Cybersecurity Within The Applications Of Environmental Standards

Erik Buschardt

Webster University

Abstract

This paper will serve to explore how cybersecurity is affected by the response, progression, technological evolution and market-based innovations of sixteen officially documented National Critical Infrastructure Sectors, with regards to increased environmentally-friendly standards of emission, transmission, and/or production within real-time scenarios. In addition, a four-part threat assessment matrix is introduced and performed within each category, both before and after the application of said standards. If the operation of any sector's facilities are not currently environmentally-friendly, as defined or otherwise established as a statistical norm and best practice, using a definition that comes from a consensus of professional environmental advocacy organizations such as the Leadership in Energy and Environmental Design (LEED) or the Carbon Trust Standard, various alternatives are explored and researched findings are documented accordingly. Discovering such findings will inform the reader if a current worldwide trend of environmental conservatism and sustainability may or may not significantly improve the cybersecurity readiness posture for each sector of critical infrastructure within the United States.

Keywords: cybersecurity, critical infrastructure, threat assessment matrix, analysis, environmental standards, best practices

Table Of Contents

Cybersecurity, both as an art form and as a science, as come to light in recent decades as the global community seeks to change a large paradigm shift. Originating as an afterthought, the concepts of security of worldwide web traffic, network infrastructure and the computing network as a whole, never seemed to catch on mainstream until it was too late. Two years after Target's infamous data breach happened, the author was fortunate enough to journey through an amazing set of insightful curriculum, two classes of which are combined into this capstone master's thesis. The goal is to combine modern concepts of threat analysis and resolution, with an environmental frame and viewpoint, so as to not rehash old concepts told through previous theses generated via said journey. Specifically, there are sixteen (16) economic sectors of industry as identified by the United States Department of Homeland Security, known as Critical Infrastructures. Each will be identified, assets explained, threats outlined, alternative environmental best-practices introduced, and countermeasures given. By presenting a thesis with this unique set of ideas, it is sincerely hoped that the reader will come away with a greater appreciation for the science of cybersecurity within the application of environmental standards.

I. The Chemical Sector

First, the Chemical Sector primarily consists of organizations and companies who manufacture and sell naturally- and artificially-created chemical product commodities including pharmaceutical medications, fertilizers, herbicides (e.g. weed killers), pesticides, growth hormones for livestock, and fungicides within the agricultural industry. Specifically, the pharmaceutical industry has played a significant role since the mid-nineteenth century and towards the advent of

the twentieth, by creating and advancing effective technological solutions to various ailments ranging from the common cold to allergies, birth control, and many more uses, as administered by a doctor's prescription, recommendation(s), and/or over-the-counter medications as a primary healthcare solution.

In addition, the advancements in consumer-driven convenience goods, (everything from plastics, synthetic rubbers, petroleum-based goods, to environmentally sustainable recycled materials), are considered in this sector to be dependant on available finite resources since the dawn of the Industrial Revolution. The Department of Homeland Security, in conjunction with the United States Food and Drug Administration (FDA), is responsible for the safety and security of these chemicals used on a daily basis throughout agricultural communities and manufacturing plants around the country. Chemical uses will vary based primary on utility, but will typically fall under one or more of the following categories including (1) Agricultural and rural usage, (2) Pharmaceutical medications, and (3) Consumer products for a retail market. Specific critical assets include the place of development, research and manufacture for each chemical agent, as well as any significant point of distribution, as the chemical(s) comes to market. (Chemical Sector, n.d.)

The threats facing the Chemical sector include any and all violations of security in tampering with the manufacture of raw materials, and/or the distribution of chemical products as a finished product, including those violations of corporate espionage studied in previous cybersecurity classes at Webster University such as CSSS 5130: Intelligence and Counterintelligence.

Examples of chemical espionage includes the threats faced by the Dow Chemical Company on a daily, even hourly basis, with regards to the risks of intellectual theft of corporate trade secrets including chemical formulas, patented designs, and new product technologies by overseas hackers. Motivations for these espionage attempts include randomized tradecraft, gaining knowledge or supplies in order to carry out acts of terrorism worldwide, as well as political or environmental activism against any number of products already released to market, or even to attempt to discover products still under development. In the testimony provided, (Kepler, p. 13-16), Dow requests the aid and cooperation of the federal government in order to successfully implement a number of planned strategies going forward with regards to chemical cybersecurity.

Chemical espionage attempts continue to threaten the chemical sector, going so far back as 2011 in a documented case against 29 companies, as well as "another 19 in various other sectors, primarily the defense sector." (Rohrlich, J.) According to this whitepaper, these nineteen companies cited were apparently the target of an intellectual properties espionage campaign that lasted over two and a half months, which were determined to have originated from an online network originating from the United States, but controlled and owned by a "20-something male located in the Hebei region in China." as part of a remotely controlled malware botnet. As part of our studies, it is reinforced over and over again that the majority of weaknesses in our network of global communications (Email and HTTP being chief protocols of this network of networks) are continually being exploited by state-sponsored college-age kids from China, Russia, the Ukraine, as well as other developed regions.

All measures of corporate security presently maintained in the securing of trade secrets, with regards to the manufacture of chemical goods at present, would translate well to the sourcing of sustainable resources and biodegradable or renewable products such as those used in the consumer and retail marketplace. Most significantly, the petroleum industry would endure the most long term changes to their business model and materials sourcing, and could profit greatly from if executed properly. Furthermore, toxicity levels related to cancers and other long term illnesses leading up to and including death, as related to such agricultural products as pesticides, herbicides, and other mannerisms of organic destruction, could be minimized to acceptable tolerances, should the marketplace demand more organic materials be sold competitively, as is fortunately the trend. From a cybersecurity perspective, the infrastructure and machinery in place would not be placed at intolerable levels of risk, if there was a redundant capacity for the harvesting of sustainable, renewable and organic materials. (Morgalwalp, D. W., n.d)

The global chemical sector, buying and trading with various shippers and suppliers around the world, ensures that essentially no part of the world is safe from accidental leakage or spillage from a potentially hazardous chemical, either from an accidental event or a cyberterrorist event. What must be considered is risk management, where the largest quantities of each chemical, sorted by level of hazardous safety and risk to any surrounding population, be safeguarded appropriately and proportionately. With regards to intellectual property and trade secrets in chemical formulas (for example the recipe for Coca Cola, or pharmaceutical formulations, or even to know what Red 40 means on a food package), physical measures must be in place to safeguard this data from theft. (Xue, 801)

II. The Commercial Facilities Sector

The Commercial Facilities Sector consists of any and all publicly accessible buildings and/or designated landmarks for a wide variety of purposes including commerce, tourism, entertainment, healthcare, and healthcare facilities. The common factor in these types of facilities is that security is kept at an unobtrusive and discrete minimum, in order to maximize and facilitate these purposes described. Usage of commercial facilities will vary based on the nature of the industry that the facility is a part of, for example a gambling casino for a gaming company, or a clinic for a hospital conglomerate group.

