Cassandra Lalli

Cybersecurity Program

Business/Organizational Description

Directions: Select an area of the industry that you are interested in and create a hypothetical business. Use the following sections to define the business environment; these items will vary depending on your business type. Feel free to adapt this document as needed. **Note:** Students may adapt their hypothetical business developed in CYB-630 or CYB-650 for this assignment. However, additional details will be required.

Business Details

Company Name

New Yorks Finest Hospital

Established Date

April 9th, 2000

Physical address

345 Dove st

New York, NY 11225

Phone and Fax Numbers

222-222-3456

Website URL

Newyorksfinesthospital.com

Email Address

cassanova@newyorksfines.com

Business Basics

Vision Mission Statement and Goals

A. Mission Statement

New Yorks Finest hospital opened in 2000 to help the people of New York with no insurance and provide treatment to the soldiers coming home from the war. established in the time of the great depression New Yorks Finest priority is to help all New Yorkers in the working class with the finest hospital care at affordable pricing.

B. Vision Statement

New Yorks Finest's 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.

C. Goals and Objectives

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 health care that is affordable.

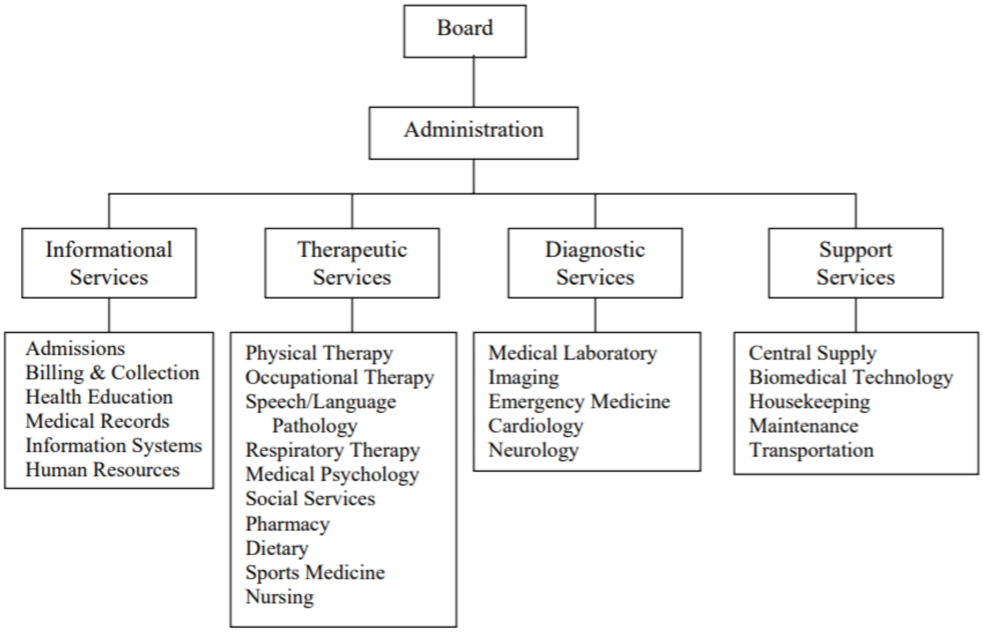
D. Industry Information/Experience

Due to the rapidly increasing demand for medical supplies that can help control the COVID-19 (coronavirus) pandemic, purchase costs are expected to rise for the Hospital industry. For more detail, please see the Current Performance chapter. Industry revenue is expected to plummet in 2020 alone as patients cancel elective and nonemergency procedures. For more detail, please see the Current Performance chapter. Demand for healthcare services is expected to rise among those with coronavirus and those concerned that they may have contracted coronavirus. For more detail, please see the Demand Determinants chapter.

