)
[19] The Register, World's biggest DDoS attack record broken after just five days (March 2018)
[20] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 2016 Annual Vulnerability Coordination Report (September 2017)
[21] Trend Micro, New Linux Malware Exploits CGI Vulnerability (March 2017)
[22] Malwarebytes Labs, Cybercrime tactics and techniques: 2017 state of malware (January 2018)
[23] FBI, 2017 Internet Crime Report (May 2018)
[24] Dragos, CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations (September 2018)
[25] Federal Bureau of Investigation (FBI), Quick Look: 250 Active Shooter Incidents in the United States From 2000 to 2017 (January 2018)
[26] Deloitte and Manufacturers Alliance for Productivity and Innovation, Cyber risk in advanced manufacturing (November 2016)
[27] Verizon, 2018 Data Breach Investigations Report (March 2018)
[28] American Society of Civil Engineers (ASCE), 2017 Infrastructure Report Card, March 2017
[29] U.S. Department of Labor, Labor Force Statistics from the Current Population Survey (January 2018)
[30] Centers for Disease Control and Prevention, Opioid Overdose (August 2017)
[31] DHS Office of Intelligence and Analysis (I&A), Unmanned Aircraft Systems Addressing Critical Infrastructure Security Challenges (February 2017)
[32] DHS I&A, Emerging Adversary Use of Unmanned Aircraft Systems Present Detection and Disruption Challenges (July 2015)

Appendix A. Resources

Key resources for this document are listed below in alphabetical order within each chapter topic. Entries without links are available from the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) website. HSIN-CI is the primary system through which private-sector owners and operators, DHS, and other federal, state, and local government agencies collaborate to protect the Nation's critical infrastructure. HSIN-CI provides real-time collaboration tools including a virtual meeting space, document sharing, alerts, and instant messaging at no charge. Visit www.dhs.gov/hsin-critical-infrastructure for more information.

Supply Chain Security and Resilience

The Asian Journal of Shipping and Logistics, Cost Consequences of a Port-Related Supply Chain Disruption (September 2015) https://www.sciencedirect.com/science/article/pii/S2092521215000504#bbib0055

Crime Science: An Interdisciplinary Journal, Defining the types of counterfeiters, counterfeiting, and offender organizations (December 2013) https://crimesciencejournal.springeropen.com/articles/10.1186/2193-7680-2-8

Defense Systems Information Analysis Center, Combating Counterfeit Components in the DoD Supply Chain (March 2015) https://www.dsiac.org/resources/journals/dsiac/spring-2015-volume-2-number-2/combating-counterfeit-components-dod-supply

DHL, A Look Back at 2015: The Top 10 Supply Chain Disruptions (January 2016) http://www.delivered.dhl.com/en/articles/2015/11/a-look-back-at-2015-the-top-10-supply-chain-disruptions.html

DHS, Critical Manufacturing Sector-Specific Plan (May 2016) https://www.dhs.gov/sites/default/files/publications/nipp-ssp-critical-manufacturing-2015-508.pdf

Flight Safety Australia, For the want of a genuine part… (April 2015) http://www.flightsafetyaustralia.com/2015/04/for-the-want-of-a-genuine-part/

Forbes, Supply Chain Risk a Hidden Liability for Many Companies (October 2012) https://www.forbes.com/sites/steveculp/2012/10/08/supply-chain-risk-a-hidden-liability-for-many-companies/

The Journal of Commerce, Mergers hit nine-year high in 2015, show little signs of slowing (January 2016) https://www.joc.com/international-logistics/logistics-providers/mergers-hit-nine-year-high-2015-show-little-signs-slowing_20160105.html

OCIA, Consequences to Critical Infrastructure from Container Shipping Disruptions (April 2017)

Resilinc, EventWatch 2015 Annual Report (January 2016) https://www.resilinc.com/eventwatch-2015-annual-report/

Reuters, Boom, bust and boom again for rare earths? (September 2017) https://www.reuters.com/article/us-china-rareearths-ahome/boom-bust-and-boom-again-for-rare-earths-idUSKCN1BC4OF

Trucks.com, Torrid Rate of Trucking Mergers Pauses, but More Consolidation Expected (September 2016) https://www.trucks.com/2016/09/20/trucking-mergers-paused/

