CISA
CYBER+INFRASTRUCTURE

Chemical Sector Landscape

AUGUST 2019

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Contents

Executive Summary

The Chemical Sector is an integral component of the U.S. economy that manufactures, stores, uses, and transports potentially dangerous chemicals upon which a wide range of other critical infrastructure sectors rely. Securing these chemicals against a growing and evolving risk landscape requires vigilance from both the private and public sectors. A number of factors may affect the critical infrastructure security and resilience posture of the chemical industry and its stakeholders. 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, Chemical 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 Chemical Sector security and resilience risk management planning consideration.

Natural Hazards: Adverse events caused by Earth's natural processes, such as floods, tropical cyclones (e.g., hurricanes and typhoons), wildfires, tornadoes, earthquakes, and tsunamis. Natural hazards have the potential to cause substantial loss of life, property damage, and economic damage (through direct disruption or destruction of facilities, operations, or the infrastructure on which they depend). For the Chemical Sector, natural hazards can threaten conditions for the safe manufacture, handling, and storage of materials by disrupting operations, communications, and power systems, inflicting physical damage to infrastructure, displacing the workforce, and limiting the transportation of products. Extreme natural hazards can create dangerous conditions involving hazardous materials that under normal conditions the sector handles with mitigated risk.

Cybersecurity: Information technology (IT) intrusion attacks by sophisticated cyber threat actors. Intrusion attacks can be sponsored by nation-states or independent cyber actors focused on the disruption of U.S. critical infrastructure with an intent to exploit vulnerabilities via the theft of sensitive information and disruption and destruction of essential services. Cyberattacks may also be inadvertently caused by unwitting employees, contractors, or vendors. For the Chemical Sector, major cybersecurity issues include impacts to both IT and operational technology (OT) systems and operations due to targeted or opportunistic attacks (e.g., advanced persistent threat, distributed denial of service, or malware and ransomware), disruptions of cloud-based services, or the manipulation of industrial control systems (ICSs). The combination of reliance on ICSs for chemical manufacturing process control with the potential for run-away reactions without proper controls and the secondary risks associated with accidental release of hazardous materials makes cybersecurity an indispensable part of operational safety and security. Increased connectivity and disruptive digital technology can expand the potential attack surface.

Supply Chain Security and Resilience: Dependence on both domestic and global supply chains to deliver raw materials, chemical feedstocks, process components, final products, and IT/OT equipment. Though the market-driven chemical industry is resilient to smaller supply chain disruptions, sector organizations are susceptible to larger incidents from counterfeit or inadequate components or feedstocks. For the Chemical Sector, major supply chain security and resilience issues include the challenges of lean processes and just-in-time practices, cybersecurity risks along the supply chain, and global transportation industry trends conflicting with chemical industry growth.

Criminal Activities and Terrorism: 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, firearms, and vehicular attacks. These attacks can have catastrophic impacts on lives, facilities, and operations. Predominant issues regarding criminal activities and terrorism for the Chemical Sector include armed attacks at facilities, theft of high-value or potentially dangerous products (e.g., hazardous material, explosive precursor chemicals, and precursor materials used for the production of crude chemical or biological attack agents), the threat of malicious insiders, and suspicious activities (e.g., photography) at facilities and operations. Theft from sector facilities and suspicious activity may be indicators of preparation for future attacks (with explosives, toxins, or poisons) on the Chemical Sector, other sectors, or the public.

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 Chemical Sector, crosscutting security and resilience issues include aging transportation infrastructure; dependencies on other critical infrastructure sectors; incidents involving chemical transport, storage, production, and research; opioid production, transport, and security; 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 Chemical Sector. Government stakeholders and industry partners may use this document to help identify and address 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 Chemical 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 Chemical Sector changes, this document may be updated.

Natural Hazards

Natural hazards include major adverse events caused by Earth's natural processes, including floods, tropical cyclones (e.g., hurricanes and typhoons), 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 and the infrastructure on which they depend. The severity of a natural disaster is measured in terms of lives lost, property damage, economic disruption, the costs associated with restoration, and the affected population's ability to rebuild.

Major security and resilience issues for the Chemical Sector regarding natural hazards include earthquakes in the Pacific Northwest and central states; flooding along the Gulf Coast and in northern central states; tropical cyclones along the Atlantic Coast and Gulf Coast; and disruptions in surface, rail, barge, and pipeline transportation that could result from any natural hazard in any location. Recognizing and addressing these risks 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 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.[1] Figure 1 provides a map of these events. Such large-scale events have cascading impacts across sectors and regions, with the potential to cause drastic disruptions to Chemical Sector facilities and companies (e.g., long-term physical damage, disruption of access, power and fuel loss, and feedstock and supply chain disruption).

Figure 1. *2017 U.S. Billion-Dollar-Loss Natural Disaster Events*
Source: National Oceanic and Atmospheric Administration (NOAA)

- **Long-Term Physical Damage:** Physical damage to Chemical Sector facilities from such large natural hazards can be catastrophic, with recovery times extending for months or years. Long-term disruption of chemical facility operations affects the safety, security, and resilience of the facility and the surrounding communities.
- **Disruption of Access:** Major natural hazards typically will cut off or drastically restrict access to Chemical Sector facilities affected by the event. This hinders response and recovery efforts and can lead to secondary disasters (depending on the facility) as 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 the potential for cascading failures from energy disruptions are of great concern to the Chemical Sector.
- **Feedstock and Supply Chain Disruption:** Feedstock is the raw material required to supply industrial processes. Limited access and the disruption of critical transportation modes (e.g., maritime, road, rail, and pipeline) to Chemical Sector facilities from natural hazards can result in the loss of feedstocks needed for chemical manufacturing or the dispatching of product to clients. Whether a direct halting of the flow of feedstock or a lack of personnel or systems to control its influx, feedstock loss and associated supply chain breaks can cause significant local disruptions.

Earthquakes

Major earthquakes are a significant threat to the Chemical Sector. A strong earthquake in the Cascadia seismic zone in the Pacific Northwest or the New Madrid seismic zone in the Central United States has the potential to cause significant chemical industry disruptions.

- **Cascadia Seismic Zone:** A 9.0-magnitude earthquake in the Cascadia seismic zone would severely damage a significant number of petrochemical pump stations along the Olympic and Oregon Line, a refined-product pipeline system, as well as a substantial number of refined-product terminals in the region. The resulting inability to store and distribute fuels locally is likely to have a major effect on regional fuel supplies. The challenge to mitigate disruptions in shipping fuel and petrochemicals (by surface, rail, and barge transportation) in the region could be further complicated by tsunami flooding at the mouth of the Columbia River.[2]
- **New Madrid Seismic Zone:** A 7.0-magnitude 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, Energy, and Transportation Systems Sectors along the Mississippi River. Total estimated economic loss for such an event could reach several hundred billion dollars.[3]

Flooding

Increased likelihood of flooding along the Gulf Coast and in the North Central United States increases risk to chemical facilities in those regions. Facilities built within 100- to 500-year floodplain areas per U.S. Federal Emergency Management Agency mapping may be more at risk than previously estimated. In recent years, flooding from extreme rainfall events has increased, including several occurrences of 100- and 500-year floods. This trend is projected to continue, increasing the flood risk in many parts of the Nation.[4] Past major events (e.g., Hurricane Harvey and the 2011 and 2015 flooding events along the Mississippi and Red Rivers) have threatened Chemical Sector operations at locations along the Gulf Coast and major rivers of the Central United States. The primary concern with disruption of chemical facilities due to a flood event is the interruption of the supply chain of key chemicals. Refineries and chemical plants that depend upon barge

deliveries as their primary resupply mechanism will likely suffer a greater impact than facilities that rely on pipelines and railroads for the transportation of goods. Flooding could also potentially damage production facilities and storage tanks.

- **Equipment Floatation:** Some equipment can suffer damage or failure due to floatation upon flood impact. Floating storage tanks can tear pipe or tubing connections and lead to releases of hazardous materials.
- **Electrical Damage:** Flooding of electrical equipment can lead to short-circuiting and power blackouts, which could result in the failure of cooling units, pumps, and electrically operated safety systems.
- **Flood Path Debris:** Floating debris dragged along with the floodwaters poses a threat to equipment and can lead to the release of hazardous substances.
- **Hazmat:** Some hazardous materials released by flood impact can react with the floodwaters to generate toxic or flammable vapors, 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.

Transportation Disruptions

Any natural hazard can lead to significant Chemical Sector impacts from disruptions in transportation systems. Chemical Sector products and facilities rely on the secure flow of surface, rail, barge, and pipeline transportation. Natural hazards that compromise these modes can have significant impacts on Chemical Sector operations as well as cascading impacts on other interdependent sectors.