Critical assets for a commercial facility will vary based on the activity maintained inside each building, but fall into eight general categories or sub-sectors: (1) Entertainment and Media (for example, broadcast media and motion picture studios), (2) Gaming (including casinos), (3) Lodging (for example hotels and motels), (4) Outdoor Events (including parade routes, fairgrounds, amusement parks, as well as campgrounds), (5) Public Assembly (for example convention centers, arenas, stadiums, zoos, aquariums, museums, theatres and concert halls), (6) Real Estate (both commercial offices, and residential units including apartment buildings, as well as self-storage facilities), (7) Retail (for traditional shopping malls as well as any outdoor retail district such as Laclede's Landing), (8) Sports Leagues, (stadiums and their immediate surroundings).

Specific critical assets in common with all eight sub-sectors in this Commercial Facility Sector include all entry and exit bottleneck points, as well as any common points of assembly within the commercial facility, for example a front desk, a central atrium/meeting place, or a checkout counter located near exits. (Commercial Facilities...)

A number of recent data breaches as researched in Webster University's graduate level course CSSS 5990 sections 05 and 08: Advanced Topics and Malware, taught by Adjunct Professor Oladipupo ("Ladi") Adefala, reveal a vast number of virtual bloody casualties involving large corporations, government agencies and retail outlets as each having suffered massive security and data breaches as evidenced by destructive malware payload attempts delivered within their network infrastructure. These companies and government agencies include but are not limited to: Adobe Systems (2014), AT&T (2015), Anthem Incorporated (2015), America Online (2004, 2006, 2014), Ashley Madison (2015), Barnes & Noble (2012), CardSystems Solutions Inc. (2005), Citigroup (2005, 2011, 2013), The Commission on Elections (2016), Countrywide Financial Corp (2006, 2011), CVS Health (2015), the Democratic National Committee (2016), eBay (2014), Facebook (2013), Gawker blog (2010), Gmail (2014), Home Depot (2014), JPMorgan Chase (2010, 2014), Michaels (2014), Neiman Marcus (2014), the United States Office of Personnel Management (2015), Scottrade (2015), Sony Online Entertainment (2011), Sony Pictures (2011, 2014), Target (2013), TD Ameritrade (2007), Trump Hotels (2014), UK Revenue & Customs (2007), UCLA Medical Center, Santa Monica (2015), United Parcel Service (2014), United States Department of Veteran Affairs (2006), National Archives and Records Administration (U.S. military veterans' records, 2009), Verizon Communications (2016), Walmart (2015), The Washington Post (2011), Yahoo (2012, 2013, 2014, 2016), and Zappos (a subsidiary of Amazon.com, 2012). (Granville, K.)

Oftentimes, organizations will discover abnormalities in their network monitoring procedures well after the fact, in some cases not at all. Other organizations have been advised via third party vendors that their systems have been compromised, at which point internal

investigations will usually begin. By that time, however, the loss of records and personally identifiable information (including social security numbers, addresses and credit card numbers) will range from the tens of thousands to the millions. Reasons for the hacks vary widely, but include common factors such as insider threats, accidental publication and disclosure, political objectives, accidentally misplacing media or equipment, poor security procedure, to elaborate hacking via malware and payload delivery (malicious email attachments or embedded website links) as discussed above.

Of course, data breaches are not the only cyber threats facing the commercial sector on a given day. Physical threats such as explosives or other direct violence introduced by specific threat agents continue to persist, counter measured of course by a careful balance of law enforcement and common sense law security procedure. Covert cybersecurity initiatives may also be maintained, such as a network of surveillance cameras, motion sensors, alarms or the like. (Deloitte Center)

Introducing a commercial building as ecologically friendly will require a certification from a number of official sources including Leadership in Energy and Environmental Design (LEED), Excellence in Design for Greater Efficiencies (EDGE), and Performance Excellence in Energy Renewal (PEER), administered through Green Business Certification, Inc, (GBCI). Common starting points in the conversion to sustainable energy use for a commercial facility includes the source of electric power, sewage and water utilities from the municipalities in which the building is located. Additional enhancements subject to environmental certifications include advanced HVAC usage, as well as an efficient use of greywater (stormwater runoff from roofs and patios, etc).

Buildings that rely solely upon their own immediate environments, at least in terms of electrical and utilitarian needs, tend to be more resilient upon widespread cybersecurity incidents such as those involving traditional grid-based power outages. Costs for the installation and daily operation of secured environmental alternatives may exceed initial investment earmarks for some companies. As a financial compromise, a mixture of technologies can come into play initially, such as solar powered backup generators, should a cyberterrorism event occur to a place of business or corporate headquarters campus. (Boeing, 13)

As previously mentioned, the employment of closed-circuit video cameras may be enough deterrent for some attempts. Additional layers of security may include internal motion sensors, timed door locks, card keys used for authorized persons, biometrics, key codes or key-phrases. In terms of data manipulation, the latest in encryption algorithms, two-factor authorization, limitation of data to certain locations, strong password management, and regular user education will provide a strong cybersecurity posture in terms of commercial facilities within the United States, (Deloitte).

III. The Communications Sector

The Communications Sector consists of all national and international telecommunications and data infrastructures, for both analog and digital means of transmission. This includes all wireless networks, satellite operators, Internet Service Providers (ISPs) as well as cable companies. Since the birth of the modern telecommunications infrastructure in the 1830s, there has been a gradual saturation of the worldwide telecom market, marked by spikes of activity with the adoption of new technologies in this sector. Specifically, within the latter half of the 20th century, the world

shifted to the power of digital transmissions, which began to replace analog. Critical assets include all transmission nodes, telephones, ports, terminals and gateways that form the cellular, wireless and land-based infrastructures, as well as all networks that intersect and interconnect these communication and data nodes. (What is the…)

While no major disruptions on the order of magnitude of previous data breaches have taken place within the communications sector, the Obama Administration remains committed to the closing of reported vulnerabilities within the national telecommunications infrastructure before a malicious hacker exploits these vulnerabilities. That said, however, all transmissions are subject to data interference or noise, which is a primary concern for the cybersecurity professional, as we seek to focus on the minimization and eradication of said noise. (Yes, there have been Denial of Service attacks performed on a smaller scale, but I would argue this does not fall under the category of a communications network failure, insomuch that the attack was indeed successfully transmitted and executed). Due to multiple backup and redundancy systems built into commercial networking infrastructure, the change of a widescale communications failure remains minimal. In the worst-case scenario, transmissions are completely disrupted due to either an accidental intentional attack, with an indefinite or undetermined amount time for the restoration of service. To that end, public-private partnerships remain vitally important to solve current threats facing the communications sector and the international network of data transmission and related services, (Executive Order).