World Economic Forum, Enabling Trade: Valuing Growth Opportunities (February 2013) https://www.weforum.org/reports/enabling-trade-valuing-growth-opportunities

Natural Hazards

Central United States Earthquake Consortium, After-Action Report (September 2014) http://www.cusec.org/capstone14/documents/CAPSTONE-14_AAR.pdf

Natural Hazards, Industrial accidents triggered by earthquakes, floods and lightning: lessons learned from a database analysis (October 2011) https://link.springer.com/article/10.1007/s11069-011-9754-3

NOAA, Atlantic Hurricane Season Outlook (May 2018) http://www.cpc.ncep.noaa.gov/products/outlooks/hurricane.shtml

NOAA, Billion-Dollar Weather and Climate Disasters (January 2018) https://www.ncdc.noaa.gov/billions/overview

NOAA, National Hydrologic Assessment (Spring Flooding Outlook) (Annual, March 2018) http://www.nws.noaa.gov/oh/

OCIA, Columbia River Basin Petroleum and Refined-Product Supplies: Disruptions and Mitigations Under Cascadia Subduction Zone Earthquake Scenario (July 2016)

OCIA, Flooding and Potential Effects to Critical Infrastructure (Annual, April 2017)

Cybersecurity

Cisco, 2018 Annual Cybersecurity Report (February 2018) https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

DHS and FBI, Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors (June 2017)

DHS I&A, Intelligence Assessment: Increasing Use of Ransomware May Threaten US Civilian Government and Critical Infrastructure Networks (August 2016)

DHS I&A, Likely Advanced Persistent Threat Actors Attempt Phishing Attack against South Dakota-Based Energy Company (August 2017)

Dragos, CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations (September 2018) https://dragos.com/wp-content/uploads/CrashOverride-01.pdf

Dragos, TRISIS Malware: Analysis of Safety System Targeted Malware (December 2017) https://dragos.com/blog/trisis/TRISIS-01.pdf

E-ISAC, Internet of Things DDoS White Paper (October 2016) https://nhisac.org/wp-content/uploads/2016/10/Internet-of-Things-DDoS-White-Paper-2.pdf

FBI, 2017 Internet Crime Report (May 2018) https://pdf.ic3.gov/2017_IC3Report.pdf

FireEye, Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure (December 2017) https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

ICS-CERT, 2016 Annual Vulnerability Coordination Report (September 2017) https://www.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf

ICS-CERT, Advisories (multiple dates) https://www.us-cert.gov/ics/advisories

ICS-CERT, Alerts (multiple dates) https://www.us-cert.gov/ics/alerts

Industrial Internet Consortium: Industrial Internet of Things Volume G4: Security Framework (September 2016) https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

Malwarebytes Labs, Cybercrime tactics and techniques: 2017 state of malware (January 2018) https://www.malwarebytes.com/pdf/white-papers/CTNT-Q4-17.pdf

McAfee Labs, 2017 Threats Predictions (annual, November 2016) https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf

McAfee Labs, 2018 Threats Predictions (annual, November 2017) https://securingtomorrow.mcafee.com/mcafee-labs/2018-threats-predictions/

McAfee Labs, Threats Report (Quarterly, April 2017) https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf

National Institute of Standards and Technology (NIST), Commission on Enhancing National Cybersecurity Report on Securing and Growing the Digital Economy (December 2016) https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

OCIA, Cybersecurity Risks Posed by Unmanned Aircraft Systems (May 2018)

OCIA, Industrial Control Systems Overview (March 2018)

OCIA, Potential Impacts of WannaCry Ransomware on Critical Infrastructure (May 2017)

OCIA, Ransomware: Goals of Malicious Actors and Current System Vulnerabilities (June 2017)

OCIA, Risks to Critical Infrastructure that Use Cloud Services (June 2017)

The Register, World's biggest DDoS attack record broken after just five days (March 2018) https://www.theregister.co.uk/2018/03/05/worlds_biggest_ddos_attack_record_broken_after_just_five_days/

SANS Institute, Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017 (annual, March 2017) https://www.sans.org/reading-room/whitepapers/analyst/cyber-security-trends-aiming-target-increase-security-2017-37702

SANS Institute, The Industrial Control System Cyber Kill Chain (October 2015) https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

Symantec, Internet Security Threat Report (annual, April 2017, 2018) https://www.symantec.com/security-center/threat-report