E. Major Stakeholders

Patients, physicians, employees, the broader community, and legislative and regulatory bodies

F. Company Organizational Flow (to include a diagram)



Products and Services

A. Main Products (described in detail)

New York Fines takes pride in its state-of-the-art and top-line medical equipment. As one of the best ranking hospitals in Major cities, It is important to have all equipment up to date and working in present condition. With that said our Main Products are listed below

Hospital Stretchers

This is to transport the patients, if a stretcher is ripped or not working to seniority ability they must be filed with the right person so a replacement form will be made ASAP.

Defibrillators

Defibrillators restore normal rhythm to the heart. This is vital, all ambles and patient rooms must have 1 in-store, for an emergency. Each day the defibrillators will be checked and logged in the inventory report.

Anesthesia Machines

Anesthesia machines include added tools such as a ventilator, suction unit, and patient-monitoring devices. These machines make it so that any patent receiving surgery can receive the proper dose of anesthesia. Every night they must be logged with the inventory.

Sterilizers

Every form must have Sterilizers due to covid-19 regulations. A member of staff is responsible to make sure that all sterilizers are in proper locations and filled at all times.

EKG/ECG Machines

This allows doctors to monitor patients' heart rates and is a must in every patents room.

Computers

There must be a computer in every room. At new Yorke's Finest, We use both PC and MAC. This will allow the doctors to easily pull up patent information and log any changes to patents.

B. Service Offerings

New Yorks Fines Hospital offers a wide range of services from patient care to rehabilitation for any resident in the New York area. We also offer emergency services and have 5 ambulances in the facility. Some of our most notable servest for the average person are:

- ➔ short-term hospitalization
- ➔ emergency room services
- ➔ general and specialty surgical services
- ➔ x-ray/radiology services
- ➔ laboratory services
- ➔ blood services
- ➔ primary care services
- ➔ mental health and drug treatment
- ➔ infectious disease clinics
- ➔ hospice care
- ➔ dental services
- ➔ translation and interpreter services

We pride ourself on the Friendliness and fast pace of the hospital, creating an atmosphere of rapport with our clients. New York Fines is a Government hospital, with sister hospitals in 3 other major cities (Chicago, Seattle, Los Angeles, and Texas).

C. Consumer Base

New yours fines Hospitals do not discriminate. No matter the age, race, religion, or person we will take them in. As a government organization, we must provide all personnel with quality health care. With this said we have noticed through our database that Men ages 30 to 50 with military backgrounds and women ages from 18 to 30 have a higher rate of visitation. We believe that this is due to one of two situations.

1. No health insurance, We do not turn away people for health insurance. We are also transparent with our prices. With the Lowest price of any health care we will not charge you over 10$ for most medicines, Over 100$ for any medical attention, and 500$ for any life-saving surgeries. This cost may also be waived at the discretion of your doctor.
2. Convenience, with 2 hospitals located in any burrow of New York you will have a New Yorks Fines hospital there.