Major telecoms have decided to offset their environmental and utilitarian impact by planting trees in preserved woodlands in a marketing effort to appeal to consumer's shifting tastes regarding

sustainability. Further revenues can be generated by donating in an honoree's name for the preservation of said forests and conservation areas, going forward. (Green Telecom)

With regards to cybersecurity in telecoms, while disaster recovery and business continuity plans are already in place, more can be done to reduce the visual clutter of telephonic and data lines by placing them in underground cable corridors, alongside utilitarian pipelines. (Solar Roadways Specifics) Reducing the visual clutter of above-grade cables will decrease the accidental risk of interruption during a rainstorm or winter blizzard, while also decreasing the ease of sabotage by malicious cyber agents of simply cutting the active power and data lines (insulation from electroshocks notwithstanding).

Countermeasures to cybersecurity threats posed within the Communications Sector includes the mandate to safeguard all data and transmissions that are carried on public telephonic and data cables that exist throughout the national infrastructure. To the extent that eavesdropping and "man in the middle" attacks could be carried out by malicious threat agents any wireless local hotspot such as a Panera Bread or Starbucks, it is ultimately the responsibility of the user. (Rosenfield, Everett, H).

IV. The Critical Manufacturing Sector

The Critical Manufacturing Sector includes all industrial-grade machinery and fabrication plants within the United States, including a number of industry specialities such as the mining of natural metals, the manufacture of diesel, gasoline and electric plants, as well as the production and shipment of large transport vehicles such as locomotives, trucks, container ships, and cargo aircraft.

Critical assets will include any sensitive component involved in the manufacture of large equipment, the place of manufacture, as well as any distribution centers as these products ship to the final customer. (Critical Manufacturing Sector)

In terms of Critical Manufacturing, cybersecurity professionals at the Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT) have noted that cyber and malware-based attacks have doubled in 2015 versus previous years on record, up to a total of 295, or almost one per day. These include attacks on vehicle manufacturers, as well as producers and shippers of electrical equipment, machinery and the processors of raw metals. Causes for an attack in these cases will usually fall under one of three categories: (1) infestations or data breaches via criminal malware, (2) disruptions of service attempts, and (3) theft of intellectual property or corporate trade secrets in preparation for an upcoming planned attack event. (U.S. Sees Jump)

Plants and factories that manufacture critical goods must continue to remain vigilant with regards to outdated methods of protection, including but not limited to routers and corporate firewalls, as well as software and filtering solutions that enable employees to access external networks, as these indicators of compromise may be the key to introducing a malicious payload into the internal corporate system for deployment and exploitation. Not only on a computer-based network secured with the latest available operating system patches, but the factory machines themselves, which may operate with a set of programming instructions that predate the current era of computing, (think COBOL and FORTRAN). While cybersecurity professionals occupy their time developing and maintaining the current fleet of deployed equipment throughout their company, a hacker with enough time on their hands and given a factory with default internal

settings may seek to exploit the factory floor's robotic equipment itself, placing the entire company at risk of compromise and/or complete shutdown.

This sector plays a unique role in the national economy because of the sources of materials harvested, as well as the methods of production in order to produce finished factory goods. With regards to environmentalism and sustainability, it is in the company's long term interest to harvest renewable materials, as well as to recycle goods that have expired a useful operations life cycle. This is especially true with materials such as aluminum, stainless steel, glass, plastics and certain paper-based goods. As stated before, as a factory produces these renewable and recycled goods, a company will need to implement cybersecurity technologies such as "smart" firewalls, which adapt the flow of acceptable network traffic based on learned past policies implemented by the organization. Other next-generation cybersecurity tools for use by the Critical Manufacturing Sector include anti-malware software solutions for factory floor robotic tools, backups including secondary robotic tools, and some degree of isolation from the corporate network so that in the event of a cyberterrorism event affecting the entire manufacturing plant, not all systems are taken down. (McLaughlin, K.)

The Critical Manufacturing Sector will continue to phase out obsolete equipment, as well as isolate machinery which may pose a cybersecurity threat when networked together with external corporate data infrastructure. If there are patches available to fix known vulnerabilities with existing robotics, it the responsibility and mandate of the organization in order to maintain cybersecurity compliance. In addition, any increase of utilitarian (chiefly power-based) efficienciencies in terms of robotic and other mechanical equipment on the factory or sales floor

will not only reduce the calculated carbon footprint of the organization, but will serve to enhance the organization's cybersecurity posture, should utilitarian blackouts occur for any reason. (LeClair, J., 100-105)

V. The Dams Sector

The Dams Sector is described as the infrastructure that contains and manages the nation's system of controlled water reservoirs for various purposes. These purposes include local agricultural irrigation, river navigation, sediment and flood control, recreation, as well as industrial waste management. Critical assets include the reservoirs, aquifers and generators contained in the power plants located at or near the dam itself. It is estimated that hydroelectric facilities and assets currently protect approximately 40% of the national population from the effects of flooding, while irrigating at least 10% of rural croplands. (Dams Sector)

Threats facing the Dams Sector include any number of software or hardware-based attacks that, if successfully deployed and implemented, would cripple the infrastructure in a number of ways. A dam or hydraulic system could be disabled or hijacked so as to operate the dam improperly and maliciously, causing economic and operational damage. In addition to the potential theft of intellectual property with the safe operation of machinery and equipment, a hacker could overload the equipment, use the equipment to mount attacks on other systems, operate machinery in ways that would cause flooding and irreparable damage and casualties to surrounding communities, conduct surveillance or otherwise gain information regarding the facility or personnel, including operating schedules, security and contractors on site. (U.S. Dept. of Homeland Security / Dams Sector)

Climate changes as well as an evolving cyber landscape continue to define risk elements to the Dams Sector. As more extreme weather events persist (such as storms, tornadoes, drought), dams and hydroelectric grid-based systems for local communities will be at the forefront of concern. It is no small coincidence that such large objects as dams will remain a target for physical attack via traditional or cybersecurity means. Plant operators continue to strike a balance between ecological concerns and long term weather events, needs of the community as well as that of the national power grid, as well as any upgrading of internal mechanics to new hardware and software solutions, similar to cybersecurity needs posed by the Critical Manufacturing Sector. (Dams Sector)

A risk management strategy for the dams sector will rely on a multilayered approach, consisting of preventive risk management, adherence to a sound crisis management program, emergency action plan, business continuity policy, disaster recovery effort, and of course the notification of any emergency and its aftermath to proper authorities as well as affected communities in a timely manner. This will affect both physical as well as cyber-intrusion events in a similar manner, however the nature of each individual threat as they play out will determine the proper response course for individual hydraulic stations and power plants. [U.S. Dept. of Homeland Security, (2015)]

VI. The Defense Industrial Base Sector

The Defense Industrial Base Sector, also known as the Military–Industrial Complex (MIC), is a large formal alliance between the United States military and companies of private industry. Research and development of military-grade weaponry, components and/or subsystems are manufactured as per military specifications under contract. More than 100,000 companies and

contractors provide design capabilities, production, delivery and maintenance to the Department of Defense. MIC companies include domestic as well as foreign entities. This Sector does not include the commercial infrastructure of the companies involved in the MIC, but only the weapons, vehicles, and other systems as manufactured.

