Cassandra Lalli

Cybersecurity Framework Report

For this assignment New York's Fines will be working with the HITrust framework to both meet compliance and continue to keep our company safe from cyber threats. We will be transitioning from NIST framework with HIPAA regulations to one of those with Hitrust certification and

HIPAA regulations. The CSF contains 14 control categories, comprising 49 control objectives and 156 control specifications. The CSF control categories, accompanied with their respective number of control objectives and control specifications for each category, are

0. Information Security Management Program (1, 1)

1. Access Control (7, 25)

2. Human Resources Security (4, 9)

3. Risk Management (1, 4)

4. Security Policy (1, 2)

5. Organization of Information Security (2, 11)

6. Compliance (3, 10)

7. Asset Management (2, 5)

8. Physical and Environmental Security (2, 13)

9. Communications and Operations Management (10, 32)

10. Information Systems Acquisition, Development, and Maintenance (6, 13)

11. Information Security Incident Management (2, 5)

12. Business Continuity Management (1, 5) 13. Privacy Practices (7, 21)

(HITrust.2020)

The cybersecurity environment

Processes

As it stands, New York's Finest implements a NIST framework. We will be translating this current framework to the HITrust framework. Since the HITrust framework works of response through protocols and ancestors we have created a hybrid solution implementing the ISO, HITrust, and HIPAA requirements. Below is our strategy for implementation.

Information

The HITrust categorizes risk factors into 3 categories organizational Factors, Regulatory Factors, and System Factors this will be outlined in the risk assessment below. From this, we have started planning responses for each factor from high to low in the diagram below.

Systems directly involved in the delivery of services

New York Fines does not deliveries of medical services. Our ambulance is through the government FDNY and Government ambulance. Through this, we work with third-party clients such as solar winds to secure that system. Any medical delivered to on sight facilities is also taken care of through SolarWinds. It was disclosed that there was a cyber breach and solar winds will be securing all aspects of this to us shortly, we have already notified the government authorities that New yorks fines were a part of a said breach as well as state officials and news outlets.

Risk Management Practices

Below are the risk management practices that New York Fines implements to keep our systems up to date as well as secure.

Contingency Planning Process: For our contingency Planning process it is important to identify a chain in command. By doing this we will effectively be outlining who to go to when something happens and who will respond to what. One person in the IT team will be designated to convey all information to the stakeholders for they should be updated as soon as possible. system admins will monitor, along with one member of its team of their choice to make sure all systems are adequately safeguarded. On the first and 15th of the month, a pen test will partake of the companies system the report of findings will be written up and given to the CISCO. the CISCO will then delegate the jobs of Harding systems and making patches throughout the team.

The Data Backup Planning Process: the most crucial part of the backup plan is the data backup. data back up will ensue 3 to four times a week. every Sunday the systems will have a full backup followed by a mirror backup on Monday. Tuesday and Wednesdays are the slowest foot traffic to the hospitals the next backup will be on Friday. if there is abnormal foot traffic at the hospital on Tuesday and Wednesday the mirror backup will take place on Wednesday as well.

The Disaster Recovery Planning Process: For the Recovery Process please see the document labeled Disaster Recovery. this document outlines the recovery process in case of elemental hazards. the four entities the hospital must report to in case of a breach of data and any other problem. it is advised that when a disaster happens in the cyber domain the chief cisco officer must be the first notified. Once notified they will take necessary precautions and report the incident to the rightful parties.

The Emergency Operations Mode Planning: For Emergency Operations all patients must be immediately moved to the closest hospital that is in critical condition. warming blankets will be handed out to all other patients and will then be monitored every 30 mins on the dot. if any signs of their condition are worsening they must be moved to the nearest hospital. this is in case of a ransomware attack and all computers are rendered useless. for any other type of emergency, the wing of the hospital must be closed down and patients must be moved to a new wing of the hospital. the computers in the infected wing will go on a code blackout until the cyber team can assess the problem and deal with it. this must be reported in the first hour of suspicious activity.