Technology and Security Solutions

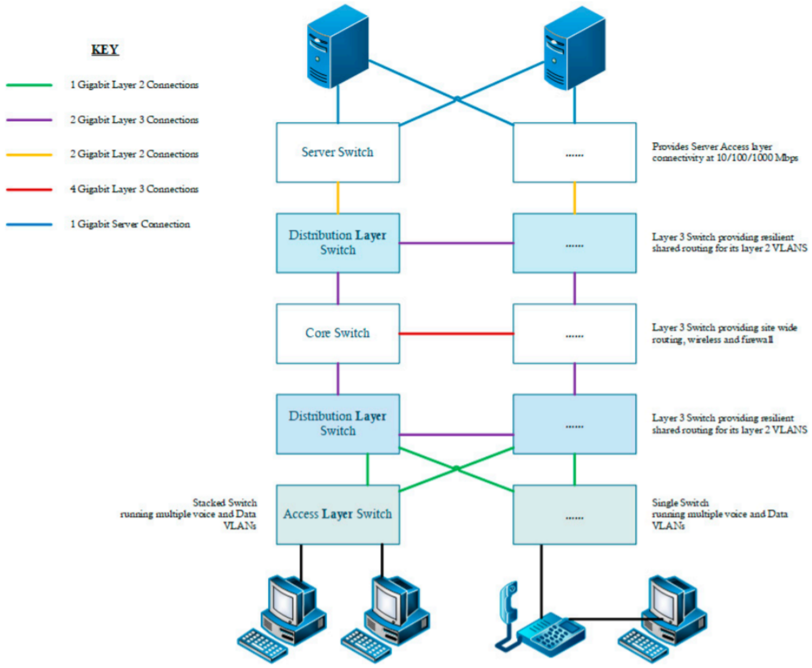
New York Fines prides itself on being top of the industry when it comes to our technology and Security solutions. To start with our technology includes but is not limited to. Our online portal and app, allow patients to check their status as well as make appointments with the clinic and see the latest news about the hospitals and our advancements. Hospital-issued Tablets, allow our doctors to update charts and view data at the drop of a dime. Due to the Covid-19 pandemic, the tablets and ports also allow patients to look up symptoms as well as Video conferences with doctors. More technology includes card readers, computers, and laptops for staff and medical equipment that is listed in the above areas. On the patent floor, the hospitals tend to use MAC due to their user-friendly interface and in the inner department, employees will use PCs. Both computers will be running on different networks to secure the network and create a division if a hacking attempt is made via network devices. For our security Solutions, New Yorks Fines runs off of a hybrid solution. We also Abide by HIPPA, HITRUST, MARS-E, and PCI DSS. Each of these compliance is necessary when it comes to the hospital due to the value of your data. Both MARS-E and HIPPA do not have an official certification program but we must comply and minimize the risk. All of the hospital labs will have biometric scans to enter orexis. All exit doors to the hospital will have security posts 24/7. Security cameras will be placed strategically throughout the hospital on each floor so that there are no blind spots, the exception to this rule is patient rooms. Altho there will be no video surveillance, there will be audio surveillance put in place in patients' rooms. All patients must be made aware of this and sign both a nondisclosure and privacy contract when being admitted into the room. In the main offices of the hospitals, NO PATIENT WILL BE ALLOWED TO ENTER. This area is for authorized personnel only. In this along with video and audio surveillance, there will be biometric scans for each door to the departments. No person from another department should enter another department without permission from the respected department head. There will be a common area in which staff can talk between each intersecting department and discussion should be made there. Phishing emails will be sent at random dates throughout their year, this will then determine the status of the company and the cyber efforts. Along with this, each employee will attend a mandatory assembly to learn and be tested about the company's cyber policies and safe online practices. Along with this, each employee will be assigned new passwords every 5 months issued by the cyber team. you may keep them in a safe place at your workstation but they must not be written down anywhere online. On the virtual front New Yorks Fines uses all cisco products, this includes routers, wires, and switches. We use both network firewalls and host-based firewalls, Host-based firewall are implemented through the hospital while network-based is implemented through the main building. For any employee working from home due to covid-19 restrictions, this employee will be issued a work laptop. This laptop will be registered with the network and have a VPN, employees will not access the hospital's internal network unless on this device. Employes are also not allowed to modify the device in any way, doing this will mean automatic termination. The hospital uses ISO 9001 standards paired up with NIST Framework. with allows the company to keep up with any threat that may arise. Pairing the ISO9001 with NIST also allows the company to reach complacent and keep all of our files together when being audited. Finally, New Yorks Fines utilize an MCPSs system. Healthcare organizations differ from other enterprise networks through their use of medical cyber-physical systems (MCPSs). MCPSs are inexpensive personal monitoring devices that can record and transmit multiple physiological signals. Encryption of this data is required for secure storage, secure transmission, and secure computation. MCPSs consists of four layers, which need to be considered and secured. (Kocabas.2016)

The data acquisition layer has a body area network (BAN), which are wearable sensors that facilitate the collection of patient medical information.