- **Surface:** Over half of domestic chemical industry shipments are conveyed with trucks on highways and roads. When natural hazards affect surface transportation in areas critical to Chemical Sector supply chains, major delays and losses can occur.
- **Rail:** Trains ship bulk volumes of chemical products in shipping containers, usually on a path toward exportation sites. During normal conditions, railways often become clogged in metropolitan areas. If a natural hazard disrupts rail service, these delays can become debilitating to Chemical Sector companies relying on bulk transportation, as delivery times cannot be guaranteed or readily estimated.
- **Barge:** Although comparatively not as significant as truck and rail transportation overall, shipping via barge and canal is important to Chemical Sector facilities located along major rivers of the United States. Flooding and drought from natural hazards can severely hinder inland waterway transportation and contribute to Chemical Sector losses.
- **Pipeline:** Chemical products (especially organics and petrochemicals) and feedstocks (e.g., natural gas, ethylene, and naphtha) are safely and effectively transported through pipelines. Incidents such as wildfires, tropical cyclones, tornadoes, earthquakes, and floods can shut down or destroy critical pipelines, disrupting Chemical Sector operations and potentially causing secondary disasters.

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 above in Figure 1, three major hurricanes affected the United States in 2017—the first time since 2005 that three major hurricanes made landfall in a single year. These storms caused losses in excess of $206 billion.[5] Other historical hurricane events such as Katrina, Rita, Ike, Sandy, and Matthew have also shown how devastating these

events can be to all critical infrastructure sectors. The Chemical Sector may be more susceptible to disruptions in the regions along the East and Gulf Coasts where tropical cyclones tend to strike.

- **Tropical Cyclone Preparedness:** Chemical 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 conducting 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 Maria, Harvey, Rita, and Katrina have demonstrated, the impact of tropical cyclones can go well beyond the potential threat to employees and physical damage to facilities and their communities. While most 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 (necessary to manufacture chemicals), and inert gases (necessary to purge pipelines and valves), while damaged roads and rail lines prevented the delivery of products to consumers. Ultimately, this led to higher natural gas costs and curtailed the delivery of chemicals essential to producing important everyday items such as clean drinking water and life-saving medicines.

Case Study: Hurricane Harvey Impact at a Chemical Facility

In August 2017, Hurricane Harvey brought unprecedented levels of rainfall to Texas. The hurricane floodwaters shut down the power system and backup generators of a Texas chemical manufacturing facility, disabling its refrigeration system. The result was thermal runaway of temperature-sensitive chemicals, leading to fires and explosions that released gases and smoke into the local community. All of the facility's employees were evacuated, as were more than 200 residents who lived within a 1.5-mile radius of the facility, and 21 people sought medical attention from reported exposure to noxious fumes.

The U.S. Chemical Safety Board (CSB) investigated the event and found that the facility had established—and followed—policies and safeguards for hurricanes. Workers moved the sensitive chemicals from low-temperature warehouses, where the chemicals were normally stored, to refrigerated trailers used for shipping. Several of the trailers were relocated to a high-elevation area to keep them from the floodwaters' reach, but three could not be moved. When the rising waters caused the refrigeration to fail, the chemicals inside caught fire.

While the facility did prepare, the plans did not account for Harvey's level of severity. In its investigative report, the CSB called for more robust industry guidance to help hazardous chemical facilities better prepare for extreme weather events. Recommendations included conducting analyses to determine susceptibility to extreme natural events, evaluating the adequacy of safeguards, applying a conservative risk management approach, and ensuring that critical safeguards and equipment are not susceptible to failure by a common cause. In the announcement of the final report, the CSB chairperson said, "Considering that extreme weather events are likely to increase in number and severity, the chemical industry must be prepared for worst case scenarios at their facilities."

Cybersecurity

The Chemical Sector is subject to a wide range of risks stemming from cyber threats and hazards. Sophisticated cyber 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, there is increased risk for wide-scale or high-consequence events.

Issues that present higher cybersecurity risk for the Chemical Sector include advanced persistent threat (APT) attacks, cloud-based services, distributed denial of service (DDoS) attacks, industrial control systems (ICSs), increased connectivity and disruptive digital 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 groups pose significant risk to the Chemical 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 facility'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 facility. APTs therefore take advantage of opportunities at multiple stages to gather information and develop and validate their attacks.

VPNFilter, Dragonfly, and Hatman are three recent notable examples of malware that, because of their sophistication, appear to have 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.[6]
- **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 equipment safely.

In 2017, a petrochemical facility in Saudi Arabia was attacked using Hatman. The sophisticated attack was intended to sabotage the facility's operations such that safety controls would fail, triggering an explosion. Though the attack was unsuccessful in causing an explosion or hazmat release (owing to an error in the code), the incident demonstrated how similar cyberattacks may be used to cause physical destruction of critical infrastructure.

Cloud Services

Chemical Sector companies are increasingly incorporating cloud services into their business operations. Many companies are adopting cloud software-as-a-service (SaaS) to enhance business functions in the areas of IT, human resources, marketing, and supply chain. Advanced cloud services offer benefits such as scalability, high availability, advanced data analysis and storage, and decreased ownership cost. However, these benefits may come with new cybersecurity issues. In addition to presenting many of the same cybersecurity issues as physical IT (e.g., denial of service, APT, stolen credentials, and phishing), cloud services exhibit virtual susceptibility to attacks, including hyperjacking, escalation, and virtual machine escape.

- **Hyperjacking:** The hypervisor (software that manages virtual machines on a physical system) is compromised, providing a cyber threat actor with control of those underlying virtual machines.
- **Escalation:** A cyber threat actor breaks out of the virtual environment to gain elevated access to resources that are normally protected from the user.
- **Virtual Machine Escape:** The cyber threat actor escapes a virtual machine (a virtual system or application that is running inside a physical system) and interacts directly with the virtual machine's hosting environment.

Distributed Denial of Service Attacks

DDoS attacks are a growing threat. The strategy uses many Internet-connected devices in combined denial-of-service attacks, generating immense bandwidth loads to the point of disruption or creating openings for malware to be deployed. Recent high-profile examples include the September 2016 attack of a French web-hosting company and the October 2016 attack against a major domain name system (DNS) service provider.

- **Web-Hosting Provider Attack:** In September 2016, one of the largest DDoS attacks ever to occur was carried out on a French web-hosting provider. The attack activated over 150,000 "Mirai" malware-infected Internet-connected security cameras. The devices simultaneously consumed over one terabit per second (Tbps) of network throughput (also referred to as bandwidth) and crippled providers' and their clients' websites. Using vendor and manufacturer default passwords for Telnet access compromised the security cameras.[7]
- **DNS Attack:** In October 2016, another Mirai malware DDoS attack was carried out on a major DNS service provider. The attack flooded 1.2 Tbps of Internet traffic (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 the September 2016 attack, the DNS attack employed compromised Internet-connected security cameras.[8]

Common security devices that use high-bandwidth connections, such as security cameras and digital video recorders, may be vulnerable to manipulation for DDoS attacks. In addition, as the Chemical Sector introduces more Internet-connected devices into its processes (see Internet of Things summary below), the risk of DDoS attacks increases.

Increased Connectivity and Disruptive Digital Technology

Chemical Sector companies are adopting physical–cyber business models and practices to streamline operations and promote growth in the chemical industry. Over the next 5 years, chemical companies are expected to invest 5 percent of annual revenue in digital operations, including the digitization of existing products and services, as well as developing new digital services or employing data analytics and automation in processes and services.[9] Combining physical and digital technologies introduces new cybersecurity issues, including increased points of access through which malicious code could be introduced or data could be stolen, and cascading failures 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.
- **Cascading Failures:** Automated systems that are dependent on interconnected devices may be vulnerable 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 processes within Chemical Sector facilities. As the Chemical 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 ICS across all sectors has steadily increased since 2010.[10] Common high-risk ICS cyber issues include buffer overflows, use of hard-coded credentials, and cross-site scripting.

- **Buffer Overflows:** Software programming errors can cause data-writing buffers to extend beyond their boundaries and overwrite adjacent memory blocks. This can corrupt data, crash software, or allow for the execution of malicious code. Vulnerable ICS components 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.
- **Hard-Coded Credentials:** Static passwords and access keys in ICS components can allow a cyber threat actor to bypass authentication configurations and requirements, gaining malicious control of HMIs, PLCs, or other networked ICS devices. Such 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.