Testing and Revision Procedures: Testing will happen twice a month. In this test, the pentester will test all systems to see what needs Harding and what safeguards are adequate. After the pentester is done a member of the IT team will audit the system to see if the new changes reach compliance. one bot has made a written summary of what changes need to be made. The paper will be handed to the CISCO, through his recommendation the task will be distributed throughout the IT team and made within the first 48 hours. Once this is done a system revision document will be written up and given to all stakeholders.

Threat Environment

Hospitals are open to a plethora of threats. It is important to understand all forms of threats below are 2 charts, the first chart is less serious threats. There are threats that are classified as low to mid, with an unlikely to likely range.

Chart 1 (Cassandra, L. 2020)

Potential categories of Threat	Description
Network infrastructure failures or errors	Connection failure Unsecured wireless network Network software failure Network congestion Switch port problems Routers or switches hang
Deviations in quality of service	Minimum technology of transfer (TOT) from contractors and technology vendors
Operational issues	Lack of training for staff System documentation not systematically managed
Communications interception	Spoofing/impersonation due to unsecured network
Masquerading	Insiders Service providers Outsiders
Acts of human error or failure	Entry of erroneous data by staff Accidental deletion or modification of data by staff Accidental misrouting by staff Confidential information being sent to the wrong recipient

	Storage of data or classified information

Chart 1 outlines the lower levels of risk. Each risk has a likelihood of happening but can be dealt with swiftly. This will allow the cyber team to focus on more critical aspects of the risk environment in chart 2.

Chart 2. (Cassandra L. 2020)

Power failure/loss	Server down due to power failure Air-conditioning failure of the server Interruption by the service provider (e.g. electrical department and internet service provider)
Acts of human error or failure	Entry of erroneous data by staff Accidental deletion or modification of data by staff Accidental misrouting by staff Confidential information being sent to the wrong recipient Storage of data or classified information in unprotected areas by staff

Technological obsolescence	Outdated hardware Outdated application software Outdated system software Obsolete network equipment
Hardware failures or errors	Insufficient storage space Hardware maintenance error
Software failures or errors	Application software failure Software maintenance error
Malware attacks (malicious virus, worm, Trojan horses, spyware, and adware)	Embedding of malicious code due to the usage of wireless and mobile technologies Introduction of damaging or disruptive software

In chart 2 these are risks that are on a high level of risk as well as a mid-range in likelihood. Knowing this if any of the above risks are they must have the full attention of the cyber team. If the cyber team is unavailable the company must go into a code blackout. Some threats are and shut down any nonessential hardware, computer, or equipment.

Legal and Regulatory Requirements

The Internet of Medical Things Resilience Partnership Act (2017)

This act is to make a public and private partnership with stakeholders. This acts targets medical equipment and allows transparency when it comes to cyber-attacks along with how to deal with them.

The Medical Device Cybersecurity Act of 2017

This bill amends the Federal Food, Drug, and Cosmetic Act to require the Food and Drug Administration (FDA), in coordination with others, to create a cybersecurity report card for devices that have network or Internet connectivity, connect to an external drive or external media, or have any other cyber capability. Report cards must contain specified information, including: (1) information pertaining to the essential elements described in the most recent version of the Manufacturer Disclosure Statement for Medical Device Security, (2) a cybersecurity risk assessment conducted by the manufacturer or third party, and (3) whether the device is capable of being accessed remotely. A cyber device manufacturer must include a report card in any premarket notification or application for premarket approval. The FDA shall provide a copy of a device's report card if requested by a health care industry entity or an entity with a valid interest in the report card. (Blumenthal,2017)

21st Century Cures Act (Cures Act)

The Curse act covers innovations and advances to patients who need them faster and more efficiently. This makes sure that organizations are securing their patients.

Internet of Medical Things Resilience Partnership Act of 2017

This bill will join public-private partners, allowing for third-parties medical device manufacturers to secure all of their equipment for distribution. These companies will develop their framework for securing systems.