Critical assets in the Defense Industrial Base Sector include all manufacturing plants and facilities that produce weapons systems, support systems, transport vehicles, or other equipment that is expected to aid in the successful completion of any mission. (Defense Industrial Base Sector)

Within the scope of the Defense Industrial Base (DIB), a 2012 memorandum from the Office of the Deputy Secretary of Defense of the United States highlights the importance and relevance of a proposed Cyber Security and Information Assurance (CS/IA) program as well as an optional Enhanced Cybersecurity Services (DECS) component of the CS/IA proposal.

Under this program, the Department of Defense (DoD) would provide classified and unclassified cyber threat information and best practices to DIB companies. In turn, DIB participants would report incidents that may involve DoD information or components, in order to develop a coordinated mitigation strategy as well as a resolution of damage assessments of compromised information, when warranted.

Needless to say, the Defense industry as a whole remains a prime target for government espionage, in particular the sort of foreign intelligence that nation-states such as Russia and China seek to exploit every hour of every day. Participation in the sort of structured policy environment, such that the CS/IA and DECS would provide, would benefit our national cybersecurity posture greatly. (DoD's Defense Industrial Base Cybersecurity Information Sharing Program)

Eventual reduction in the usage of fossil fuels as well as the migration towards renewable energies will help to mitigate the dependency on foreign fossil fuels, as well as reduce any political risk associated with these dependencies. Fuel for military vehicles is a critical part of any worldwide operation, and a sustained supporting effort is essential for the success of a mission. For that reason, it is in our national interest to reduce the risk inherent in any fuel or power grid supply, should resources become scarce in the long term. (Redesigning defense)

With regards to the penetration of third party vulnerabilities inherent in each new contractor hired for defense work, we bear in mind the vulnerabilities exposed by the private retail industry from 2013 to the present day, which is enforcement of corporate and military-grade information classification and data policy with each new username and password created, and levels of access granted. An abuse of these privileges will result in poor management of data and at worst, a data breach of significant magnitude.

VII. Emergency Services Sector

The Emergency Services Sector (ESS) consists of millions of highly-skilled professionals, that together with specially-equipped vehicles, equipment and facilities, perform routine prevention and awareness activities, as well as incident management in the case of local emergencies. The ESS includes private sector resources such as security management organizations, private incident-response management providers, as well as corporate entities that respond to on-campus incidents. Critical assets of this sector include the personnel, equipment, vehicles and facilities, as

well as any local or on-campus routes taken to ensure a prompt response to any immediate threat or incident.

The cybersecurity posture of the Emergency Services Sector remains highly critical, due to the threat posed to first responders by the persistence of anti-police protests among activists and hacktivists, by threat agents who seek to fulfill their own respective political agendas, regardless of current authority. In addition, any police unit or law enforcement agency that receives media attention due to perceived gender or racial bias towards members of the public would be a target for such attacks as a distributed denial of service (DDoS), whereby their web servers are repeatedly hit by inbound HTTP requests, until they are overwhelmed by demands, and shut down automatically. Another hactivist strategy is "doxing", where personal information of particular police officers, detectives, or other agency personnel is released or leaked. This enables other protestors and activists to target the officers personally. (Emergency Services Sector)

Other threats include website defacements, manipulation of public opinion via social engineering, and classic malware cases such as the delivery and exploitation of government systems due to ransomware.

For those new to the concept, ransomware is a version of malware delivered to a targeted system, that when executed, hijacks all available data and encrypts or otherwise removes it, forcing the victim to pay a ransom or bounty in order to restore their data. Within the Emergency Services Sector, such exploitation of government systems via malware or ransomware would place untold numbers of the public at risk.

Hazardous materials as installed in modern technologies such as cell phone batteries and millions of related consumer products place additional cost burdens on local first responder resources. This poses a dual threat matrix of environmental as well as cybersecurity risk. With regards to environmental concerns of hazardous materials within the scope of the Emergency Services Sector, safeguards such as additional containment, security and proper disposal procedure must be in place to ensure the minimization of threats posed should hazardous materials be obtained illegally and used improperly, as would be the case in weaponizing a payload for malicious intent, or even accidentally disposing of in local rivers or streams, (see Water and Wastewater Sector: Threats), [Trench, N. J., & Wieder, M. A. (n.d.).]

Backup procedures, as part of a disaster recovery scenario, will be essential here. If a dispatch or primary communication system were to go down during an emergency deployment of services to the public at large, that incident may suffer fatalities or other disastrous results. It is in the taxpayer's interest to fund cybersecurity training scenarios, so that first responders may apply industry best-practices towards each emergency deployment, whether it be a residential firefighting scenario, a criminal data breach involving the theft of corporate commercial assets, or a HIPAA violation at a local hospital.

VIII. The Energy Sector

The Energy Sector is perhaps the most valuable of all Sectors in that it provides the basic and fundamental resources in order to power all other sectors. Presidential Policy Directive #21 defines this sector as a unique "enabling sector", which is responsible for influencing all other

sectors in a direct manner. For example, fossil fuels including petroleum-based products, power vehicles used in the Emergency Sector, the Transportation Systems Sector, electricity and power needs for the Commercial Facilities Sector and the Defense Industrial Base Sector, as well as others.

Critical assets of the energy sector will include all extraction and drilling equipment, personnel, facilities, any supporting equipment, as well as power lines, cables, pipes and other distribution nodes used to transport the fuel from the initial extraction point to the final customer. (DHS/Energy Sector)

The Energy Sector remains one of the most critical sectors within our Critical Infrastructure matrix, as it encompasses the fuels and materials for which other sectors such as Transportation and Information Technology would run, on a most fundamental level. Indeed, any data breach within the consumer retail space involving credit cards, social security, names and addresses would dwarf in comparison to the scope and magnitude of destruction that a breach of security within the Energy sector would provide. (Krancer, M.)

Recently, the Wall Street Journal reported that among a study group of 625 IT executives in western countries, almost half (48%) believe that a cyber-attack on national energy infrastructure is likely within the next three years. In addition to threats placed on the sector, is the lack of resources available to combat these threats. JP Morgan's annual expenses on cybersecurity are projected to more than double to $500 million over the next five to ten years.

Indeed, we are woefully underprepared for an imminent attack on the nation's power grids, generators, plants, oil drilling apparatuses, and auxiliary network systems. The numbers tell the

story: "In one instance, 73 percent believed they could detect unauthorized software added to their network, but only 59 percent of those knew how long it would take to detect the intrusion. In another case 84 percent thought that they would receive an alert within hours if an unauthorized device was found accessing their system, but 52 percent of these respondents did not know how long it took to generate these alerts." (Olenick, D.)