Talos, New VPNFilter malware targets at least 500K networking devices worldwide (May 2018) https://blog.talosintelligence.com/2018/05/VPNFilter.html

Trend Micro, New Linux Malware Exploits CGI Vulnerability (March 2017) http://blog.trendmicro.com/trendlabs-security-intelligence/new-linux-malware-exploits-cgi-vulnerability/

US-CERT, Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (March 2018) https://www.us-cert.gov/ncas/alerts/TA18-074A

US-CERT, Heightened DDoS Threat Posed by Mirai and Other Botnets (October 2016) https://www.us-cert.gov/ncas/alerts/TA16-288A

US-CERT, The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations (September 2016) https://www.us-cert.gov/ncas/alerts/TA16-250A

Verizon, 2018 Data Breach Investigations Report (March 2018) https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Criminal Activities and Terrorism

CSO Online, Sinovel Wind Group found guilty of IP theft, fined $1.5 million (July 2018) https://www.csoonline.com/article/3256305/sinovel-wind-group-found-guilty-of-ip-theft-valued-at-800-million.html

Deloitte and Manufacturers Alliance for Productivity and Innovation, Cyber risk in advanced manufacturing (November 2016) https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html

DHS I&A Reference Aid: Malicious Terrorism Hoaxes Likely to Endure, Strain State and Local First Responder Resources (August 2016)

DHS I&A, Roll Call Release: Online Information May Provide Potential Roadmap for Crude Chemical–Biological Attacks (March 2017)

DHS I&A, Roll Call Release: Small-Scale Poisons and Toxins Primer: Botulinum Toxin (August 2017)

DHS I&A, Roll Call Release: Small-Scale Poisons and Toxins Primer: Nicotine (March 2017)

DHS I&A, Roll Call Release: Small-Scale Poisons and Toxins Primer: Ricin (March 2017)

DHS I&A, Roll Call Release: Terrorist Chemical and Biological Agents of Opportunity Primer: Hydrogen Sulfide (August 2017)

DHS I&A, Trend Analysis: Terrorist Incidents in the US, Canada, and Europe, May–August 2016 (October 2016)

DHS I&A, Trend Analysis: Terrorist Incidents in the West, September–December 2016 (April 2017)

FBI, Quick Look: 250 Active Shooter Incidents in the United States From 2000 to 2017 (January 2018) https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents-graphics

House Homeland Security Committee, Terror Threat Snapshots (December 2016, February 2017, April 2017)

Institute for Economics & Peace, Global Terrorism Index 2017 (Annual, November 2017) http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf

NCTC, Counterterrorism Digest (weekly, multiple 2017 dates available)

OCIA, Awareness of Indicators of Peroxide-Based Explosives May Aid in Disruption of Attacks (June 2017)

OCIA, Commercial Facilities Sector Remains Attractive Target for Vehicle-Ramming Attacks (May 2017)

Crosscutting Issues

Centers for Disease Control and Prevention, Opioid Overdose (August 2017) https://www.cdc.gov/drugoverdose/opioids/index.html

CERT, Common Sense Guide to Mitigating Insider Threats (December 2016) http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

CERT, Insider Threat Center (April 2016) http://resources.sei.cmu.edu/asset_files/Brochure/2016_015_001_452233.pdf

DHS Science and Technology Directorate, Cyber Security Division – Insider Threat Brochure (March 2016) https://www.dhs.gov/sites/default/files/publications/508_CSD_Insider%20Threat_Onepager_20160303_Final.pdf

DHS I&A, Emerging Adversary Use of Unmanned Aircraft Systems Present Detection and Disruption Challenges (July 2015)

DHS I&A, Unmanned Aircraft Systems Overview and Response Considerations (March 2017)

DHS, Unmanned Aircraft Systems Addressing Critical Infrastructure Security Challenges (February 2017) https://www.dhs.gov/sites/default/files/publications/uas-ci-challenges-fact-sheet-508.pdf

Idaho National Laboratory, Evaluation of Unmanned Aerial Systems Threat against U.S. Critical Infrastructure (May 2017)

Intelligence and National Security Alliance, Assessing the Mind of the Malicious Insider (April 2017) https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_Mind_Insider_FIN.pdf

Journal of Economic Geography, The good, the bad and the ugly: the socioeconomic impact of drug cartels and their violence (October 2017) https://doi.org/10.1093/jeg/lbx034