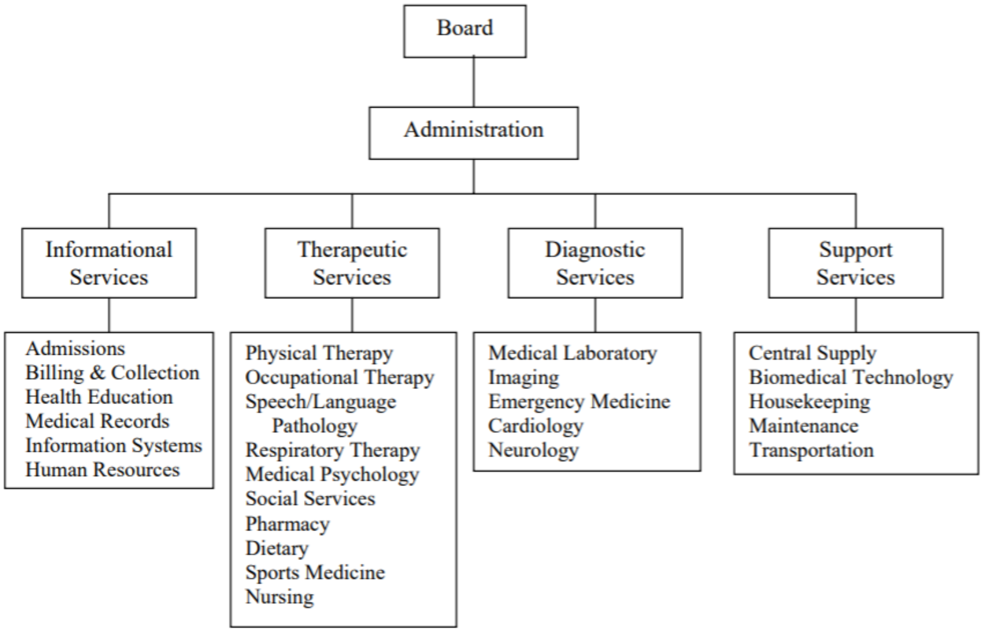
Federal Food, Drug, and Cosmetic Act (FD&C Ac**t)**

This act mostly covers any food or drug distributed in the U.S. but is also covers any equipment sold or used as well. Mostly quality issues but one part that pertains to the Cyber department is the inventory list. All hospitals must have an inventory of any medical equipment that is lost or stolen. This includes computers and laptops owned by the hospital.

Business/Mission Objectives

New yorks finest vision is to open at least one hospital in every state with similar names but the state's name before Finest. It is our goal to provide excellent care to our country, members who serve, and the working class. Cut wait time and allow new doctors and nurses who are new to the industry and promising candidates. As of now New Yorks's finest are in all major cities (California finest, Chigo fines, Trantos fines, Miami Finest..etc) but will be expanding to states without major cities as well. everyone should have affordable health care

Organizational Constraints



Future Cybersecurity Policy Implementations

The critical cybersecurity needs

To reach compliance New yorks fines high-riskimplement the following safeguards as shown by HIPAA. Physical safeguard standards are put in place to enable cybersecurity and privacy measures to operate efficiently, under lock and key. Here are some examples:

- Facility access controls
  - This includes Contingency Operations, Facility Security Plan, Access Control and Validation Procedures, and Maintenance Records.
- Workstation use and security
  - This includes Contingency operation, Facility security plan, Access control, and validation procedures Maintenance records, Standard: Workstation use, standard:

    Workstation security, Standard: Device and media controls, Data backup, and storage.

- Device and media controls
    - This includes disposal, media re-use, accountability, and data backup and storage.

Technical safeguards are enabled to ensure that information is only accessed by authorized personnel and only transmitted over networks securely:

- Access control ensures unique user identification, emergency access procedures, automatic logoff, and encryption and decryption.
- Audit controls focus on hardware, software, and procedural mechanisms for recording and examining activities.
- Integrity controls deal with mechanisms designed to authenticate electronic personal health information (e-PHI).
- Transmission security regulates integrity controls, encryption, and safeguards against unauthorized access of e-PHI during transmission.
- Physical control regulates security measures of Closed-circuit surveillance cameras. Motion or thermal alarm systems.
-

organization's cybersecurity risk assessment to include:

The likelihood of risks occurring and the resulting impact

When taking hospitals into account it is shown that breach incidents are on a rise of 10 percent a year. One of the leading cyber attempts attacks on hospitals is Ransomware attacks. In 2017 hospitals across us were hit with high-profile ransomware and malware attacks, this showed a lack of organizational maturity vulnerabilities and exposure to complex cyber risks.