The data concentration/aggregation layer, consisting of transmitting the gathered information to a gateway server through short-range wireless, such as Bluetooth, due to the low computational power of sensors with a BAN.

The cloud processing and storage layer consists of the long-term secure storage, processing, and analytics of medical information. (Kocabas.2016)

The action layer involves either active or passive use of the data. Active usage employs an actuator using the data and the algorithms used to perform data analytics to be directly influenced by the data, such as through the use of a robotic arm in robot-assisted surgery. Passive action visualizes the data to provide decision support to medical professionals.


KEY
1 Gigabit Layer 2 Connections
2 Gigabit Layer 3 Connections
2 Gigabit Layer 2 Connections
4 Gigabit Layer 3 Connections
1 Gigabit Server Connection
Server Switch
......
Provides Server Access layer connectivity at 10/100/1000 Mbps
Distribution Layer Switch
......
Layer 3 Switch providing resilient shared routing for its layer 2 VLANS
Core Switch
......
Layer 3 Switch providing site wide routing, wireless and firewall
Distribution Layer Switch
......
Layer 3 Switch providing resilient shared routing for its layer 2 VLANS
Stacked Switch running multiple voice and Data VLANs
Access Layer Switch
......
Single Switch running multiple voice and Data VLANs

The figure above is a representation of the 3-layer network topology overview of how our hospital network is configured. The diagram demonstrates the principle of how the network is configured, it is replicated several times over and thus is too big to be represented by this diagram.

Cybersecurity Framework

System Design

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 the 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 the 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 company's system and the report of findings will be written up and given to the CISCO. the CISCO will then delegate the jobs of Harding systems and make patches throughout the team.

The Data Backup Planning Process: the most crucial part of the backup plan is the data backup. data backup will ensure 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. Some threats 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 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 act 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 on 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 for 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.

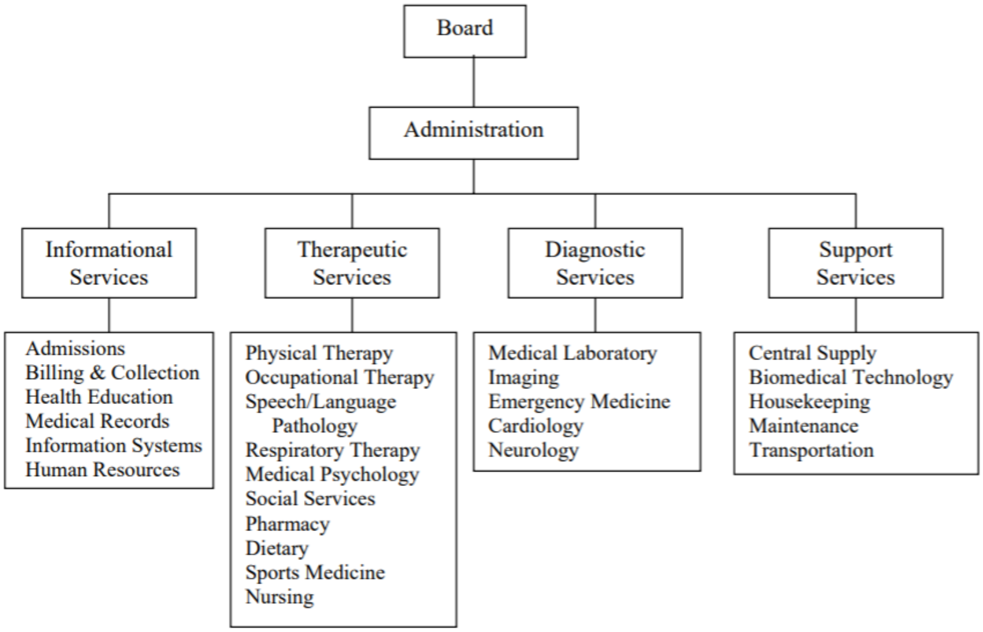
Federal Food, Drug, and Cosmetic Act (FD&C Ac**t)**

This act mostly covers any food or drug distributed in the U.S. but it 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-risk implement 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.