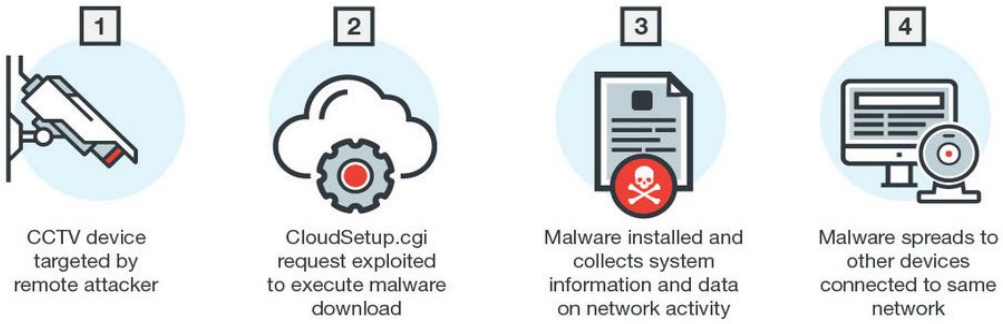
Internet of Things

A system of interrelated computing devices with unique identifiers and the ability to transfer data over a network without operator interaction is commonly referred to as IoT. Internet-connected devices are becoming more generally used in the Chemical Sector for manufacturing, processing, conveying, and assessing chemical products. IoT sensors and analyzers are used to 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) is used to optimize supply chains and reduce operating costs.

The rapid increase in IoT use in the sector, as well as all over the world, leads to increasing cybersecurity concerns regarding opportunities for sector devices to be attacked, use of unrelated consumer-level devices against sector infrastructure, and business operations susceptibility to DDoS attacks.

- **Multitude of Devices:** Increasing the number of IoT devices in Chemical Sector operations increases the number of ways sector organizations can be attacked. Wireless communication between IoT devices in chemical facilities often transmits proprietary or confidential information on products or business operations. This information could be stolen or infected with malware—whether remotely, internally through an insider, or in proximity to the facility. Figure 2 provides an example of IoT malware delivery.
- **Chemical Operations as a Target:** Cyber threat actors seeking to harm or exploit Chemical Sector organizations may employ many external IoT devices in coordinated attacks for economic espionage, disruption of operations, or destruction of property.
- **DDoS Attacks:** As described above, IoT devices can be exploited via malware manipulation to carry out DDoS attacks. The malware saps network bandwidth and can compromise the performance of the infected devices.

Figure 2. *Example Infection Pathway of IoT Malware*
Source: Trend Micro



Malware and Ransomware

Malware and ransomware are common attacks on all business IT networks and can infect Chemical Sector organizations as well. Malware (a term derived from "malicious software") is the mechanism by which cyberattacks are carried out. The variety of malware affecting IT continuously expands. In 2017, a major cybersecurity provider discovered nearly 670 million new variations of malware.[11] Malware may be introduced in IT systems and networks deliberately by a cyber threat actor, or inadvertently introduced by sector employees, contractors, or vendors. Ransomware attacks are on the rise across all sectors, and business systems are at increased risk of attack. 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 attacker requests a ransom in exchange for decrypting the data and returning functionality. 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.[12] 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.[13] Major examples of large-scale ransomware attacks include the May 2017 "WannaCry" attack and the April 2016 attack of a U.S. utility company.

- **Phishing:** One of the most common mechanisms by which malware is delivered to IT systems and networks is phishing, which is a type of social engineering (i.e., manipulating interpersonal relationships). Phishing refers to malicious emails designed to trick the recipient into opening a

malicious attachment, visiting a malicious website, or sharing sensitive information (e.g., passwords, account numbers, or personal information). Spear phishing is a more targeted form of phishing intended to inflict malware on or solicit confidential or sensitive information from a specific person or organization. The number of phishing emails and compromised vendor email accounts targeting multiple utility industries has increased in the recent past. In 2017, spear phishing was the most often employed attack vector in targeted cyberattacks.[14]

- **WannaCry:** Organizations all over the world discovered their systems were encrypted by the WannaCry ransomware in May 2017. WannaCry exploited security vulnerabilities released in leaked National Security Agency documents and spread by infecting Windows computer systems not patched to eliminate the security vulnerability. 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.
- **Business Network Threat to Control Systems:** Malware and ransomware attacks commonly target business networks, but for industries that rely on ICSs, such as in the Chemical Sector, control systems may be threatened as well. 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.

Case Study: Attack on Water Utility Chemical Controls

In March of 2016, hackers infiltrated the control system at a water utility to alter the levels of chemicals used to treat tap water. The "hacktivists" compromised the company's computers by exploiting unpatched web vulnerabilities found in its Internet-facing customer payment portal. The incident—which involved SQL injection and phishing—exposed aging AS/400 operational control systems that managed controls regulating valves and ducts that regulate the water flow and chemicals to treat the water. Using credentials found on the payment application, the actors interfaced directly with the water district's valve and flow control application. Four separate connections over a 60-day period were found, and in two instances, the attackers changed the chemical levels, handicapping water treatment and production capabilities so that recovery time for replenishing water supplies increased.

An IT security service vendor discovered the attack after the company requested investigation into unauthorized access to its operational systems and unusual patterns of valve and duct movements. The vendor's risk analysis team found evidence that the hacktivists had twice manipulated the valves controlling chemical flows. Although the vendor found that many critical IT and operational technology functions ran on a single AS/400 system, the actors seemingly lacked the knowledge of SCADA systems or the intent to do any harm.

Luckily, the water company was able to reverse the changes before utility customers were affected by the hackers' tampering with water treatment systems. However, the hack resulted in the exposure of personal information of the utility's 2.5 million customers (fortunately, there is no evidence to date that this information has been monetized or used to commit fraud). The successful hack identifies a clear need to invest in intrusion detection, prevention, patch management, and analytics-driven security measures. The IT security vendor's risk team provided a report with actionable intelligence—the type of insights organizations need to leverage to better detect, prevent, and respond to advanced attacks. In addition, training on identifying and reporting phishing scams can serve as the first line of defense against cyber-based threats.

Supply Chain Security and Resilience

The Chemical Sector relies heavily on complex, effective global and domestic supply chains to deliver raw materials, chemical feedstocks, process components, and final products. Important supply chain security and resilience issues for Chemical Sector organizations include the challenges of lean processes and just-in-time (JIT) practices, cybersecurity risks along the supply chain, and global transportation industry trends conflicting with chemical industry growth.

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 in the Chemical Sector. 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:** Many industries have adopted JIT inventory methods as a highly efficient, competitive approach—qualities progressively necessary in increasingly fast-paced markets. The JIT approach makes companies highly reliant on the suppliers that provide the multitude of inventory when needed—not earlier, not later. Deviations in highly synchronized JIT supply chains can present production challenges. For example, unexpected increases in orders can cause backups or rushes in production, compromising smooth workflows, quality assurance, and safety.
- **Global Supply Chains:** The global chemical industry supply chain is a recent and evolving phenomenon, making it challenging for industry to control. The supply chain involves many moving and disparate parts that are difficult to predict and monitor, and a disruption to any one of them entails 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 modern virtual technologies are under threat from cyberattack. The Chemical Sector can absorb small supply chain disruptions by market forces driving producers and vendors to fill in where disruptions occur. However, sector organizations are at risk of disruption from compromised, counterfeit, or sub-standard chemical products, feedstocks, or IT and operations equipment and software.

Supply Chain Cybersecurity

Chemical 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 turn problematic if the contractor or vendor has been compromised. The supply chain for software itself represents another cybersecurity concern, as compromised software introduced along the supply chain could be used to attack Chemical Sector networks. Sophisticated threat actors exploit vulnerabilities deep in the IT supply chain as a foothold from which they can gain access to sensitive and proprietary information further along the chain. In addition, cyber threats to the supply chain are interconnected with physical security.

- **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.

- **Software Supply Chain:** In 2017, software supply chain attacks increased dramatically across all sectors.[15] By attacking software providers, attackers replace legitimate business software with maliciously modified versions, unbeknownst to end users. For example, Chemical 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. For example, compromised software used in an ICS could cause ICS network vulnerability or instability and lead to failure of physical operations of the ICS. The converse is also true: physical security supply chain impacts can affect cybersecurity. Counterfeit hardware introduced into physical control systems—such as electronic door locks, security cameras, or UASs—could render a facility vulnerable to specific cyberattacks.

Transportation Industry Trends

Recent increased production and growth in the Chemical Sector poses challenges to the sector when coupled with changes in the maritime, rail, and motor carrier transportation industries. The chemical industry experienced growth in 2017 and 2018 and anticipates its continuation. An inability of transportation systems to keep pace with this growth could lead to excess inventories due to transportation delays, increased capital expenditures in infrastructure to address congestion and delays, and increased operating costs due to logistical inefficiencies. As changing transportation market pressures incentivize global and domestic transportation companies to consolidate and/or lead to their failure, Chemical Sector operations may be disrupted.