Several factors were the cause of these cyber risks for the health care sector:

- The industry's rapid adoption of digital systems.
- The emergence of health data as a high-value target for cybercriminals (ie. sensitive patient data to confidential research and intellectual property)
- The rise of healthcare organizations as high-profile targets for hacktivists and nation-states
- The technical and organizational complexity of the industry, which makes it difficult to implement and maintain tight security controls

The risks internally and externally

Out-of-date software, insecure protocols, misconfiguration, and password flaws are some of the most high risk threats to a hospital's network. Wile risk implements insecure protocols, password flaws, and patching flaws are the biggest threat to an internal network. Most hospitals are indeed understaffed when it comes to the IT department in hospitals and unfortunately, New Yorks Fines is one of them. This means that addressing these issues may be somewhat difficult, but when we review our gab report one thing we are trying to do to raise the level of maturity of the company is hiring 10 full-time staff in the IT department. This process will be done by the head of the department to find the best-suited individual. So far New Yorks Fines has not had any of these risks internally or externally, But we do not plan on it for the future either.

The acceptable level of risk

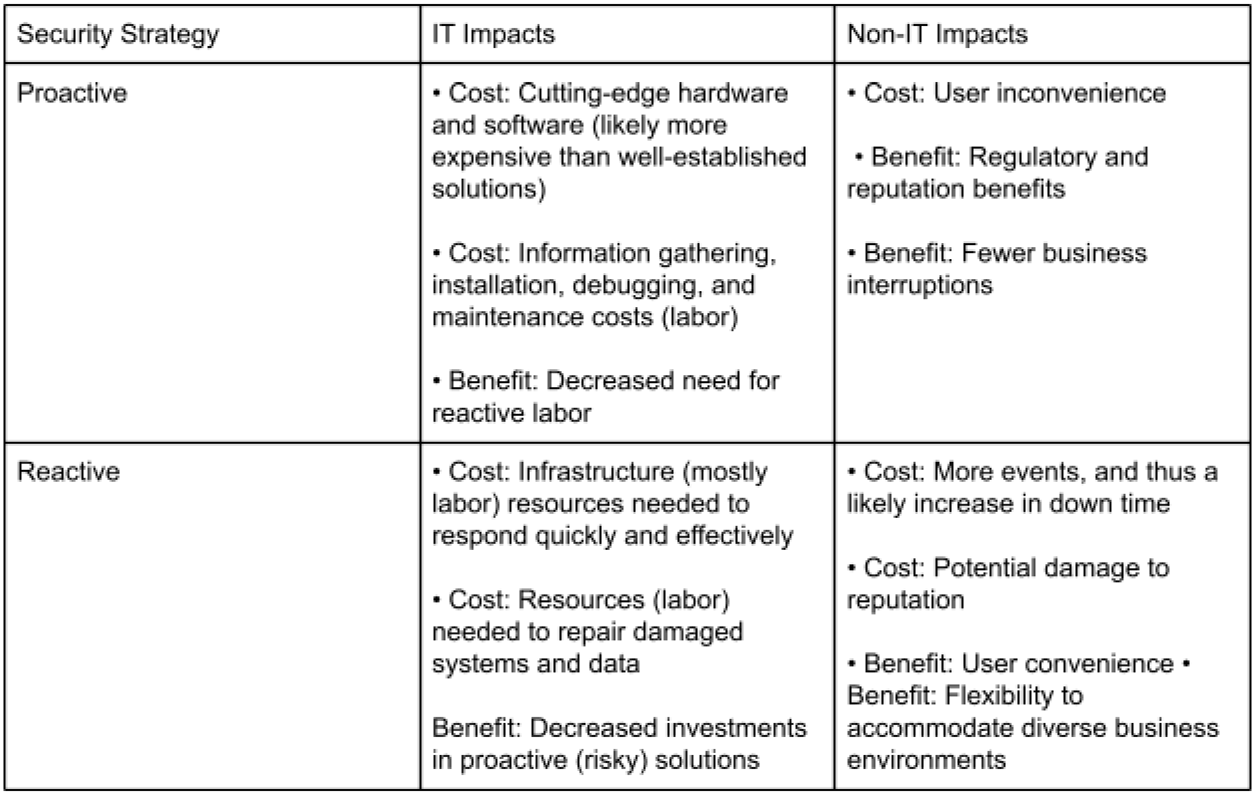
New York's Fines implements two types of strategies: a proactive strategy and a Reactive strategy. Proactive strategies tend to lead to few breaches while a reactive strategy will be more cost-effective. We believe that the most efficient strategies rely on existing, proven security technologies and then to be able to quickly implement patches when new viruses are identified.