HSIN-CI Suspicious Activity Reporting (SAR) (multiple 2016–2018 dates)

The National Insider Threat Task Force (NITTF), Government Best Practices for Insider Threat (June 2016) https://www.dni.gov/files/NCSC/documents/products/Govt_Best_Practices_Guide_Insider_Threat.pdf

OCIA, Insider Threat Behaviors and Mitigation Recommendations (March 2017)

OCIA, U.S. Critical Infrastructure 2025: A Strategic Risk Assessment (April 2016)

OCIA, Impacts to Memphis Supply Chain from Mississippi River Crossings Shutdown (July 2017)

SANS Institute, Insider Threat Mitigation Guidance (October 2015) https://www.sans.org/reading-room/whitepapers/monitoring/insider-threat-mitigation-guidance-36307

U.S. Department of Labor, Labor Force Statistics from the Current Population Survey (January 2018) https://www.bls.gov/cps/cpsaat18b.htm

Appendix B. Tools, Training, and Programs

Relevant tools, training, and programs that may help Critical Manufacturing Sector stakeholders address the security and resilience issues described in this document are listed below. These resources are organized by alphabetical order within each chapter topic. This listing is not exhaustive but provides key resources sector stakeholders may find useful.

Supply Chain Security and Resilience

Academy of Aerospace Quality (AAQ) Counterfeit Parts Course – This online course outlines the impacts of counterfeit parts, as well as how different organizations address the problem. http://aaq.auburn.edu/counterfeit-parts

American Bearing Manufacturers Association's Customs Education Seminar – ABMA offers this training opportunity to help government law enforcement improve customs enforcement against counterfeit bearings. https://www.americanbearings.org/page/anti_c_domestic

Electric Power Research Institute Training – EPRI offers this nuclear-industry-specific training that includes modules describing counterfeit, fraudulent, and substandard items; identifying the risks they present; and describing actions that can be implemented to reduce risk. https://www.epri.com/#/pages/product/1020955/?lang=en

U.S. Department of Defense, Defense Acquisition University – This series of guidebooks, best practices, and training courses focuses on counterfeit parts. https://www.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=5ea0eba7-13f0-40be-9ec7-0e1fa52934ad

U.S. Nuclear Regulatory Commission (NRC) Counterfeit, Fraudulent, Suspect Item (CFSI) Training Offerings – The U.S. NRC Information Notice 2012-22 lists training opportunities for education and awareness on counterfeit, fraudulent, or suspect components. https://www.nrc.gov/docs/ML1231/ML12318A216.pdf

Cybersecurity

CERT Network Security Training – This training provides technical staff members, engineers, software managers, and technical leads best practices and practical techniques for protecting the security of their organizations' information assets and resources. https://www.cert.org/training/

Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance – This DHS guidance document was developed to help Critical Manufacturing Sector owners and operators use the voluntary NIST Framework for Improving Critical Infrastructure Cybersecurity. https://www.dhs.gov/publication/critical-manufacturing-cybersecurity-framework-implementation-guidance

Cyber Security Evaluation Tool (CSET) – CSET is a DHS product that assists organizations in protecting their key national cyber assets. This desktop software tool guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. https://www.us-cert.gov/ics/Assessments

Cybersecurity for Small Businesses – This 30-minute, self-paced training exercise from the Small Business Administration provides an introduction to securing information in small businesses. https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses

DHS Critical Infrastructure Cyber Community (C3) Voluntary Program Small and Midsize Business (SMB) Toolkit – To help business leaders get started, DHS has provided a list of top resources specially designed to help SMBs recognize and address their cybersecurity risks. https://www.us-cert.gov/sites/default/files/c3vp/smb/Top_SMB_Resources.pdf

Federal Virtual Training Environment (FedVTE) – FedVTE is a free online, on-demand cybersecurity training system that is available to government personnel and veterans. Managed by DHS as part of the National Initiative for Cybersecurity Careers and Studies (NICCS), FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis. https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte

Federal Communications Commission Small Biz Cyber Planner – This planner helps businesses create custom cybersecurity plans and includes information on cyber insurance, advanced spyware, and how to install protective software. https://www.fcc.gov/cyberplanner

Federal Trade Commission: Protecting Small Businesses – This small business website helps business owners avoid scams, protect their computers and networks, and keep their customers' and employees' data safe. https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/small-businesses