- **Driving Growth:** Expansion in the chemical industry in the United States has been fueled by relatively low feedstock and energy costs in recent years. This is largely due to the low cost of abundant natural gas for use as a chemical manufacturing base and a source of energy. Unites States-based chemical manufacturers are therefore slated to use this globally competitive advantage to drive investment in new projects and objectives (including creating over 400,000 new jobs and generating over $300 billion in economic output by 2025).[16]
- **Transportation Limitations:** Although rapid growth in the industry is expected to continue, limitations in transportation logistics will restrain growth to less than its potential. Transportation systems may be unable to match the pace of industry growth because of shortages in skilled and certified truck drivers, inadequate capacity and capability of Gulf Coast ports to address increasing growth volumes, and delays from rail congestion.
- **Increased Costs:** As transportation systems become more challenged to meet the chemical industry's growing demands, operating costs may increase. Transportation delays may necessitate that companies hold excess inventory, capital expenditures may be needed to respond to congestion and delays, and unreliable schedules may engender logistical inefficiencies.
- **Trucking Consolidations:** Mergers and consolidation in the trucking industry have been occurring at a rapid rate in the past few years. 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.[17] Such large-scale consolidation can decrease competition and lead to many smaller companies failing. This volatility can cause unforeseen disruptions in the Chemical Sector.
- **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.[18] Major changes in container shipping such as this can affect the supply and value chains of the Chemical Sector by slowing production, increasing operating costs, and reducing product value.

Case Study: Hurricane Maria's Disruption of the Medical Products Supply Chain

In September 2017, Hurricane Maria made landfall on the island of Puerto Rico, causing over a billion dollars in damage and leading to the deaths of thousands of American citizens throughout late 2017 and early 2018. In addition to the human toll and economic impact, the hurricane also affected the pharmaceutical and medical products manufacturing industry. Ten percent of United States pharmaceutical product manufacturing is based in Puerto Rico. Maria severely disrupted the supply chain for both the manufacture and delivery of pharmaceuticals and medical products throughout the United States. This disturbance led to critical shortages of pharmaceutical and other health products (e.g., saline, intravenous bags, and medical gases) during a nationwide outbreak of a particularly strong strain of influenza in late 2017. The disruptions highlighted several other vulnerabilities in the U.S. supply chain for pharmaceuticals and medical products in the months following this natural disaster.

The U.S. Food and Drug Administration (FDA) reported in November 2017 that it was monitoring 90 medical products for potential hurricane-related shortages. Interviews with supply chain officials at affected pharmaceutical companies indicated that most factories were able to restart at least some operations quickly after the storm. However, officials at all companies noted that damage to roads and the fuel supply made it difficult for employees to travel to work. Damage to sea and airports also reportedly made it difficult to transport needed goods on and off the island, delaying the recovery. The FDA commissioner noted in an October 2017 interview that many pharmaceutical companies on the island were "manufacturing well short of [full capacity]" after the storm.

In 2018, The U.S. Department of Homeland Security's Public-Private Analytic Exchange Program (AEP) conducted a study to identify recommendations for protecting the pharmaceutical supply chain as a component of critical infrastructure vital to U.S. national security interests. The recommendations were developed to mitigate future supply chain disruption by increasing private-sector and government coordination. To continue the AEP's efforts, public- and private-sector organizations are collaborating on providing incentives for greater cooperation, prioritizing the U.S. pharmaceutical industry as a unique critical infrastructure component and national security asset, creating an industry-wide list of medications deemed "critical," and streamlining the approval process for backup medications and alternative sources of temporary production.

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, firearms, and explosive attacks.

In the Chemical Sector, security and resilience issues regarding criminal activities and terrorism include armed attacks at facilities (with weapons or vehicles), theft of hazardous material, theft or use of explosive precursor chemicals (chemical substances that can be misused to manufacture homemade explosives), theft or use of precursor materials used for the production of crude chemical or biological attack agents, the threat of malicious insiders, and suspicious activity at facilities and operations (oil and petrochemical refineries in particular). Recognizing and mitigating these risks could help to limit the financial, operational, and human impacts of deliberate attacks and terrorism.

Armed Attacks

Armed assailants' deliberate attacks on Chemical Sector assets and personnel could include active shooter incidents (attacks with firearms), attacks with improvised explosive devices (IEDs), or vehicle attacks. Injury and loss of life are the obvious impacts of such attacks. An armed attack could destroy critical facility assets and cause explosions and release of hazardous materials (hazmat), threatening the safety of nearby communities and the environment. Hazmat may also be targeted for malicious release directly from a facility. Armed attacks can also affect Chemical Sector facility operations through the loss of employee hours and downtime from compromised equipment or facilities.

- **Active Shooter Incidents:** 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).[19]
- **Vehicle Attacks:** Passenger cars, cargo vans, box trucks, or semi-trailers could be loaded with explosive devices and used in attacks on Chemical Sector facilities. Vehicles could be used to breach security perimeters and provide a means for conducting an armed attack; ramming facility assets could cause hazmat release.
- **Incident Timing:** Armed attacks are dynamic and quickly evolve. Often, the immediate deployment of law enforcement is required to stop an attacker's aggressive action and mitigate harm to potential victims. However, because such situations are also frequently over prior to the arrival of law enforcement, Chemical Sector organizations must be prepared both mentally and physically to address an active shooter situation prior to law enforcement arrival.
- **Operational Impacts:** Facilities and equipment may be damaged from firearms or explosions 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.

Chemical Theft and Diversion

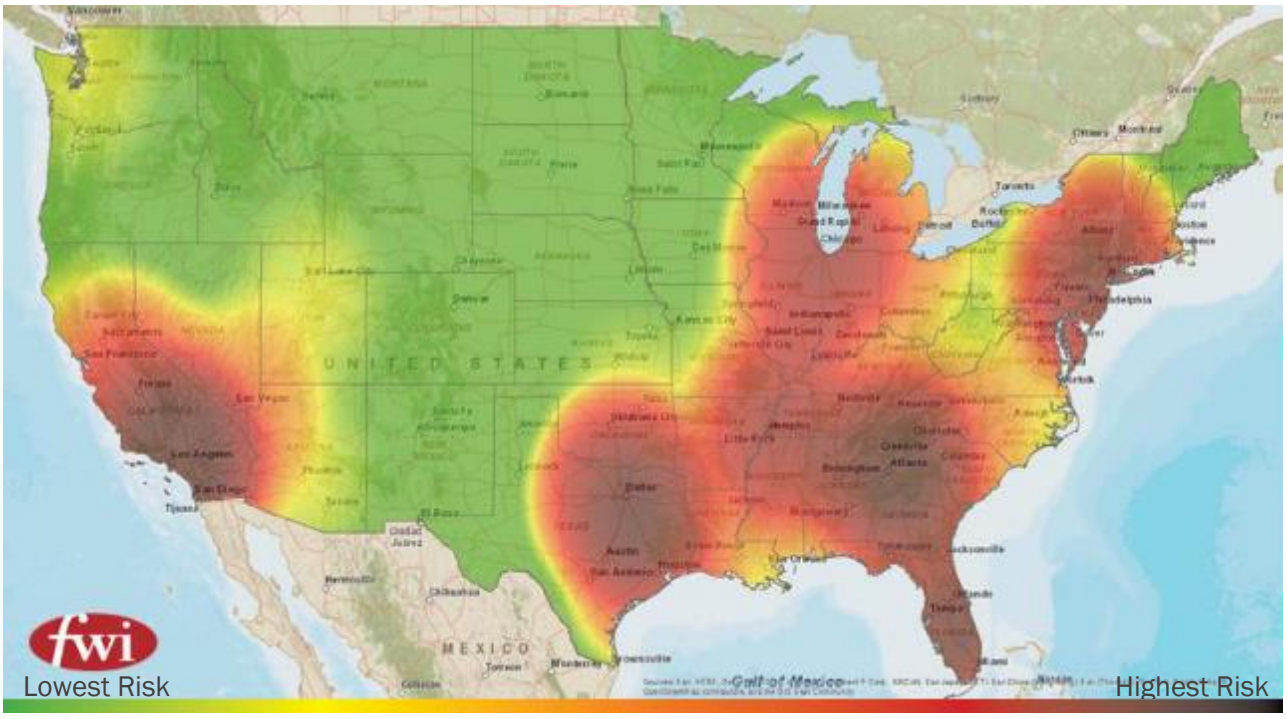
Malicious actors continue to target hazmat for theft or diversion to obtain materials for use with criminal intent or in chemical dispersal devices and explosives. Theft and diversion may occur at sector facilities where hazmat is used or outside of facilities as materials are transported or delivered. This external theft

and diversion may occur by obtaining hazmat transportation credentials, stealing vehicles and cargo during transport, and exploiting cyber vulnerabilities within transportation networks.