These strategies include:

- Hiring Pentesters to test systems
- Firewalls, Antivirus or anti-malware software, Password protections, Spam filters, Ad blockers
- Threat hunting
- Proactive network and endpoint monitoring
- Staff training

The table below shows an overview of the labor costs of a proactive or reactive strategy.

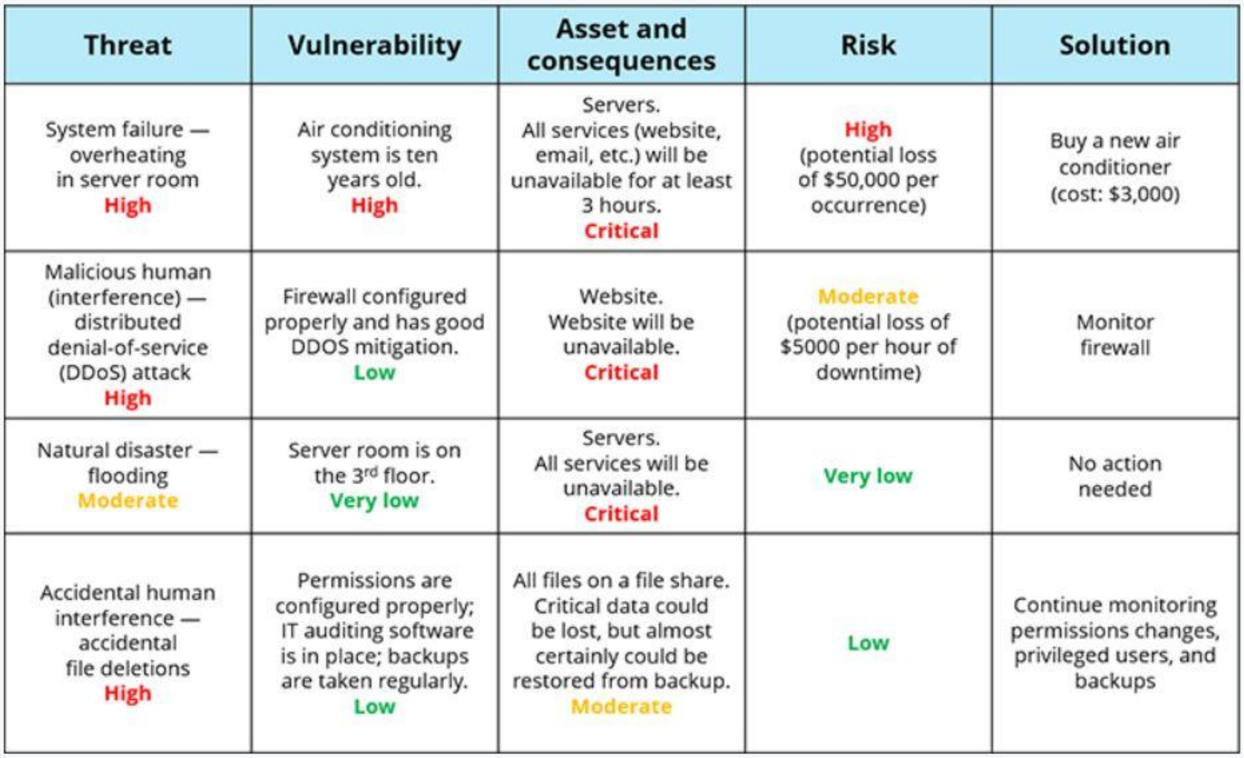
Proactive strategies tend to have regulatory and reputational benefits.