In short, the loss of productivity and quality of life that we endure during a simple localized blackout event, magnified towards the scale of the entire country, for an unknown amount of time, would be rather unprecedented in our history.

Environmental alternatives as well as cybersecurity risks associated with the current petroleum-based economy of the nineteenth and twentieth century go hand in hand. Based on previous research conducted at Webster University (CSSS 5120 Cybersecurity Infrastructures by Dr. James Curtis, Fall II, 2015), renewable sources of energy decreases both the risk of depletion of energy resources, as well as the political risks associated with such depletions. As noted in such research, most conflicts will begin as the depletion of resources is realized, (Chuck, H.)

It is absolutely imperative that the energy sector figure out commonsense approaches towards resolution of vulnerabilities inherent in outdated power equipment, turbines, pipelines and switches. This and many other red flag warnings comes at a time that the Cyber Emergency Response Team (part of the Department of Homeland Security) investigated up to 79 cyberattacks directed towards energy sector plants and equipment for fiscal 2014. While environmental considerations may be taken into account, redundancies and backups play a critical role here and in the disaster recovery plans of other sectors (such as Healthcare and Nuclear) as well.

IX. The Financial Services Sector

The Financial Services Sector presently consists of a global network of depository institutions (including retail banking, brokerage and investment firms), as well as the proprietary networks that intertwine these institutions. In addition, the financial markets are regulated within the United States by a number of governmental agencies including the Securities and Exchanges Commission, the Financial Industry Regulatory Authority (FINRA), the Commodity Futures Trading Commission (CFTC), the Federal Reserve System ("Fed"), and the Federal Deposit Insurance Corporation (FDIC), among many others.

The Financial Services sector is utilized by individual and corporate consumers as a regulatory standard for the value of currency used every day. Of course, specific critical assets include banknotes and coinage, as well as all machinery used to produce this currency at the United States Mint, but critically, more and more assets are being transferred via digital means. That means that the official proprietary and private subnetworks used, as layered on top of the public Internet topology, remains at a significant risk of interruption at any given point. Sublayers of any publicly-facing network, including Virtual Private Networks (VPNs) remain a critical asset in the daily functioning of the Financial Services Sector.

In addition, the hardware and software solutions used in financial transactions remains mission critical to each organization and network. Some are off-the-shelf (i.e. Dell workstations), and others are platform-based and web-based software solutions, custom built for the industry (i.e. Oracle Databases, or Business Intelligence Solutions).

In September of 2011, the Federal Bureau of Investigations presented a comprehensive listing of cyberthreats that persisted at that time. They include account takeovers and identity theft (primarily through the use of malware distributed via social engineering), third party payment processor security breaches, ATM card skimmers and POS malware at retail centers nationwide. (Statement before the House)

In addition to these technical aspects of fraudulent activity, we see another significant threat, as humans are oftentimes the greatest risk in any organization. Bribery, coercion and political corruption can derail the mission and values of any financial institution, as we have seen with the resignation of John Stumph, the former CEO of Wells Fargo & Company, (d.b.a. Wells Fargo Bank, N.A.), with regards to the manipulation and mishandling of customer accounts in October of 2016. Dishonest management and employees could also "rig the system" to their favor, by enabling or engaging in money laundering schemes or other related fraudulent behavior. While there have been significant improvements to the awareness of cybersecurity practices among corporate (white-collar) workers due to training, there is still much room for improvement in terms of user engagement and with regular updates to these industry-wide best-practices. (Statement before the House).

Any significant improvement within a financial institution's carbon footprint will have significant benefits for the environment as well as the organization's bottom line in terms of facilities and operational costs, but it is as of yet unclear how ecological standardization will affect the worldwide transfer of funds as per this sector's primary function. Banknotes and coinage must

still exist, as per monetary policy, but it will continue to decrease in our daily lives in developed first-world countries. (Rojas, A.)

The security and integrity of data payment transfers lies at the heart of the financial sector, and is central to its mission in the national economy. Virtual currency alternatives such as Bitcoin threaten to undermine traditional standardization of monetary policy as put forth since the agricultural and industrial revolutions, and are usually not as accepted as government-backed currency. Paypal, on the other hand, handles currency based on government-issued banknotes, and remains a powerful partner on the global currency stage, along with Mastercard, Visa, and American Express. Therefore it remains essential to ensure that state-of-the-art financial protocols such as Financial Information eXchange (FIX) stay within acceptable levels of risk tolerance, in order to guarantee the securing of digital payment formats.

X. The Food and Agricultural Sector

The Food and Agriculture Sector falls under the joint responsibility of the United States Department of Agriculture (USDA) as well as the Department of Health and Human Services, (HHS). Roughly 20% of the United States' economy falls under this category, which includes any and all infrastructure and facilities for restaurants, grocery stores, food manufacture, processing and shipping, as well as cold storage and refrigeration. This sector remains almost exclusively under private ownership, outside of government regulation and authority.

Critical assets of the Food and Agriculture Sector currently includes all places of food manufacture and processing, the transportation infrastructure including all cold-storage vehicles and

distribution points, as well as final customer delivery sites such as restaurants, hotels, and others included in the Commercial Sector.

In a 2016 report published by the Food and Drug Administration (FDA) in conjunction with the United States Department of Agriculture (USDA), the threats facing the Food and Agriculture Sector increased dramatically with the introduction of "smart farming", or the applications of precision-guided agricultural technologies. "Smart farming" is a method of rural land use that enables a sustainable return, based on the availability and yield of crops on a rotational basis, using advanced satellite-based technologies such as Global Positioning Systems (GPS), false-color imaging, and a slew of related technologies in order to increase a farm's real-time situational awareness, and determine such land features as precision topography, organic matter content, nitrogen levels, projected crop yield in a given season, pH balance, etc.

Having such technologies available will of course increase the chances of a cyber threat agent maliciously act upon and manipulate the findings of these coordinated technologies, not to mention the exploitation of the devices themselves. The results of such hacking could be disastrous for a rural-based agricultural community, as well as the network for which the farmer's smart tools communicates with around the world. Motives for hacktivists of precision-based "smart farming" might include the protest of genetically modified crops, for example, lest we forget the willpower of a malicious hacker from the Ukraine with lots of spare time on his hands. (“Smart Farming”)

Cybersecurity motives for the conversion of routine agricultural processes such as traditional farming to smart farming come at a price. Any as-of-yet undisclosed vulnerability within the smart farming toolkits provided by such top manufacturers as John Deere, Caterpillar,

AGCO Corporation and others are subject to exploit and data manipulation, with unknown results. In this case, we see that the environmental sustainability methods as exemplified by smart farming actually increases, rather than decreases, the risk for exploitation. This is in sharp contrast to trends displayed by such sectors as Energy and Water Treatment. ("Smart Farming")

XI. The Government Facilities Sector

The Governmental Buildings Sector currently consists of a large portfolio of buildings and facilities, located within the United States as well as overseas, either leased or owned by local, state, federal, as well as tribal governments. Uses of these facilities include commercial business use, official state events, scientific research and study, among other uses. Critical assets of military installations, courthouses, labs, as well as embassies include computer equipment, servers, network infrastructure, as well as any data or transactional paperwork that serves as a primary function of the facility, for example any lab equipment or samples. In a cyber context, CI will include physical protection elements such as secured key card locks, mantraps, closed circuit television, access control systems, as well as the people and supporting agents (bomb sniffing dogs for example) assigned to protect such facilities, and who may possess operational knowledge of the layout or functioning of these facilities and/or systems.