- **Prevalence:** In 2015, over 750 cargo thefts took place in the United States (according to a supply chain security firm). Of those cargo thefts, nearly 90 percent occurred while the trailers and containers were stationary and unattended in unsecured parking areas including truck stops, public parking lots, carrier lots, and drop lots.[20] Figure 3 provides a map of cargo theft risk in the Nation.
- **Targets:** Factors frequently used in targeting a victim include high-value and high-target load (usually identified by a $250,000 insurance requirement), cross-country transport during a weekend (Wednesday through Friday pickup and Monday or Tuesday delivery), out-of-state actors, load applications applied for within 15 to 20 minutes of posting, and team drivers.[21]
- **Methods:** Most commonly identified theft methods include use of Internet load message boards to obtain sensitive information, insider information and collusion, and cyberattacks on transportation IT systems.

Hazmat theft presents a substantial risk for chemical manufacturers and the supply chains that are responsible for delivering these materials to end users or processing facilities. Chemical Sector organizations can mitigate vulnerabilities and increase awareness of hazmat theft through background checks, credential verification, surveillance and intrusion detection systems, tracking devices, security training, and information sharing.

Figure 3. *Highway Motor Carrier Cargo Theft in the United States*
Source: Freight Watch International



Crude Chemical or Biological Attack Agents

Violent extremists 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). Chemical Sector facilities that use or produce these chemical or biological agents may be targeted for theft, diversion, sabotage, or exploitation.

- **Common Targets:** Known precursors used for the production of crude chemical or biological attack agents include commonly available chemicals, industrial toxins, and toxic plants or gases. Specific toxins and chemicals for which terrorist or violent extremist publications have shown interest include botulinum toxin (a powerful neurotoxin), ricin (a deadly toxin produced from castor beans), and hydrogen sulfide (a toxic gas used in chemical refining and processing, food processing, and leather tanning).
- **Suspicious Activities:** Actions that may indicate plots to use a crude chemical or biological weapon include purchases (or attempted purchases) of controlled chemical substances, large purchases of toxic compounds or plants, chemical odors in residential areas, or increases in thefts of toxic or similar chemicals in a small area or short period of time.

Explosive Precursor Chemicals

Interest in precursor ingredients of explosives is a potential indicator of deliberate criminal activities or terrorism. As with crude chemical or biological attack agents described above, violent extremist publications often describe processes and components for manufacturing explosives. The chemical precursors of such explosives in Chemical Sector facilities may be targeted for theft, diversion, or exploitation.

- **Triacetone Triperoxide (TATP):** TATP is a highly explosive chemical that is used in industrial organic chemistry reactions and the production of resins and composites. It also is a byproduct of certain industrial organic chemistry syntheses. TATP has been used in recent high-profile terrorist attacks in France, Belgium, and Turkey. Chemical Sector facilities that use or produce TATP or similar explosive precursors may be targeted for nefarious activities.
- **Indicators of Chemical Explosives Manufacturing:** In addition to securing specific chemicals that may be targeted for illicit explosive manufacturing, Chemical Sector facility owners and operators should maintain situational awareness of potential indicators of explosive manufacturing. For facilities that use or produce known explosive precursors, awareness of the following suspicious activities or characteristics in the surrounding community supports chemical security.
  - **Odors:** Foul odors or caustic fumes coming from a room or building or emanating from sewers and drains
  - **Building Damage:** Damage to ceilings and walls, such as corrosion of metal surfaces, structural damage, or paint discoloration from harsh chemical fumes
  - **Large-Scale Ventilation:** Presence of large industrial fans or multiple fans in windows for no apparent purpose
  - **Consumer Chemical Refuse:** Presence of large numbers of discarded containers for hydrogen peroxide, acetone, nail polish remover, or paint remover
  - **Chemical Storage:** Presence of metal or plastic drums for storing precursor chemicals or final explosive products
  - **Conspicuous Equipment:** Presence of laboratory equipment, glassware, ice baths, thermometers, coffee filters, gloves, or protective eyewear (often similar or identical to illicit narcotics laboratory equipment)
  - **Chemical Injuries:** Injuries consistent with experimentation with explosives and chemicals, such as missing fingers or scarring, skin and hair discoloration, or burns on skin without a reasonable explanation

Insider Threats

The insider threat can be described as an insider using his or her authorized access, wittingly or unwittingly, in a way that harms the organization's resources, personnel, facilities, information, equipment, networks, or

systems. Insiders may be current or former employees, contractors, or business associates who have gained inside information concerning the organization's security practices, data, and computer systems. Insiders pose a substantial threat to Chemical Sector organizations because they have knowledge of and access to proprietary systems that allow attackers to bypass security measures through legitimate means. Insiders may sabotage facility processes, intentionally release hazmat from the facility, or conduct cyberattacks within the organization's IT systems and networks. Important insider threat considerations for Chemical Sector organizations include identifying behavioral indicators of potential insider malicious acts, implementing insider threat mitigation best practices, vetting personnel thoroughly before hiring, and recognizing, monitoring, and reporting on suspicious activities.

- **Behavioral Indicators:** Conduct 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 (see Behavioral Indicators above), developing clear reporting and investigating mechanisms, and training employees in recognition and reporting. In the absence of an existing program, Chemical Sector organizations should consider developing an insider threat program (appropriately depending on organization mission and available time and resources) to officially document and implement insider threat mitigation strategies. At a minimum, demonstrating to employees that the organization is eager to help them through difficult times will likely eliminate potential insider threat incidents and prevent loss.
- **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 background checks, risk-based analysis of positions, and training for employees conducting hiring activities. Personnel conducting interviews and background checks should be trained to recognize, identify, and document suspicious or concerning details or behaviors of potential employees or contractors. Calling attention to indicators of potential for malicious insider actions during the hiring process can prevent insider attacks from occurring.
- **Personnel Surety:** Chemical Facility Anti-Terrorism Standards (CFATS)-covered facilities must comply with Risk-Based Performance Standard (RBPS) 12 – Personnel Surety by establishing a program to ensure facility personnel and unescorted visitors with access to restricted areas have undergone background checks regarding identity, legal authority to work, criminal history, and, where applicable, screening for ties to terrorism.
- **Suspicious Activity:** Suspicious activities that may indicate an insider threat include collecting excessive information or data (beyond the need entailed by the individual's job duties), frequent unexplained travel, contact with competitors (unrelated to job duties), demonstrating undue interest in areas that are outside their job duties, or working uncommon hours without approval.

Suspicious Activity

Unexplained surveillance of critical infrastructure facilities containing dangerous chemicals may be linked to plans for targeting those facilities for attacks that could cause the release or explosion of such chemicals. Recent suspicious activity reports (SARs) of unexplained photography of oil and petrochemical refineries may indicate an increased interest in attacks on Chemical Sector facilities. Several examples in 2017 include suspicious photography at oil and petrochemical refineries and storage facilities (e.g., photographing facility

structures and employee movement from parking lots and through perimeter fencing). The following examples represent recently common SARs of suspicious photography at critical infrastructure facilities.

- **Photographing Facility Structures:** An unidentified individual drove into the administrative building parking lot at a refinery. The individual parked the vehicle, exited, and began taking photographs of the refinery through the perimeter parking lot fence. The individual departed the site prior to the arrival of facility security and the local police department.
- **Photographing Employees:** Four individuals were observed taking photographs of a refinery. Two of the individuals photographed employees entering and exiting the facility. Facility security made contact with the individuals and informed them they were not authorized to be on the refinery property. The individuals remained outside the facility and continued taking photographs. Security contacted the local police department; police responded and made contact with the individuals, who refused to answer any questions.

Case Study: TATP Attacks

Improvised explosives are a common feature of several attacks in the West, including terrorism events in Paris, France; Brussels, Belgium; and Istanbul, Turkey. Commercially available precursor materials such as hydrogen peroxide, acetone, and other chemicals—such as TATP, among others—can be used to produce improvised explosive devices (IEDs). The Brussels attackers used explosive devices with 30–60 pounds of TATP; the IEDs killed 32 civilians and injured over 300 more. In Istanbul, assailants fired on travelers and Turkish law enforcement before detonating person-borne IEDs; the attack resulted in 42 deaths and over 250 wounded.

