**1. Please define what "Cyber Infrastructure" is? Please define what "Critical Infrastructures" are? (5 points)**

Cyber Infrastructure is a federal research term to describe any IT systems that have or could have the capability to be powerful. cyberinfrastructure is a solution to the problem of connecting computers, and people. Like data storage, data management, data mining, the internet, and other computer services distributed over the internet. [1] The key is to make use of advanced information technology systems easy to use.

Critical Infrastructures are the foundation essential services that sustain American Society, Economy, Security, and Health. There are 16 critical infrastructure sectors Chemical, Commercial Facilities, Communication, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food/Agriculture, Government Facilities, Healthcare/Public Health, Information Technology, Nuclear Reactor/Materials/Waste, Transportation Systems, and Water/Waste Water Systems. These sectors work together to sustain the greater whole. Each one of these sectors falls into one or more of the essential services I talked about earlier. [2]

**2. You need to spend some time researching on the Internet and/or any other resources to find out some real-world Cybersecurity projects related to Cyber Infrastructure and Critical Infrastructure. After conducting your research, please list and briefly describe (1)FOUR real-world Cyber infrastructure security project cases, and (2) FOUR critical infrastructure security project cases respectively. (30 points)**

**1.**

<https://www.sans.org/reading-room/whitepapers/casestudies/case-study-home-depot-data-breach-36367>

The Case Study: The Home Depot Data Breach is a case study about the large amount of payment card information theft at Home Depot in 2014. Customers that had used a payment card at Home Depot as far back as April of 2014 is vulnerable of having their card information stolen. Thank goodness I was on my mission for the later part of 2014, and I dont shop at Home Depot very often. Similar to the [Target data breach of 2013.](http://www.nbcnews.com/tech/security/target-reaches-settlement-visa-over-2013-data-breach-n412071) [3]They explained how after the card information was stolen they use the information on the card to buy gift cards at major stores to buy items and they usually resale these items to gain a profit. This process is very difficult to track. several ways Home Depot and Target plan to prevent future attacks, chip and pin cards, Mobile payments, point to point encryption, anti virus with HIPS Capabilities, POS network on it’s own private VLAN, USB port blockers, and getting rid of Windows XP machines. How the hackers obtained this information was through an outside vender, and planted malware that records the ram data off of a POS terminal while the payment data is in clear text.

<https://www.sans.org/reading-room/whitepapers/casestudies/phish-33139>

The article Inside a Phish is an case study about an phishing campaign. A search warrant was executed by law enforcement at a ISP on the phishing emails senders email address. Which lead to some insights revolving around this phishing campaign. “A phish is a fraudulent message that attempts to impersonate an institution that you have a relationship to get you to provide personal information or to perform a desired action.”- SANS Definition. The emails were obtained through PHP scripts gathering email addresses. These PHP scripts are used to gather other useful information like name, address, payment info, past information, and other relatable information. The key is to gather as much information as possible to be more credible in the email. these emails are emailed in masses to as many people as possible. How to [prevent phishing](http://www.identitytheftkiller.com/prevent-phishing-scams.php) [4] to be successful is educating people, always be hesitant to emails asking for personal information, never click links, beware of popups, protect your computer, check online accounts often, and communicate personal information via phone or secure websites.

<https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412>

The article Critical Controls that Could Have Prevented Target Breach is a case study on How target was hit in December of 2013 with over 40 million credit cards being stolen from 2000 Target stores by accessing the data off of POS systems. I touched on this earlier with the Home Depot case study. The same processes in that cases study will help a future data breach. several ways Home Depot and Target plan to prevent future attacks, chip and pin cards, Mobile payments, point to point encryption, anti virus with HIPS Capabilities, POS network on it’s own private VLAN, USB port blockers, and getting rid of Windows XP machines. The Target Breach is a prime example of why companies need to keep uptodate with current attacks, and how to prevent them. If Home Depot would have learned from Targets data breach then they would have prevented the attack in the first place.

<https://www.sans.org/reading-room/whitepapers/casestudies/home-securing-internet-cafes-whie-maximizing-customer-freedom-1519>

The article Away from home. Securing Internet Cafes While Maximizing Customer Freedom is about security on open wifi networks, the specific example was internet cafe’s. This article addresses five different aspects to running a safe secure open internet environment network design, Private information protection, building and deploying ghost images, antivirus concerns and implementation, and billing software and its role in increasing physical security. Some things you can do to improve your security on a company's network is implement an Intrusion Detection System, firewalls between the gateway and internet, closing all the non needed ports, keep the POS off the guest network, caching proxy for web and ftp traffic(ISA Server), protect physical access to the network, and implement antivirus. How as a user on an open network can protect themselves is turn off sharing, enable firewalls, use https and ssl, use a VPN with an SSL encryption, turn off any connections that you aren't using, use antivirus, keep you patching uptodate, forget unused networks, and two factor authentication. [5]