Threats to government-run facilities, federal buildings and other supporting infrastructure such as associated parking garages, interconnecting roads, or security checkpoints are subject to similar threats as other commercially-run facilities, magnified to a certain extent due to the direct association of the federal government of the United States, and the authority of our country's place

in the world community. This is none more apparent than on overseas mission work, with military installations, sea-based resources, aircraft, diplomatic infrastructure, and each visiting official to any number of countries at any time under constant threat.

That said, cyber-related threats include the manipulation of classified information on government-run servers, the integrity of the servers themselves, embedded encryption technologies employed, as well as the many roles that information technology plays out with the physical assets mentioned above. (U.S. Government Accountability Office, 2015)

Sustainable alternatives as well as cybersecurity threats within the scope of government-run facilities will be similar in scope and nature to buildings within the commercial facilities sector. Specific cybersecurity threats to federal complexes and installations have been described above.

XII. The Healthcare and Public Health Sector

The Healthcare and Public Health Sector of the United States consists of public and private facilities designed to defend the economy and public at large from such threats as terrorism, natural disasters, as well as biological and viral outbreaks. Currently, information is shared between the public sector (government-run facilities) as well as private research facilities, as the majority of facilities available are corporately owned. As such, this sector is particularly dependent on related sectors such as Emergency Services sector, the Energy sector, as well as the Information Technology sector for the continuity of service and operations.

Specific critical assets of the Healthcare and Public Health Sector includes health care centers such as large hospitals, small health clinics, retail outlets specializing in the sale of

over-the-counter (OTC) medications and health-related equipment. Other critical assets of the Healthcare and Public Health sector include private research facilities such as those funded by the government, as well as privately-owned research facilities such as those found in academia and large universities, including of course medical campuses such as Harvard Medical School, the National Institutes of Health, Johns Hopkins, The Mayo Clinic, The Texas Medical Center (currently the largest medical center in the world), as well as a plethora of other campuses.

Threats to the national healthcare sector include the protections of patient data as guaranteed by the Health Insurance Portability and Accountability Act (HIPAA) of 1996. These protections include the confidentiality, integrity, and availability of a patient's medical data, made available to any physician or doctor of the patient's choosing, Power of Attorney notwithstanding. Because of the sensitivity of any medical data, threats include improper, accidental or premature disclosure to any third party. Other examples of cybersecurity risks to the healthcare field include the physical security that surrounds any medical center, in addition to the business continuity deployment and resources plan of action that a healthcare may choose to employ, in the event of an attack or data breach. (“How Can I Protect Healthcare”)

Environmental considerations and enhancements to healthcare facilities will be similar in scope and nature to those of the Commercial Facilities sector, with the major exception of any specific requirements that directly affect daily operations in such organizations as hospitals and clinics. Similar methodologies of isolated backup power grids fueled by renewable technologies such as solar cells are recommended and encouraged.

XIII. The Information Technology Sector

The Information Technology Sector, as defined within the scope of the Department of Homeland Security, encompasses all hardware and software solutions that serve the public in a noncommercial manner, that is to say, outside the scope of private commercial activities within the United States. Together with the Communications Sector, the Information Technologies Sector also includes networked activity, including the Internet.

Since the early days of post-WWII computational development (i.e. IBM Automatic Sequence Controlled Calculator (ASCC), a.k.a. Harvard "Mark I") mainframes, terminals and networks were built with speed and convenience at the forefront of design considerations. Programmers and hardware vendors were anxious to make a profit selling software and hardware solutions either bundled together (as in the case of Apple) or separately (Microsoft et al).

As a result of a rapid worldwide growth adoption rate of computational power within the twentieth and twenty-first centuries, we risk the confidentiality and security of all data contained therein. This is primarily due to a lack of consideration of security-related technologies that will ensure the confidentiality, integrity and availability of data. Certain risk management strategies included maintaining an offline backup solution, but in order to perform transactional data effectively, we need network connectivity of some kind. These security strategies persist today, from the prohibition of external USB thumb drives, to the adoption of "air gaps", or physical distance maintained between terminals, wifi or bluetooth notwithstanding.

As we know from recent cybersecurity coursework here at Webster University, there is much to learn from previous mistakes. From the leaking of consumer credit card data in 2013, to

the threats of Russian espionage with the presidential election of 2016, the cybersecurity professional must ultimately ensure that confidentiality and integrity of data be maintained, while balancing the availability of this data to relevant parties. ("High Technology Sector - Cyber Security Briefing")

In conjunction with the communications sector, the information technology sector will benefit from the adoption of sustainable and renewable sources of power sources, as well as creative ways that various components of hardware utilize this electrical power. For example, Google Green was created as part of a larger effort by Google to minimize expenditures associated with Google's power consumption and data server farms located around the world. In addition to that primary mission, a larger goal is to produce and sell clean energy. As part of the author's explorations into the Energy Sector's sustainability activities, funding takes place primarily through a nonprofit Google.org. From their powerful example, we can see a correlating trend whereby investments in clean energies result in reliable sources of fuel for the nation's information technology infrastructure, resulting in an improved cybersecurity readiness posture. Similar cross-investments continue to persist across other technology giants such as Microsoft, Apple, Facebook, Samsung and Dell. ("Environment")

XIV. The Nuclear Sector

The Nuclear Reactors, Materials, and Waste sector consists of all equipment and facilities charged with the primary task of obtaining, storing, operating, gaining energy from, and proper disposal of nuclear-based materials and fuels. At present, the national power grid is comprised of

ninety-nine privately-owned commercial nuclear power plants, accounting for approximately one-fifth (20%) of the nation's power consumption, (cue The Simpsons...)

However, nuclear power plants are only a part of the overall picture for this sector. Radioactive elements used in postgraduate academic lab research, for example, allow scientists to study hazardous materials for medical as well as industrial use. Practical uses of radioactive materials include radiopharmaceuticals, [Strontium 89 (Metastron®), samarium 153 (Quadramet®), and Radium- 223 (Xofigo®) for bone metastases or bone tumors, for example], as well as the proper sterilization of basic medical equipment such as surgical and blood transfusion devices and tools. Due to the nature of transporting storing spent nuclear fuels (usually by rail), close coordination with the Transportation Systems sector is imperative.