Security Strategy	IT Impacts	Non-IT Impacts
Proactive	• Cost: Cutting-edge hardware and software (likely more expensive than well-established solutions) • Cost: Information gathering, installation, debugging, and maintenance costs (labor) • Benefit: Decreased need for reactive labor	• Cost: User inconvenience • Benefit: Regulatory and reputation benefits • Benefit: Fewer business interruptions
Reactive	• Cost: Infrastructure (mostly labor) resources needed to respond quickly and effectively • Cost: Resources (labor) needed to repair damaged systems and data Benefit: Decreased investments in proactive (risky) solutions	• Cost: More events, and thus a likely increase in down time • Cost: Potential damage to reputation • Benefit: User convenience • Benefit: Flexibility to accommodate diverse business environments

(Cassandra L.2020)

An Organizational Risk Assessment Chart



Threat	Vulnerability	Asset and consequences	Risk	Solution
System failure — overheating in server room High	Air conditioning system is ten years old. High	Servers. All services (website, email, etc.) will be unavailable for at least 3 hours. Critical	High (potential loss of $50,000 per occurrence)	Buy a new air conditioner (cost: $3,000)
Malicious human (interference) — distributed denial-of-service (DDoS) attack High	Firewall configured properly and has good DDOS mitigation. Low	Website. Website will be unavailable. Critical	Moderate (potential loss of $5000 per hour of downtime)	Monitor firewall
Natural disaster — flooding Moderate	Server room is on the 3rd floor. Very low	Servers. All services will be unavailable. Critical	Very low	No action needed
Accidental human interference — accidental file deletions High	Permissions are configured properly; IT auditing software is in place; backups are taken regularly. Low	All files on a file share. Critical data could be lost, but almost certainly could be restored from backup. Moderate	Low	Continue monitoring permissions changes, privileged users, and backups

(Cassandra. L,2020)

Gaps to include

The type of audits

To measure the Compliance gap we must conduct an audit protocol, this form of audit is made by Rule and regulatory provision. it was made so that a company may address the issue of privacy, security, and breach notification separately. This effectively allows the organization to go through its safeguards and see what is working and what is not. It is in New York Finest Hospital to self-audit every 2 to 3 months. It is important for compliance to be met and for the hospitals to get all of the documentation to meet such compliance. Along with this New York's fines will register with HITrust every 2 years to complete a full audit. This will allow the company to keep HITrust certification as well as make sure the company complies with HIPAA certification.

The type of gap analysis

Desired state	Current state	Action step
It is New York's fines job and a hospital that serves its people to have the HITrust certifications as well as risk assessments and audits. We want our patients to be secure and safe when it comes to their data. We will also abide by HIPAA policies. This will allow the staff to carry out their duties with no need to fear a cyber attack. We also would like a full department of 10 for our cyber efforts.	As of now, we have not reached certification level with Hitrust but do abide by HIPAA regulations. Currently, our IT staff falls between 3 part-time employees and 2 full-time employees. we have a risk assessment, backup plans, and disaster recovery plans in place.	1. Currently in the process of securing funds for full-time staff in the cyber department 2. Once the full-time staff is secured proper documents will be made for the HITrust audit. 3. Backup plans, recovery plans, and HITrust framework will replace the old NIST framework.