Third-party observers can play a key role in identifying indicators of chemical or biological attacks and suspicious activity. In the 2016 attacks in Brussels and Istanbul, there were reports of very strong chemical odors and noxious smells emanating from the location where explosives were being developed. Third parties noticed open windows, multiple fans, and installation of a heavy metal door to conceal the toxic fumes and suspicious activity. Individually, these are harmless acts, but considered together, they can indicate suspicious activity.

As a result of the investigations following the Brussels and Istanbul attacks, the U.S. Department of Homeland Security was able to glean critical information regarding indicators of suspicious activity and chemical or biological attacks. This has helped with developing indicators of possible TATP manufacturing, as well as production of other chemicals or explosives, hence providing opportunities to disrupt these activities. Based on findings from investigating such terrorist attacks, security personnel are urged to consider protective measures that integrate available equipment, personnel, current procedures, and information to improve threat detection.

Crosscutting Issues

The Chemical Sector is subject to several crosscutting issues that can stem from infrastructure, social, technology, and economic challenges. These include aging transportation infrastructure; dependencies and interdependencies with other sectors; industrial accidents with chemical transport, storage, production, and laboratories; opioid production, transport, and security; 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 Chemical Sector requires secure transportation to operate effectively. The American Society of Civil Engineers 2017 Infrastructure Report Card rates United States infrastructure as a whole at a grade of 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.[22]

- **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 Unites States' inland waterways system, the majority of which is older than the original 50-year design life of its components. These waterways are an important part of freight transportation, connecting ocean ports with inland transportation hubs, accounting 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

Chemical Sector facilities and processes are energy- and water-intensive. The Chemical Sector is also very reliant on the Communications, Information Technology, Financial Services, and Transportation Systems Sectors. Incidents and disruptions affecting these sectors can negatively affect the Chemical Sector. Also, Chemical Sector products are vital for assets and operations of other sectors, including Critical Manufacturing, Food and Agriculture, Healthcare and Public Health, Information Technology, and Water and Wastewater Systems. Scientific laboratory research in all sectors requires Chemical Sector products.

- **Communications:** Sophisticated communications equipment is used for sector operations and control, while critical communications components are manufactured using chemical products.
- **Critical Manufacturing:** Manufacturing processes require a regular supply of a range of chemical products.
- **Energy:** Chemical manufacturing processes can require large amounts of energy, while many energy processes require specialized chemical products (e.g., explosives are essential to mining coal for energy production).
- **Food and Agriculture:** Fertilizers, herbicides, and pesticides produced by the Chemical Sector are vital for agriculture.
- **Healthcare and Public Health:** Medicines and pharmaceuticals essential for healthcare and public health operations require specialized chemicals for their production.
- **Information Technology:** IT systems are a critical component of day-to-day Chemical Sector operations. The IT Sector depends on the Chemical Sector for the raw materials used to manufacture components such as computer chips.
- **Transportation Systems:** Chemicals are transported throughout the country using all modes of transportation. Those modes of transportation rely on petrochemicals and other chemical products.
- **Water and Wastewater Systems:** Wastewater treatment and water purification processes rely on chemicals to make water safe, while chemical manufacturing requires large amounts of process and cooling water.

Industrial Accidents

Recent Chemical Security Analysis Center (CSAC) data show that chemical incidents in news reports commonly involve chemical storage, transport, production, and laboratories. Month-to-month CSAC data indicate that chemical accidents represent about one-third of all chemical incidents reported. Although the Chemical Sector operates at a high level of safety, accidents occasionally occur. Human error or faulty processes are generally factors in such accidents. The United States Chemical Safety and Hazard Investigation Board identified aging equipment and inadequate mechanical integrity and preventive maintenance programs as recurring root causes of chemical industrial accidents.

- **Industrial Accident Reporting:** CSAC analyzes monthly news reporting of chemical-related incidents all over the world. From October 2016–January 2017, 34 percent of worldwide chemical incidents involved accidents with chemical storage, transport, production, and laboratories. During the same time period, 47 percent of domestic incidents involved such accidents.[23]
- **Major Industrial Accidents:** Recent examples of major chemical accidents include an ethanol production facility explosion that killed five people, an isobutane release and fire at an oil refinery that injured several people, and a chlorine gas release at a distilled spirits facility that injured 140 people.

Opioid Production, Transport, and Security

Increased use, overdose, and illegal sale of opioids leads to increased risk of theft, attack, and potential changes in manufacturing. The opioid crisis in the United States is rapidly expanding. As a result, malicious actors seeking to steal or produce opioids for their own use or profit may increasingly target Chemical Sector pharmaceutical manufacturers for attack. Federal, state, and local government response to the crisis may introduce new regulations for these chemicals and require changes in their production, transport, and security.

- **Opioid Products:** Doctors prescribe opioids (e.g., oxycodone, hydrocodone, morphine, and methadone) to treat moderate to severe pain, but these medications can have serious risks and side effects. Fentanyl is a synthetic opioid pain reliever. It is many times more powerful than other opioids and is approved for treating severe pain, typically advanced cancer pain. Illegally made and distributed fentanyl has been on the rise in several states. Heroin is an illegal opioid. Heroin use has drastically increased across the United States among both men and women, most age groups, and all income levels.
- **Epidemic:** Drug overdose deaths and opioid-involved deaths continue to increase in the United States. 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.[24] 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.
- **Industry Production:** Opioid production facilities in the Chemical Sector may be subject to targeted attacks by those seeking to steal products or production techniques. As public awareness of the opioid epidemic increases, pressure for federal and state government response may result in changing regulations associated with opioids. Changes could include increased restrictions and heightened security requirements on production, transportation, and distribution of opioid products.

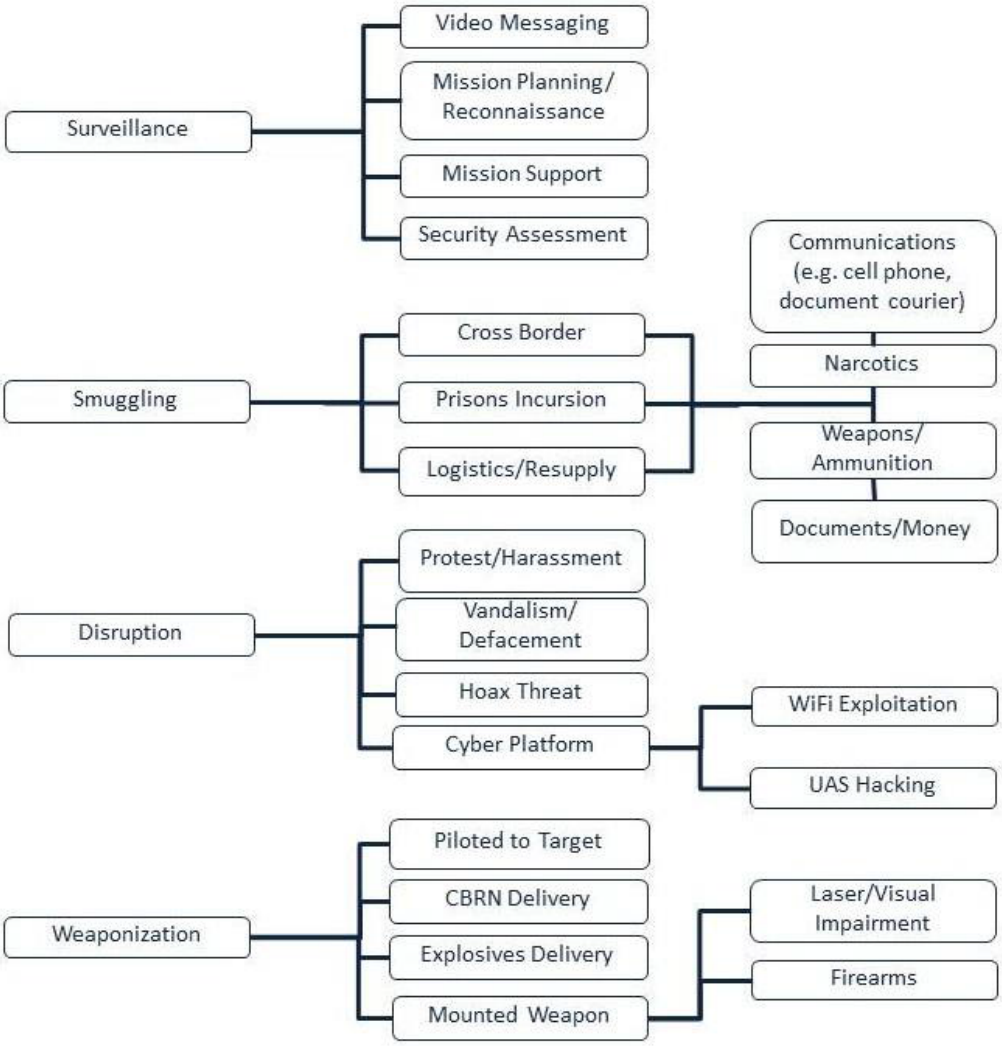
Unmanned Aircraft Systems

UASs continue to proliferate and may be used for nefarious activity, such as gathering surveillance or sensitive information or conducting physical/chemical/biological attacks. The Federal Aviation Administration 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.[25] Recent known malicious use of UASs includes Olympic stadium intrusions, smuggling operations across borders and into prisons, power infrastructure damage and outages, and radiological material delivery. Chemical Sector facilities with traditionally secure ground perimeter security are susceptible to UAS intrusion. In addition, sector facilities that use UASs in their normal operations (e.g., security or safety inspections and surveillance) may be at risk through counterfeit or altered components introduced into UASs. Malicious UAS activity (see Figure 4) typically may be categorized as follows:

- **Surveillance**: Includes adversaries leveraging 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:** Encompasses adversary use of UAS payload capabilities to deliver illicit or contraband materials to bypass security barriers
- **Disruption:** The intentional or unintentional use of a UAS that harasses, hinders, or inhibits security operations; use of a UAS to access, monitor, or attack computer networks and/or monitor or interfere with radio frequency communications

- **Weaponization:** Intentional adversary use of a modified or unmodified UAS as part of an attack intended to cause casualties or physical damage, including attempts to disrupt air traffic, crash deliberately, and deliver hazardous payload

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



Case Study: Ammonium Nitrate Fertilizer Facility Explosion

In April 2013, a fire at a fertilizer company's facility was reported to a local dispatch center in West, Texas. The blending, retail, and distribution facility had a stockpile of between 40 and 60 tons (80,000 to 120,000 pounds) of fertilizer-grade ammonium nitrate (FGAN), not including additional FGAN that was not yet offloaded from a railcar. Roughly 20 minutes later an explosion occurred, killing 12 emergency responders and 3 civilians and injuring more than 260 victims in the vicinity. The blast completely destroyed the facility and damaged over 150 offsite buildings. The explosion was one of the most destructive incidents investigated by the U.S. Chemical Safety and Hazard Investigation Board (CSB), based on loss of life among emergency responders and civilians; the injuries sustained by people inside and outside the facility fence line; and extensive damage to residences, schools, and other structures. The company filed for bankruptcy after the explosion.

Firefighters were dispatched to the scene without prior knowledge of how long the fire had been burning before it was noticed—there was no evidence of pre-incident planning addressing the likelihood of an FGAN fire at the facility. As a result, the firefighters who responded were not adequately informed or prepared to critically assess the situation before the explosion occurred. Shortly after arrival, the career fire captain advised firefighters that they did not have adequate resources to combat the growing fire. Because the firefighters were not aware of the FGAN hazard, they focused on cooling the liquid anhydrous ammonia tanks near the burning building to prevent them from rupturing or venting.

A federal and state criminal investigation determined that the incident was caused by arson. A CSB investigation found that there was no robust incident pre-planning process in place, hazmat awareness training was inadequate, and no previous FGAN-related fire emergency training or drills were conducted. Those responders trained and certified in the National Incident Management System did not establish an Incident Commander or an Incident Command System, which would have facilitated prompt and proper evacuation of nearby residents. Federal and State of Texas hazmat manuals placed little emphasis on responses to sites containing FGAN, and federal and state support for firefighters typically does not support training but instead focuses on equipment needs. Lessons learned from previous FGAN-related fires and explosions were not shared with volunteer fire departments. In addition, required training for volunteer fire protection personnel in Texas did not include response to fires involving hazmat. These were a few key findings from the incident that provide an impetus for additional training and developing improved regulations and requirements for both volunteer and career firefighters.

Endnotes

[1] National Oceanic and Atmospheric Administration (NOAA), Billion-Dollar Weather and Climate Disasters (January 2018)
[2] U.S. Department of Homeland Security (DHS) Office of Cyber & Infrastructure Analysis (OCIA), Columbia River Basin Petroleum and Refined-Product Supplies: Disruptions and Mitigations Under Cascadia Subduction Zone Earthquake Scenario (July 2016)
[3] Central United States Earthquake Consortium, After-Action Report (September 2014)
[4] U.S. Chemical Safety and Hazard Investigation Board, Arkema Fire (May 2018)
[5] NOAA, Billion-Dollar Weather and Climate Disasters (January 2018)
[6] Talos, New VPNFilter malware targets at least 500K networking devices worldwide (May 2018)
[7] McAfee Labs, Threats Report (April 2017)
[8] Ibid
[9] PwC, Industry 4.0: Building the digital enterprise (March 2017)
[10] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 2016 Annual Vulnerability Coordination Report (September 2017)
[11] Symantec, Internet Security Threat Report (April 2018)
[12] Malwarebytes Labs, Cybercrime tactics and techniques: 2017 state of malware (January 2018)
[13] FBI, 2017 Internet Crime Report (May 2018)
[14] Symantec, Internet Security Threat Report (April 2018)
[15] Ibid
[16] American Chemistry Council (ACC), Transporting Growth: Delivering a Chemical Manufacturing Renaissance (March 2017)
[17] Trucks.com, Torrid Rate of Trucking Mergers Pauses, but More Consolidation Expected (September 2016)
[18] OCIA, Consequences to Critical Infrastructure from Container Shipping Disruptions (April 2017)
[19] FBI, Quick Look: 250 Active Shooter Incidents in the United States From 2000 to 2017 (January 2018)
[20] OCIA, Infographic: Potential for Hazmat Theft during Motor Carrier Transport (April 2016)
[21] Ibid
[22] American Society of Civil Engineers (ASCE), 2017 Infrastructure Report Card (March 2017)
[23] CSAC, News Topical Analyses (Monthly 2016, 2017)
[24] Centers for Disease Control and Prevention, Opioid Overdose (August 2017)
[25] DHS, Unmanned Aircraft Systems Addressing Critical Infrastructure Security Challenges (February 2017)

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, the U.S. Department of Homeland Security (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.

Natural Hazards

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

DHS Sector Outreach and Programs Division, Chemical Sector Hurricane Exercise Fact Sheet (March 2017)

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

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

Cybersecurity

Accenture, Chemical Companies' Cloud Strategies: Current Adoption and Future Plans (December 2014) https://www.accenture.com/t20151013T135810Z__w__/ae-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_7/Accenture-Chemical-Companies-Cloud-Strategies-Current-Adoption-Future-Plans.pdfla=en

Cisco, 2018 Annual Cybersecurity Report (February 2017, 2018) https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

DHS, Cloud Security Guidance (February 2018) https://www.us-cert.gov/sites/default/files/publications/Cloud_Security_Guidance-.gov_Cloud_Security_Baseline.pdf

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

DHS Office of Intelligence and Analysis (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)

Electricity Information Sharing and Analysis Center (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

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

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

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

PwC, Industry 4.0: Building the digital enterprise, Chemicals Key Findings https://www.pwc.nl/nl/assets/documents/industry-4-0-building-the-digital-enterprise-chemicals.pdf

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

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

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

United States Computer Emergency Readiness Team (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

Supply Chain Security and Resilience

ACC, Transporting Growth: Delivering a Chemical Manufacturing Renaissance (March 2017) https://www.americanchemistry.com/Transporting-Growth-Delivering-a-Chemical-Manufacturing-Renaissance.pdf

Accenture, Chemical Industry Vision 2016: New Realities, New Opportunities (June 2016) https://www.accenture.com/t20160609T025416__w__/us-en/_acnmedia/PDF-22/Accenture-Chemical-Vision-2016.pdf

DHS I&A, Public-Private Analytic Exchange Program, Threats to Pharmaceutical Supply Chains (July 2018) https://www.dhs.gov/sites/default/files/publications/2018_AEP_Threats_to_Pharmaceutical_Supply_Chains.pdf

Elsevier, Industry 4.0: Top Challenges for Chemical Manufacturing (March 2017) https://www.elsevier.com/__data/assets/pdf_file/0005/278132/CHEM-MAN-WP-Industry-4.0-Top-WEB.pdf

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

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

Criminal Activities and Terrorism

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 (November 2017) https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91513

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)

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

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

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

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

The National Counterterrorism Center, Counterterrorism Digest (Weekly, multiple 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)

OCIA, Infographic: Potential for Hazmat Theft during Motor Carrier Transport (April 2016)

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

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

Crosscutting Issues

ASCE, 2017 Infrastructure Report Card (March 2017) https://www.infrastructurereportcard.org/wp-content/uploads/2016/10/2017-Infrastructure-Report-Card.pdf