Cybersecurity threats as they pertain to the worldwide nuclear power plant industry remain a serious risk due to a number of inherent risks with the manufacture, operation and disposal of nuclear- and radioactive-based materials available today. Landmark disaster events such as Three Mile Island (1979) and Chernobyl (1986) highlight the results of improper violations of policy-based safeguards in place at the time. Any terrorism event whose plan would encompass usage of a radiological dispersal device (RDD) in conjunction with traditional chemical explosives such as Trinitrotoluene ("TNT") as a payload device planted inside a nuclear facility would put countless lives at risk. In addition, such "dirty bombs" would jeopardize surrounding communities for decades, if not centuries, before human life were able to resume as before. (Backgrounder on Cyber Security).

Unfortunately there is no alternative towards energy compliance other than conservative use of Thorium-based nuclear fuels (including isotope Uranium-233, Plutonium-239, and Uranium-235) in order to generate the power required to maintain a community's electrical needs going forward. This is due to the powerful nature of radioactive isotopes used in the production of nuclear energy. Enriched Uranium isotopes are built for weapons-grade materials, as their potential for radioactive decay is slower, resulting in more long term damages.

That said, the production quantities of raw energy input needed to generate fusion (inspired by natural fusion activity on the Sun) have not been developed to a significant level of mass production yet as of this writing. Fusion energy (whether fuel sources be derived from Deuterium, Tritium, or Helium) is much more sustainable, as no materials are lost or wasted in the conversion from mass to energy. One may think of the fusion process as a self-rebooting mechanism: One needs an initial input of energy to convert mass into more energy, and we have not gotten there yet, however ETA estimates range from 2020 to 2030. (Should We…)

Significant security protocol and procedures must continue to be implemented at nuclear and fusion sites, due to obvious factors. Safeguards include the restriction of airspace around plants, safety drills, surveillance and increased vigilance post-9/11. (Backgrounder on Cyber Security).

XV. The Transportation Systems Sector

The Transportations Systems economic sector currently consists of all motor vehicle roadways, passenger and freight railways, commercial airports and airways, seaports, pipelines,

international shipping lanes (portions thereof within the national border), and of course domestic and international parcel post and shipping. This sector remains a vitally important component of most industries including tourism, aerospace, financial, construction, defense and arms, etc. Therefore critical assets will include most components of this sector consisting of physical infrastructure, personnel, as well as supporting technologies (ranging in everything from local street stoplights to airport runway lights, to data networks that make these systems operate smoothly.

Roads, railroads, bridges, tunnels, airports, seaports and all other manner of physical transportation all face a similar danger of integrity not unlike a pipeline or data network line or node. The public expectation that the vehicles involved are able to withstand a reasonable level of external interference from such sources as severe weather, natural topology/geology, and reconstruction of the infrastructure due to natural wear and tear over time. Vulnerabilities include bottlenecks caused by construction or rush hour traffic which would cause a large volume of vehicles to accumulate within minutes, perfect for a timed attack. Most notable is a 2015 demonstration of a jeep on a highway, attacked with a barrage of electronic signals which interacted with a central supervisory control and data acquisition (SCADA) system, eventually disabling the vehicle on I-64 here in St. Louis. (Greenberg, A).

Companies and startups such as Solar Roadways are changing the way the country views its national roadway infrastructure. They manufacture solar panels, durably built for roadway use, replacing asphalt and concrete as a primary roadway and runway application, (As of this writing, the panels are fit for small airports and small airplanes, but require further testing for the demands of an international airport.) This would affect both the Energy Sector, as well as the Transportation

Sector, again reducing our dependence on foreign petroleum products, which is known to cause excess CO2 emissions, while increasing our cybersecurity posture with real-time data about our roadways and runways. (Pave The Way…)

We are most subject to attack when nodes cluster, such as in a traffic system in a major city. Therefore my recommendations begin with a stronger onion-like multilayered protection model in major hubs and destinations, while not neglecting the absence of protections in rural areas in order to simply gain access to major centers. As stated, these protections would include a multilayered approach of detection tools in order to reduce the threat of explosive devices, or other hardware, (timed, computational or otherwise), that would endanger the public safety during a time of high travel volume, such as the end-of-year holidays.

XVI. The Water and Wastewater Systems Sector

The Water and Wastewater Sector consists of all networked infrastructure and pipeline systems that carry both freshwater, greywater and wastewater to and from our industrial centers, residences and commercial places of business. This sector also includes all facilities to filter, treat, store and deliver water services from said facilities. Ensuring a clean supply of water as well as a continuity of wastewater treatment in all communities is essential to human development as a whole. Therefore critical assets of the Water and Wastewater Sector consists of the water itself, all routing of pipes and gateways, environmental levees, etc. Close coordination with the Dams Sector is essential for the safe management of water supply.

Threats to a major water supply plant include (1) contamination by a chemical or biological agent of raw drinking supply, (2) the inability to treat water suitable for drinking, (3) chemical or biological pollution to the environment, and (4) damage to plant infrastructure. Threats to a major wastewater plant differ slightly than threats to a water plant, but include the following principal differences: (1) contamination by a chemical or biological agent as an output stream to local rivers or basins/bays, and (2) the inability to treat wastewater. (Goodwin, A.)

Contamination of inbound water treatment threats, once found, follow a systematic protocol: isolation and sanitation. If pipelines are found to be corrosive, they are scheduled to be replaced. With the case of wastewater, contamination usually takes the form of not meeting clean wastewater quality standards during a certain stage of the treatment process. Lastly, in the event of sabotage, either by a malware agent or rogue former employee, the plant is shut down, backup plants are called to action upstream and downstream, until such time the original plant can be safely restored to public service. (Water System Security…)

As we've seen, a number of industrial sectors stand ready to withstand a potential cybersecurity attack with inherently lesser risk than most sectors defined. Others have significant areas of opportunity to grow their defenses, as well as reinforce their incident management, disaster recovery and business continuity models. Overall, the research does indicate a gradual level of improvement among sectors over time, but we as a global society do need to have a greater appreciation for the cybersecurity of our networks, devices and infrastructure. If and when we do, the impact and damages of data breaches, political conflicts, and environmental best-practices,

should be minimized, as it should have been from the beginning of the computing and industrial era.

References

Backgrounder on Cyber Security. (2016, October 12). Retrieved December 5, 2016, from http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html

Boeing; et al. (2014). "LEED-ND and Livability Revisited". *Berkeley Planning Journal*. 27: 31–55. Retrieved 2016-10-15.

Chemical Sector. (n.d.). Retrieved December 2, 2016, from https://www.dhs.gov/chemical-sector

Chuck, H. (2015, December 1). Chuck Hagel: Climate Change Is a National Security Problem. *Time Magazine*.

Clarke, R., & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it.* New York: Ecco.