(Cassandra. L,2020)

A cybersecurity governance strategy

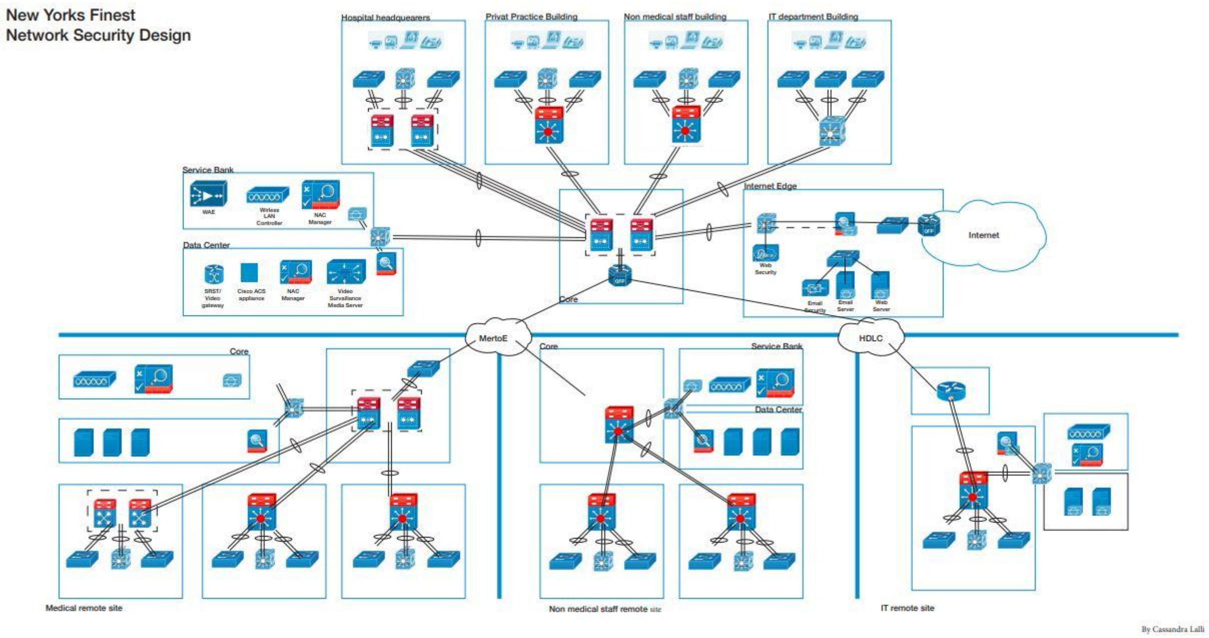
With healthcare compliance being the top priority for meeting security standards healthcare organizations such as New York's Finest must be up to date with all HIPAA standards as well and reach compliance with all new york state laws. With this said, meeting compliance regulations is not enough to protect the crucial data that is collected by the hospitals. We must stop viewing security as a compliance exercise and instead start to exact it as an independent activity with its priorities and timelines. Cybersecurity is not only an IT department priority but must be integrated into the organization as a whole. This will allow the burden of blame to fall on each department if standards are not being met as a whole. To achieve this we must instate the following:

- Executive board members Must understand cyber risk and the effect it has on the Hospital, this includes establishing a culture of security and providing sufficient budget and staff to enable execution.
- Administrators must take responsibility for cybersecurity, both tactically and strategically.
- Clinical staff members recognize their role in cybersecurity and contribute to the discussion, providing insight and finding a balance between care delivery and security controls. This includes security incident response when critical decisions affecting patient care need to be made.

A good defense makes up a strong offense in Cyberattacks. To protect the data and assets of New York's Fines a holistic, layered, and multistakeholder approach must be implemented. No cyber attack is a one-off problem and should not be treated as such. A cyber breach should be approached as a web of attacks, by integrating solutions into a cohesive whole, from the on-premise network to the cloud to the endpoint.