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

CSAC, Chemical Current News Report (Multiple dates, 2016–2018)

CSAC, News Topical Analyses (Monthly, 2016, 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

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 Office of Infrastructure Protection, CI SAR Reports (Multiple 2016-2018 dates)

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

OCIA, Aging and Failing Infrastructure Systems: Highway Bridges (September 2015)

OCIA, Aging and Failing Infrastructure Systems: Natural Gas and Hazardous Liquid Pipelines (December 2015)

OCIA, Aging and Failing Infrastructure Systems: Navigation Locks (December 2015)

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

OCIA, Impact of Population Shifts on Critical Infrastructure (July 2016)

OCIA, Infographic: Potential for Hazmat Theft during Motor Carrier Transport (April 2016)

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

U.S. Chemical Safety and Hazard Investigation Board, Arkema Fire (May 2018) http://www.csb.gov/file.aspx?DocumentId=6068

U.S. Chemical Safety and Hazard Investigation Board, Investigations (Multiple dates, 2016–2018) http://www.csb.gov/investigations/

U.S. Chemical Safety and Hazard Investigation Board, West Fertilizer Company Fire and Explosion (April 2013) http://www.csb.gov/file.aspx?DocumentId=732

U.S. Department of Justice, Local Chemical Engineer Must Pay Approximately $4 Million in Restitution for Unlawfully Possessing Trade Secrets (August 2016) https://www.justice.gov/usao-ndtx/pr/local-chemical-engineer-must-pay-approximately-4-million-restitution-unlawfully

U.S. Department of Justice, Walter Liew Sentenced to Fifteen Years in Prison for Economic Espionage (July 2014) https://www.justice.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espionage

Appendix B. Tools, Training, and Programs

Relevant tools, training, and programs that may help Chemical 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.

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 (NWS) 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

National Incident Management System (NIMS) Training Program – FEMA's NIMS Training Program offers many courses on NIMS and the Incident Command System (ICS) through the FEMA Emergency Management Institute (EMI). https://training.fema.gov/nims/

Ready Business – The DHS Ready Business program assists businesses in 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

Cybersecurity

Chemical Sector Cybersecurity Framework Implementation Guidance – This guide simplifies the NIST Cybersecurity Framework implementation process for all organizations in the Chemical Sector to apply the principles and best practices of risk management. https://www.dhs.gov/publication/chemical-cybersecurity-framework-implementation-guidance

Critical Infrastructure Cyber Community (C3) Voluntary Program Small and Midsize Businesses (SMB) Toolkit – DHS provides 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

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 IT 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

eManagement White Paper: Every Small Business Should Use the NIST Cybersecurity Framework – This white paper can help SMBs understand and use the NIST Cybersecurity Framework. The paper 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

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

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

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/

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 Cybersecurity Framework – This voluntary framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. https://www.nist.gov/cyberframework

Network Security Training – CERT Network Security 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/

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

Supply Chain Security and Resilience

Chemical Inventory Management System – Sandia National Laboratories' International Chemical Threat Reduction Department developed the Chemical Inventory Management System (CIMS) software tool to track chemicals at a facility or institution. The software CIMS tool is designed for a single central receiving/storage facility with only a limited number of CIMS authorized users, but the tool can be adapted for use at a facility with multiple points for chemical receiving and storage. http://www.csp-state.net/resources/chemical-inventory-management-system/

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

Chemical Indicators: Laboratory Security Awareness – This FBI video offers a realistic scenario that emphasizes the importance of maintaining awareness in the academic laboratory environment and reporting suspicious activity to the appropriate authorities. https://www.fbi.gov/video-repository/chemical-indicators-laboratory-security-awareness.mp4/view

Counter-Improvised Explosive Device (IED) Awareness Products – The 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, 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

Counterintelligence Strategic Partnership Program – The FBI works with businesses and academia to determine and safeguard those technologies that, if compromised, could result in significant economic and national security losses. https://www.fbi.gov/file-repository/counterintelligence-strategic-partnership-programs.pdf

Economic Espionage Campaign – The FBI launched a nationwide awareness campaign for economic espionage. https://www.fbi.gov/news/stories/economic-espionage

Guidance for the Expedited Approval Program (EAP) – This DHS guidance document provides Tier 3 and 4 chemical facilities with a better understanding of security measures that could be used to meet the CFATS Risk-Based Performance Standards. The guidance helps identify and select processes, measures, and activities that may be implemented to secure and monitor facilities. The prescriptive measures contained in the guidance are intended to apply specifically to facilities that elect to participate in the EAP. https://www.dhs.gov/cfats-expedited-approval-program

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

Insider Threat Training – The CERT Insider Threat Center provides insider threat courses, workshops, vulnerability assessments, exercises, and best practices to support insider threat programs for critical infrastructure. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91513

International Biological and Chemical Threat Reduction (IBCTR) Program – Sandia National Laboratories' IBCTR program enhances national and international security by developing and executing innovative solutions for countering biological and chemical threats worldwide. http://ibctr.sandia.gov/

IS-906: Workplace Security Awareness – This FEMA course provides guidance to individuals and organizations on how to improve 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

Jack Rabbit II Project – The DHS CSAC is leading the Jack Rabbit II project, a series of large-scale outdoor chlorine release trials conducted with a collaborative team of partners from government, industry, and academia. https://www.dhs.gov/publication/jack-rabbit-ii-program-chemical-security-analysis-center

Risk-Based Performance Standards Guidance – This DHS guidance document assists high-risk chemical facilities in selecting security measures and activities that comply with the CFATS regulations at the appropriate tier level, tailored to the unique considerations of each facility. https://www.dhs.gov/cfats-rbps

Spotting Insider Threats Guide – This 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

Suspicious Activity Reporting (SAR) Explosive Precursors Point-of-Sale Training – This interactive course, available from the Nationwide SAR Initiative (NSI), instructs sales personnel involved at the point of sale on behaviors and indicators that are reasonably indicative of potential terrorist and/or criminal bomb-making activity. The training also teaches how and where to report suspicious activity and how to protect privacy, civil rights, and civil liberties when documenting information. https://nsi.ncirc.gov/hsptregistration/explosive_precursors/

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

Crosscutting Issues

Chemical Risk Management Self-Assessment Model (Chem-SAM) – Chem-SAM, designed for small and medium chemical facilities and laboratories, allows security officers and managers to evaluate security risks, support risk management decision making, and provide better risk communication in chemical facilities by providing an assessment method that is standardized, systematic, and replicable. https://www.dhs.gov/publication/chem-sam-fact-sheet

Chemical Security Assessment Tool (CSAT) – CSAT is an online portal to help DHS identify facilities that meet the criteria for high-risk chemical facilities under the CFATS. CSAT contains applications for the Top-Screen, Security Vulnerability Assessment (SVA), Personnel Surety Program, and Site Security Plan (SSP). https://www.dhs.gov/chemical-security-assessment-tool

ChemStewards – ChemStewards is an environmental, health, safety, and security management program designed to help a facility optimize its performance, save money, and enhance its role as a good corporate citizen in a community. The program was established to meet the unique needs of the batch, custom, and specialty chemical industry. http://www.socma.com/chemstewards

CHEMTREC – CHEMTREC is an around-the-clock service available to emergency responders who need immediate information for incidents involving chemicals, hazardous materials, and dangerous goods. https://www.chemtrec.com/about-chemtrec

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

CSAT 2.0 Demonstration Webinars – DHS has recorded three webinars that walk users through the revised CSAT tools: CSAT 2.0 Portal, CSAT 2.0 Top-Screen, CSAT 2.0 SVA/SSP. https://preview.dhs.gov/chemical-security-assessment-tool

NACD Responsible Distribution – The National Association of Chemical Distributors (NACD) Responsible Distribution is NACD's mandatory, third-party verified environmental, health, safety, and security program in which members demonstrate their commitment to continuous performance improvement in every phase of chemical storage, handling, transportation, and disposal. https://www.nacd.com/rd/about/

ResponsibleAg – Endorsed by The Fertilizer Institute, ResponsibleAg is an industry-led stewardship initiative designed to help fertilizer storage and handling facilities achieve and maintain federal regulatory compliance. https://www.responsibleag.org/About.cgi

Responsible Care Security Code – The American Chemistry Council developed the Responsible Care Security Code to enhance the security of Chemical Sector facilities, their communities, and their products. https://responsiblecare.americanchemistry.com/ResponsibleCare/Responsible-Care-Program-Elements/Responsible-Care-Security-Code/

TRANSCAER – TRANSCAER is a national outreach effort that promotes safe transportation and helps communities prepare for and respond to any transportation incident involving hazardous materials. https://www.transcaer.com/national