ICS-CERT Monitor – CISA provides a newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets. https://www.us-cert.gov/ics/monitors

Industrial Control Systems Cybersecurity Training – CISA industrial control systems program training events consist of regional training courses and workshops at venues in various locations, in addition to a 5-day training event held in Idaho Falls, Idaho. https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

Internet Essentials for Business 2.0 – This guide from the U.S. Chamber of Commerce for business owners, managers, and employees focuses on identifying common online risks, best practices for securing networks and information, and what to do when a cyber incident occurs.
https://www.uschamber.com/CybersecurityEssentials

NIST Baldridge Cybersecurity Excellence Builder – This self-assessment tool helps organizations better understand the effectiveness of their cybersecurity risk management efforts and identity improvement opportunities in the context of their overall organizational performance.
https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative

NIST Framework for Improving Critical Infrastructure Cybersecurity – This voluntary framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of Critical Infrastructure and other sectors important to the economy and national security. https://www.nist.gov/cyberframework

NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide – This publication assists organizations with establishing computer security incident response capabilities and handling incidents efficiently and effectively. The document provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.
https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Stop.Think.Connect. Toolkit – The Stop.Think.Connect. campaign has an online Toolkit that includes information specific to SMBs. https://www.dhs.gov/stopthinkconnect-toolkit

United States Secret Service Electronic Crimes Task Forces (ECTFs) – ECTFs prevent, detect, and investigate various forms of electronic crimes, including cyber crime. ECTFs rely on trusted partnerships between the law enforcement community, the private sector, and members of academia to combat cyber crime through information sharing, coordinated investigations, technical expertise, and training. https://www.secretservice.gov/data/investigation/USSS-Cyber-Investigations-Flyer.pdf

US-CERT Automated Indicator Sharing (AIS) – The CISA AIS capability enables the exchange of cyber threat indicators (e.g., malicious IP addresses or the sender address of a phishing email) between the Federal Government and the private sector at machine speed. https://www.us-cert.gov/ais

White Paper: Every Small Business Should Use the NIST Cybersecurity Framework – This white paper from eManagement can help SMBs understand and use NIST's Cybersecurity Framework. It provides cybersecurity tips for SMBs aligned to the framework's core functions: Identify, Protect, Detect, Respond, and Recover. https://cyber-rx.com/wp-content/uploads/2015/08/CyberRx-white-paper_SBs-should-use-NIST-CS-Framework_FINAL-20150804.pdf

Natural Hazards

IS-324.a: Community Hurricane Preparedness – This Federal Emergency Management Agency (FEMA) course provides people involved in the decision-making process for hurricane preparedness with basic information about how hurricanes form, the hazards they pose, how the National Weather Service forecasts future hurricane behavior, and what tools and guiding principles can help emergency managers prepare their communities. https://training.fema.gov/is/courseoverview.aspx?code=IS-324.a

IS-325: Earthquake Basics: Science, Risk and Mitigation – This FEMA course presents basic information on earthquake science, risk, and mitigation. It also discusses techniques for structural and non-structural earthquake mitigation. https://training.fema.gov/is/courseoverview.aspx?code=IS-325

Ready Business – The DHS Ready Business program assists businesses with developing a preparedness program by providing tools to create a plan that addresses the impact of many hazards. This website and its tools utilize an "all hazards approach" and follow the program elements within National Fire Protection Association 1600, Standard on Disaster/Emergency Management and Business Continuity Programs. https://www.ready.gov/business

Criminal Activities and Terrorism

Active Shooter Preparedness Program – DHS maintains a comprehensive set of resources and in-person and online trainings that focus on behavioral indicators, potential attack methods, how to develop emergency action plans, and the actions that may be taken during an incident. https://www.dhs.gov/active-shooter-preparedness

Counter-Improvised Explosive Device (IED) Awareness Products – The DHS Office of Bombing Prevention (OBP) provides a wide array of awareness products—including cards, posters, checklists, guides, videos, briefings, and applications—that share counter-IED awareness information with the general public and across the public and private sectors to prevent, protect against, respond to, and mitigate bombing incidents. https://www.dhs.gov/counter-ied-awareness-products