Commercial Facilities Sector. (n.d.). Retrieved November 27, 2016, from https://www.dhs.gov/commercial-facilities-sector

Critical Manufacturing Sector. (n.d.). Retrieved October 21, 2016, from https://www.dhs.gov/critical-manufacturing-sector

Dams Sector. (n.d.). Retrieved December 2, 2016, from https://www.dhs.gov/dams-sector

Defense Industrial Base Sector Sector. (n.d.). Retrieved December 2, 2016, from https://www.dhs.gov/defense-industrial-base-sector

Deloitte Center for Financial Services. "Evolving cyber risk in commercial real estate: What you don't know can hurt you" (2015, February 25). Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-dcfs-cre-cybersecurity-051315.pdf

DoD's Defense Industrial Base Cybersecurity Information Sharing Program. (n.d.). Retrieved December 2, 2016, from http://dibnet.dod.mil/

Emergency Services Sector. (n.d.). Retrieved December 2, 2016, from https://www.njhomelandsecurity.gov/analysis/emergencyservices

Energy Sector. (n.d.). Retrieved December 2, 2016, from https://www.dhs.gov/energy-sector

Environment. (n.d.). Retrieved November 15, 2016, from https://www.google.com/green/

Executive Order -- Commission on Enhancing National Cybersecurity. (2016, February 09). Retrieved December 2, 2016, from https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity

Granville, K. (2015, February 5). 9 Recent Cyberattacks Against Big Businesses. Retrieved December 2, 2016, from http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html

Goodwin, Angela. Retrieved December 3, 2016, from http://www.waterworld.com/articles/print/volume-28/issue-4/editorial-features/water-and-wastewater-cyber-security-strengthening-the-chain.html

Green Telecom | Sustainable Communication. (n.d.). Retrieved October 21, 2016, from http://greentelecom.co.uk/business-insight/sustainability/

Greenberg, A. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway-With Me in It. Retrieved December 8, 2016, from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Hess, G. (n.d.). Boosting Cybersecurity. Retrieved December 2, 2016, from http://cen.acs.org/articles/91/i11/Boosting-Cybersecurity.html

High Technology Sector - Cyber Security Briefing | Deloitte | Analysis. (2016). Retrieved December 7, 2016, from https://www2.deloitte.com/nz/en/pages/risk/articles/High-Technology-Sector.html

How Can I Protect Healthcare and Public Health Infrastructure. (n.d.). Retrieved December 3, 2016, from http://www.phe.gov/Preparedness/planning/cip/Pages/protect.aspx

I. (2015). What is the telecommunications sector? Retrieved December 2, 2016, from http://www.investopedia.com/ask/answers/070815/what-telecommunications-sector.asp

Kepler, David, E. The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting our National and Economic Security" (2013, March 7). Retrieved from https://www.americanchemistry.com/policy/security/dow-testimony-at-joint-senate-hearing.pdf

Krancer, Michael. (2015, Nov 4). "The Biggest Cybersecurity Threat: The Energy Sector". Retrieved 2 Dec. 2016 from http://www.forbes.com/sites/michaelkrancer/2015/11/04/the-biggest-cybersecurity-threat-the-energy-sector/#5cf092f160ba

LeClair, J., & Ramsay, S. W. (2015). *Protecting our future: Educating a cybersecurity workforce*. Albany, NY: Hudson Whitman/Excelsior College Press.

McLaughlin, K. (2016, March 8). Critical Manufacturing – Implementing a CSDP. Retrieved October 21, 2016, from http://www.nationalcybersecurityinstitute.org/general-public-interests/critical-manufacturing-implementing-a-csdp/

Morganwalp, D. W. (n.d.). Agricultural Chemicals. Retrieved December 2, 2016, from http://toxics.usgs.gov/topics/agchemicals.html

Olenick, D. (2016, September 19). Energy sector cybersecurity workers overconfident in their capabilities. Retrieved December 2, 2016, from https://www.scmagazine.com/energy-sector-cybersecurity-workers-overconfident-in-their-capabilities/article/530118/

P. L. Xue, X. F. Sun, Y. Song, Y. J. Cheng, D. Z. Sun, "Risk Prevention and Emergency Countermeasures to Environmental Accidents of Chemical Industry Parks", Advanced Materials Research, Vols. 726-731, pp. 798-803, 2013

Redesigning defense: Planning the transition to the future U.S. defense industrial base. (1991). Washington, DC: US Gov. Print. Off.

Rohrlich, J. (2011). Chinese Cyber Spying Hits Chemical and Defense Firms. Retrieved December 2, 2016, from http://www.minyanville.com/businessmarkets/articles/Corporate-Espionage-dow-chemical-DUPONT-chemical/11/1/2011/id/37710

Rojas, A. (n.d.). Alternatives for Including Environmental Issues in the Financial Sector . Retrieved December 2, 2016, from http://www.incae.edu/EN/clacds/publicaciones/articulos/cen772.php

Rosenfield, Everett, H. (2015, April 8). "AT&T data breach revealed: 280K customers exposed." Retrieved December 2, 2016, from http://www.cnbc.com/2015/04/08/att-data-breaches-revealed-280k-us-customers-exposed.html

"Should We Consider Using Liquid Fluoride Thorium Reactors for Power Generation?", *Environmental Science & Technology*, July 6, 2011

Solar Roadways Specifics. (n.d.). Retrieved December 2, 2016, from http://www.solarroadways.com/Specifics/Electrical

Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit Washington, D.C., 112th Cong. (2011) (testimony of Gordon M. Snow).

Trench, N. J., & Wieder, M. A. (n.d.). *Funding Alternatives for Emergency Medical and Fire Services*(United States, Department of Homeland Security, U.S. Fire Administration) (C. Finkle, Ed.). FA-331/April 2012

United States, Department of Homeland Security. (2015). Retrieved October 21, 2016, from http://www.water.ca.gov/damsafety/docs/dams-sector-security-guidelines-2015-508.pdf

United States, Federal Bureau of Investigation, Cyber Division. (n.d.). *Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector*(pp. 1-6).

United States, Government Accountability Office. (2015). *CRITICAL INFRASTRUCTURE PROTECTION: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*(pp. 1-82).

U.S. sees jump in cyber attacks on critical manufacturers. (2016, May 13). Retrieved October 14, 2016, from http://www.reuters.com/article/us-usa-cybersecurity-infrastructure-idUSKCN0UT23U

Walsh, J. (2011, June 22). Under the Arctic Ocean, a Great Sea of Oil Awaits; Greens Fear the Push for Black Gold. *The Washington Times*. Retrieved November 16, 2015, from http://www.highbeam.com/doc/1G1-259488978.html

Water System Security and Resilience in Homeland Security Research. (n.d.). Retrieved December 2, 2016, from https://www.epa.gov/homeland-security-research/water-system-security-and-resilience-homeland-security-research

(n.d.). Pave the way for solar panel roads? - Yale Climate Connections. Retrieved December 2, 2016, from http://www.yaleclimateconnections.org/2016/12/pave-the-way-for-solar-panel-roads/