**2.**

<https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Incorporating-Resilience-into-CI-Projects-508.pdf>

The article Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects is an article on how to support development and investments in a infrastructure which will increase the durability of a critical infrastructure system. This case study lists several different ways to promote resilient infrastructure investments are projected climate change impacts, measure both direct and indirect costs and benefits, examining demographic trends, looking at the best available data, referring to science and predictive tools, considering applicable standards and best practices, doing a vulnerability assessments, performing a risk assessment and scenario planning tools, Identifying key dependencies and interdependencies, finding potential cascading effects, knowing the regional landscape, developing an incident response plan, building redundancy, budgeting migration if needed, environmental buffers, and ensuring there are manual overrides and physical backups. This Supplemental tool is very self evident, or quite obvious. The only thing I found interesting is the section about natural environmental buffers being incorporated into an infrastructure design to mitigate natural disasters.

<https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf>

This cases study the National Infrastructure Protection Plan(NIPP) is is a developed national plan to unify and enhance critical infrastructure and key resources protection efforts through the private sector, federal, state, and local government to provide identification, prioritization, and protection to these key infrastructures. The national infrastructure protection plan establishes national priorities, goals, and requirements so that “Federal funding and resources are applied in the most effective manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents...and addresses the physical, cyber, and human considerations required for effective implementation of comprehensive programs.” The national infrastructure protection plan also puts in place a risk management system that defines roles and responsibilities for each department, agency, government office, and private sector partners. The thing I liked most is that looking through this comprehensive plan(There is a lot in this article to comprehend) but everything seems to be based on a hierarchy system that loops from top to bottom.

<https://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf>

This is the specific NIPP for the Healthcare and Public Health Sector. This is the detailed plan for what the Health sector lays out the process to protect from natural disasters, pandemics, terrorist attacks, and other manmade disasters. Same as the NIPP I addressed earlier this plan addresses the processes set in place to identify and prioritize assets, assess risk, implement protective programs, and measure the effectiveness of its protective programs. what I found interesting was that one of the health sector's goals are to mitigate cybersecurity risk. I think that is amazing that cybersecurity concerns are not just in the information technology sector but is in every sector it is a concern.

<http://www.dhs.gov/sites/default/files/publications/nipp-ssp-commercial-facilities-2015-508.pdf>

This is the specific NIPP for the Commercial Facilities Sector. This sector addresses many different facilities privately owned, operate with minimal regulations, and house the business activities and U.S. economy. These facilities are involved with entertainment, Media, Gaming, Lodging, Outdoor Events, Public Assembly, Real Estate, Retail, and Sports Leagues. The things that they are concerned about is Natural disasters, armed attacker and terrorist threats, pandemics, theft, supply chain, social implications, and geopolitical problems. Same as the NIPP I addressed earlier this plan addresses the processes set in place to identify and prioritize assets, assess risk, implement protective programs, and measure the effectiveness of its protective programs. also what I found interesting was that one of the commercial sector's goals are to mitigate cybersecurity risk. I think that is amazing that cybersecurity concerns are not just in the information technology sector but is in every sector it is a concern. This plan was put together really well, I liked it the most because of the graphs and how it was put together really easy to read.