Counter-IED Training and Awareness – OBP develops tools to improve national preparedness for bombing threats at all levels of government, for the public, and within the private sector. Course options include bombing prevention workshops, soft target awareness, and surveillance detection. https://www.dhs.gov/publication/bombing-prevention-training-fact-sheet

Economic Espionage Campaign – The FBI nationwide awareness campaign is geared toward educating business and industry leaders about the growing threat of economic espionage. https://www.fbi.gov/news/stories/economic-espionage

Insider Threat project – The DHS Science and Technology Directorate Insider Threat project develops solutions that complement and expand capabilities of existing commercial insider threat tools and furthers insider threat research. https://www.dhs.gov/science-and-technology/csd-insider-threat

IS-906: Workplace Security Awareness – This FEMA course provides guidance to individuals and organizations on how to improve the security in the workplace. No workplace—be it an office building, construction site, factory floor, or retail store—is immune from security threats. https://training.fema.gov/is/courseoverview.aspx?code=IS-906

IS-907: Active Shooter: What You Can Do – This FEMA course provides guidance to individuals, including managers and employees, so that they can prepare to respond to an active shooter situation. https://training.fema.gov/is/courseoverview.aspx?code=IS-907

IS-914: Surveillance Awareness: What You Can Do – The purpose of this FEMA course is to make critical infrastructure employees and service providers aware of actions they can take to detect and report suspicious activities associated with adversarial surveillance. https://training.fema.gov/is/courseoverview.aspx?code=IS-914

IS-915: Protecting Critical Infrastructure against Insider Threats – This FEMA course provides guidance to critical infrastructure employees and service providers on how to identify and take action against insider threats to critical infrastructure. https://training.fema.gov/is/courseoverview.aspx?code=IS-915

IS-916: Critical Infrastructure Security: Theft and Diversion – What You Can Do – This FEMA course introduces critical infrastructure personnel to the information they need and the resources available to them to identify threats and vulnerabilities to critical infrastructure from the theft and diversion of critical resources, raw materials, and products that can be used for criminal or terrorist activities. https://training.fema.gov/is/courseoverview.aspx?code=IS-916

Risk Assessment & Insider Threat Training – CERT Risk Assessment & Insider Threat training teaches managers, executives, security and business continuity professionals, risk managers, compliance personnel, and insider threat program managers to develop strategies for protecting their organizations from security threats and to better manage their risks. Topics covered include the CERT Resilience Management Model (CERT-RMM), OCTAVE Allegro method, and insider threat program management best practices. https://www.cert.org/training/

Spotting Insider Threats Guide – The FBI Office of the Private Sector guide defines insider threats and lists what to do when such threats are discovered. https://www.fbi.gov/file-repository/spotting-insider-threat_508.pdf

Strategic Partnership Programs – Strategic Partnership Coordinators in FBI field offices can assist business or academic institutions with protecting their technologies and preventing significant economic and national security losses. https://www.fbi.gov/file-repository/counterintelligence-strategic-partnership-programs.pdf

Suspicious Activity Reporting Tool – The DHS HSIN-CI Suspicious Activity Reporting Tool allows non-uniformed law enforcement private-sector members to submit formalized suspicious activity reports and facilitate efficient information sharing and responsiveness. https://www.dhs.gov/suspicious-activity-reporting-tool

Crosscutting Issues

Business Continuity Planning Suite – This DHS suite is designed to be user-friendly and scalable for optimal organizational use to reduce the potential impact of a disruption to business. The suite includes business continuity planning training, business continuity and disaster recovery plan generators, and a business continuity plan validation. http://www.ready.gov/business-continuity-planning-suite

Critical Infrastructure Learning Series – Critical infrastructure experts conduct one-hour, web-based seminars on the tools, trends, issues, and best practices for infrastructure security and resilience. https://www.dhs.gov/critical-infrastructure-learning-series

FBI InfraGard – InfraGard is a partnership between the FBI and members of the private sector. The InfraGard program provides a vehicle for seamless public–private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure. https://www.infragard.org/

Overseas Security Advisory Council (OSAC) – OSAC promotes security cooperation between American private-sector interests worldwide and the U.S. Department of State. OSAC's information exchange website offers the latest in safety and security-related information, public announcements, warden messages, travel advisories, significant anniversary dates, terrorist group profiles, country crime and safety reports, special topic reports, foreign press reports, and much more. https://www.osac.gov/Pages/Home.aspx