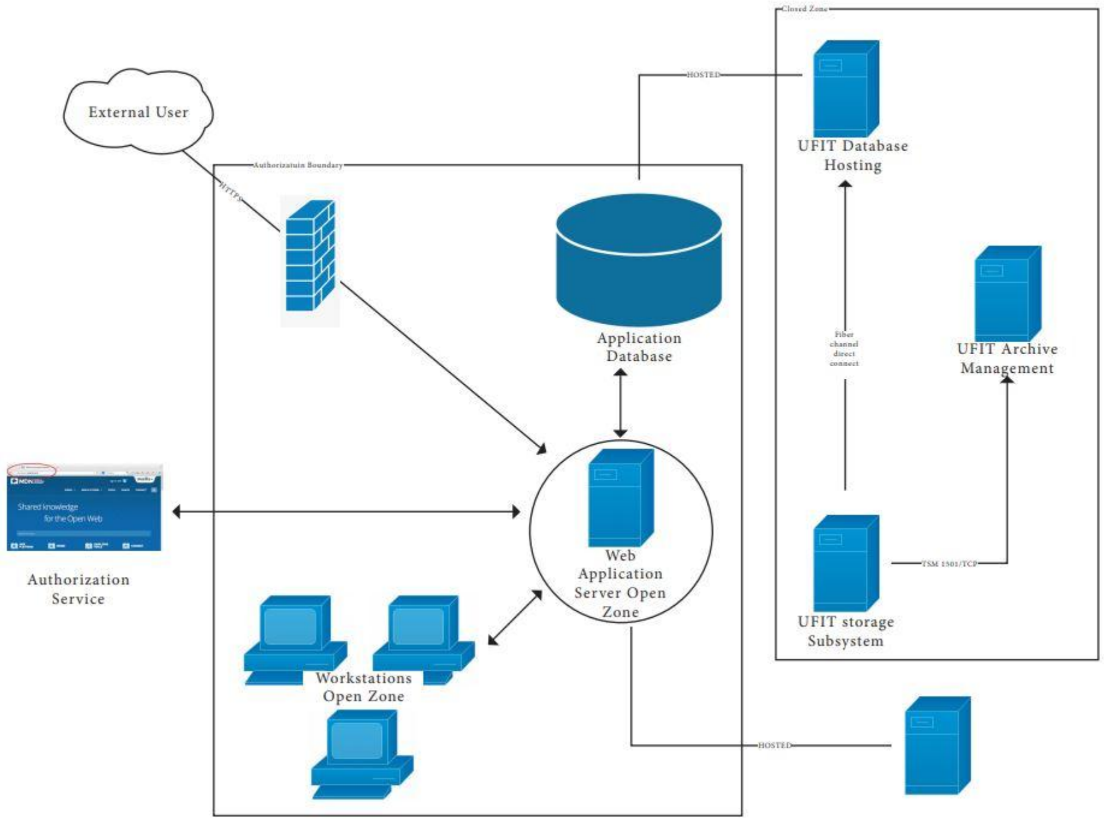
Portal data flow diagram of Hospitals operational

(Cassandra. L, 2020)



(Cassandra. L,2020)

Data Flow Chart



By Cassandra Lalli

(Cassandra. L,2020)

References

ASPR, & TRACIE. (2021, February). *HEALTHCARE SYSTEM CYBERSECURITY Readiness & Response Considerations* . asprtracie.hhs. https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf.

Blumenthal, R. (2017, July 27). *S.1656 - 115th Congress (2017-2018): Medical Device Cybersecurity Act of 2017*. Congress.gov. https://www.congress.gov/bill/115th-congress/senate-bill/1656.

CSIA. (2016, May). *Healthcare Sector Cybersecurity Framework Implementation Guide*. cisa. https://www.cisa.gov/sites/default/files/publications/HPH_Framework_Implementation_Guidance.pdf.

HITrust. (2018, February). *Implementing Cybersecurity in Precision Medicine*. hitrustalliance. https://hitrustalliance.net/content/uploads/PMIFrameworkImplementationGuide.pdf.

HITrust. (2019, September). *Risk Analysis Guide for HITRUST Organizations & Assessors* . hitrustalliance. https://hitrustalliance.net/uploads/RiskAnalysisGuide.pdf.

HITRUST. (2020, December). *Introduction to the HITRUST CSF*. HITRUST. https://hitrustalliance.net/content/uploads/CSFv9.4_Introduction.pdf.