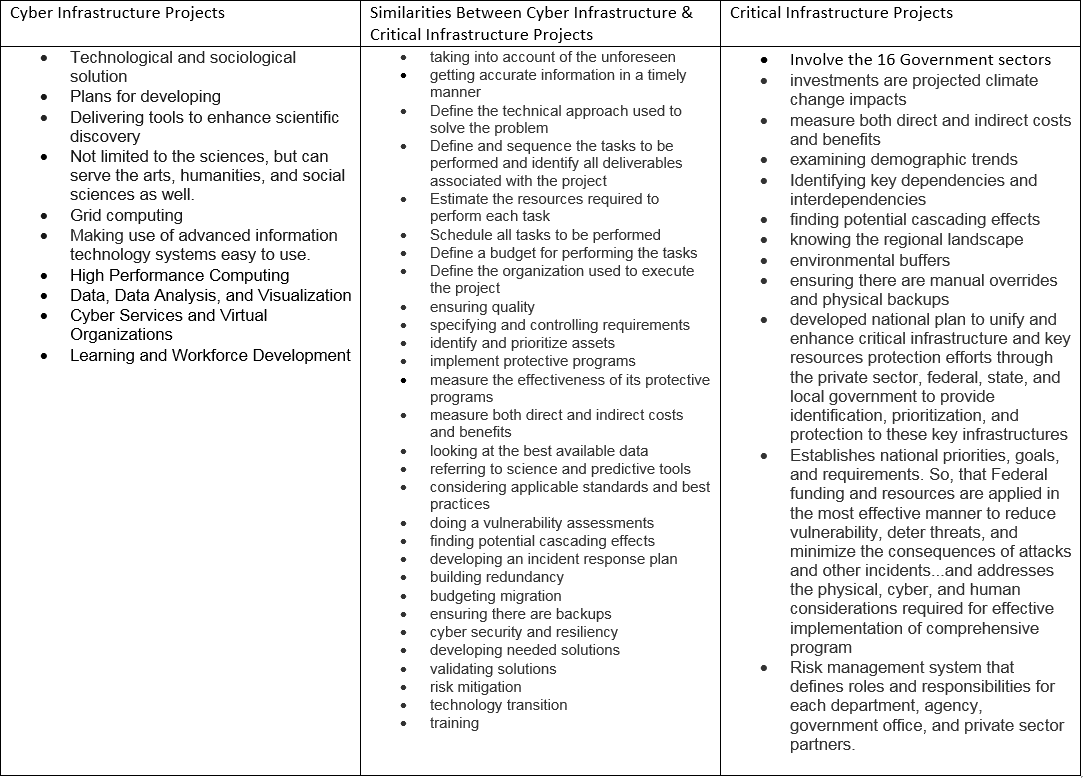
The below graph is a graph of the commercial facilities sector goals and priorities which summarizes everything quite nicely:



The below graph is a graph of the commercial facilities sectors snapshot of assets and impacts:



**3. Based on what you discovered in #2, create a table to compare similarities and differences among these projects and identify the relationships between "Cyber Infrastructure" and "Critical Infrastructures" security projects. (30 points)**



|  |  |  |
| --- | --- | --- |
| Cyber Infrastructure Projects | Similarities Between Cyber Infrastructure & Critical Infrastructure Projects | Critical Infrastructure Projects |
| · Technological and sociological solution  · Plans for developing  · Delivering tools to enhance scientific discovery  · Not limited to the sciences, but can serve the arts, humanities, and social sciences as well.  · Grid computing  · Making use of advanced  information technology systems easy to use.  · High Performance Computing  · Data, Data Analysis, and Visualization  · Cyber Services and Virtual Organizations  · Learning and Workforce Development | · taking into account of the unforeseen  · getting accurate information in a timely manner  · Define the technical approach used to solve the problem  · Define and sequence the tasks to be performed and identify all deliverables associated with the project  · Estimate the resources required to perform each task  · Schedule all tasks to be performed  · Define a budget for performing the tasks  · Define the organization used to execute the project  · ensuring quality  · specifying and controlling requirements  · identify and prioritize assets  · implement protective programs  · measure the effectiveness of its protective programs  · measure both direct and indirect costs and benefits  · looking at the best available data  · referring to science and predictive tools  · considering applicable standards and best practices  · doing a vulnerability assessments  · finding potential cascading effects  · developing an incident response plan  · building redundancy  · budgeting migration  · ensuring there are backups  · cyber security and resiliency  · developing needed solutions  · validating solutions  · risk mitigation  · technology transition  · training | · Involve the 16 Government sectors  · investments are projected climate change impacts  · measure both direct and indirect costs and benefits  · examining demographic trends  · Identifying key dependencies and interdependencies  · finding potential cascading effects  · knowing the regional landscape  · environmental buffers  · ensuring there are manual overrides and physical backups  · developed national plan to unify and enhance critical infrastructure and key resources protection efforts through the private sector, federal, state, and local government to provide identification, prioritization, and protection to these key infrastructures  · Establishes national priorities, goals, and requirements. So, that Federal funding and resources are applied in the most effective manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents...and addresses the physical, cyber, and human considerations required for effective implementation of comprehensive program  · Risk management system that defines roles and responsibilities for each department, agency, government office, and private sector partners. |

An Interesting article by nbc on the differences between cyber infrastructure and critical infrastructure. [[7]](http://www.nbcbayarea.com/news/local/Critical-Infrastructure-Vulnerable-to-Cyber-Attacks-Experts-Warn-290370921.html)

An Research project on cyber security and global interdependence: What is critical? [[8]](https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf)

**4. Furthermore, you need to answer the following question (25 points):**

**As a project manager, what is your opinions about differences between a general IT software project planning and a Cyber infrastructure and/or Critical Infrastructure Security project planning?**

I think the differences between general IT Software Projects and Cyber Infrastructures planning is the scale or the scope of each project. How big a project is and what the effects of the project is what makes the difference. Honestly other than that there is not much difference in how you as a project manager should plan both of these. Now the differences between Critical Infrastructure Security and a General IT Software projects are completely different. Critical infrastructures are on a grander scale, they encompass several agencies, Departments, governments, and even the private sector taking into account the safety and well being of every citizen. Just look at the NIPP’s critical infrastructure project. Each one of these are taken into account when planning. An IT software project should only be planned with the customers and companies best interest in mind. So, the differences are scale.

**What would be a good roadmap to plan a Cybersecurity related project (e.g., security product project, or security infrastructure project, etc.) to avoid potential project risks and failure?**

We learned in the previous discussions why projects fail, That project fail because of poor planning, not taking into account of the unforeseen, not getting accurate information in a timely manner, and the fear of failure. We can learn from this as a Project Manager we need to take all of these reasons for failure and use them in preventing current projects potential projects risk and failures. The one thing I learned from this assignment is that we need to be aware of current risks into today's world and plan accordingly. Like with the target and home depot incidents of card information being stolen from POS systems, Home Depot could have taken the information target learned an year earlier and implemented those same preventive measures into their system and maybe they would have prevented an attack. Project managers need to have certain skills to succeed organized, good multi tasker, ability to take change, know how to lead, know how/when to negotiate, detail oriented, have the ability to see problems and solve those problems quickly, and have the technical background/skill. I think with all these abilities is what makes the difference in a not only a cyber security related project but all potential projects to be successful.[6] I would like to say that I believe that every project good or bad has risk involved.

**Feel free to use Internet and any other resources to explore this question and draft your thoughts with a good logical flow.**

**5. Please reply to one of your peers' postings with supporting evidence/materials. (10 points)**

***Note: please use standard APA style to list your references.***

**Cited Works:**

* Indiana University Indiana University Indiana University. (2015, August 20). Retrieved January 22, 2016, from https://kb.iu.edu/d/auhf
* Homeland Security. (2016, January 08). Retrieved January 22, 2016, from http://www.dhs.gov/what-critical-infrastructure
* Eng, J. (2015, August 18). Target Reaches Settlement With Visa Over 2013 Data Breach. Retrieved January 22, 2016, from http://www.nbcnews.com/tech/security/target-reaches-settlement-visa-over-2013-data-breach-n412071
* Are You Phishing For Trouble? These 8 Ways To Prevent "Phishing Scams" Will Keep You From Getting Wet. (n.d.). Retrieved January 23, 2016, from http://www.identitytheftkiller.com/prevent-phishing-scams.php
* 9 Tips to Stay Safe on Public Wi-Fi. (n.d.). Retrieved January 23, 2016, from http://www.laptopmag.com/articles/9-tips-to-stay-safe-on-public-wi-fi
* Schiff, J. (2013, January 15). 7 Must-Have Project Management Skills for IT Pros. Retrieved January 23, 2016, from http://www.cio.com/article/2389129/project-management/7-must-have-project-management-skills-for-it-pros.html
* N. (2015, February 01). Critical Infrastructure Vulnerable to Cyber Attack. Retrieved January 23, 2016, from http://www.nbcbayarea.com/news/local/Critical-Infrastructure-Vulnerable-to-Cyber-Attacks-Experts-Warn-290370921.html
* Clemente, D. (2013, February 01). Cyber Security and Global Interdependence: What Is Critical? Retrieved January 22, 2016, from https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International Security/0213pr\_cyber.pdf
* Inside a Phish. (n.d.). Retrieved January 23, 2016, from https://www.sans.org/reading-room/whitepapers/casestudies/phish-33139
* The Case Study: The Home Depot Data Breach. (n.d.). Retrieved January 23, 2016, from https://www.sans.org/reading-room/whitepapers/casestudies/case-study-home-depot-data-breach-36367
* Critical Controls that Could Have Prevented Target Breach. (n.d.). Retrieved January 23, 2016, from https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412
* Away from home. Securing Internet Cafes While Maximizing Customer Freedom. (n.d.). Retrieved January 23, 2016, from https://www.sans.org/reading-room/whitepapers/casestudies/home-securing-internet-cafes-whie-maximizing-customer-freedom-1519
* Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects. (n.d.). Retrieved January 23, 2016, from https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Incorporating-Resilience-into-CI-Projects-508.pdf
* NIPP for the Healthcare and Public Health Sector. (n.d.). Retrieved January 23, 2016, from https://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf
* NIPP for the Commercial Facilities Sector. (n.d.). Retrieved January 23, 2016, from http://www.dhs.gov/sites/default/files/publications/nipp-ssp-commercial-facilities-2015-508.pdf