(The above examples were taken from Maryville University, 2021)

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.

The likelihood of risks occurring and the resulting impact

When taking hospitals into account it is shown that breach incidents are on a rise by 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 (Symantec,2018). While 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

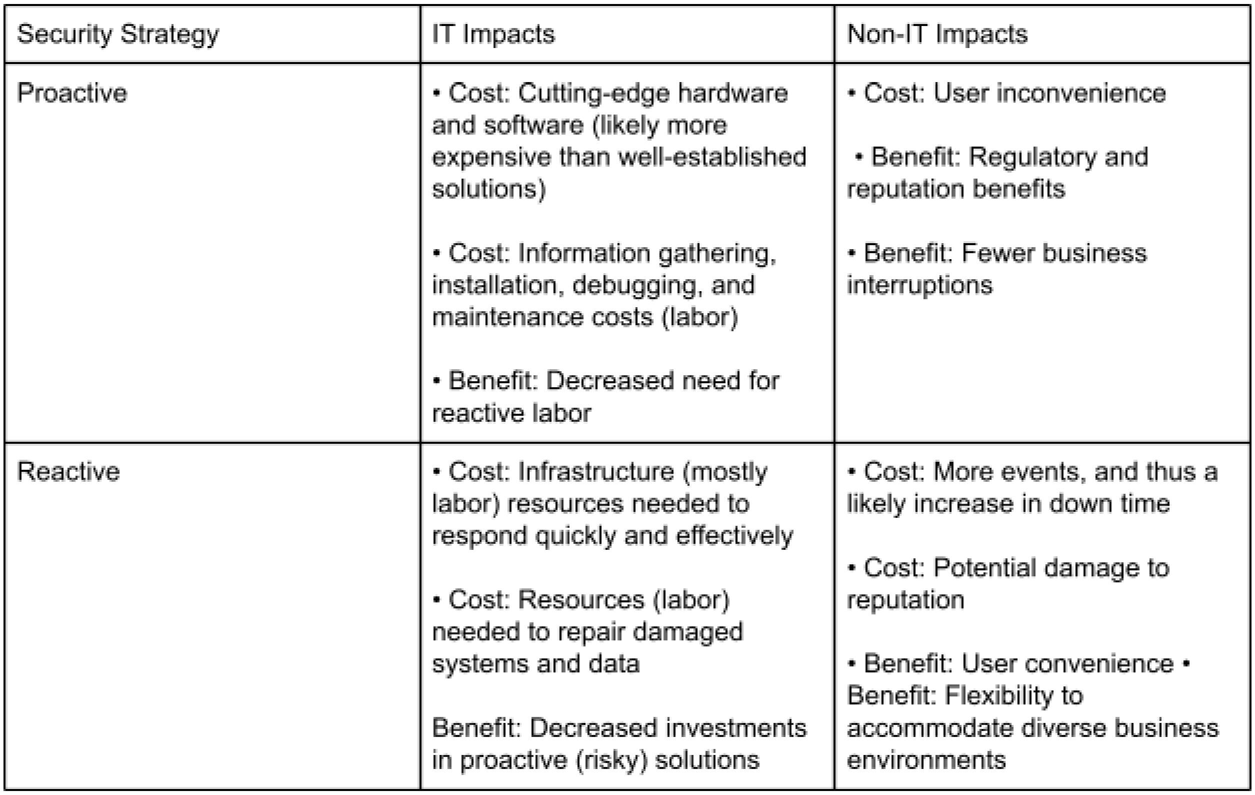
New York's Fines implements two types of strategies: a proactive strategy and a Reactive strategy. Proactive strategies tend to lead to few breaches while a reactive strategy will be more cost-effective. We believe that the most efficient strategies rely on existing, proven security technologies and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

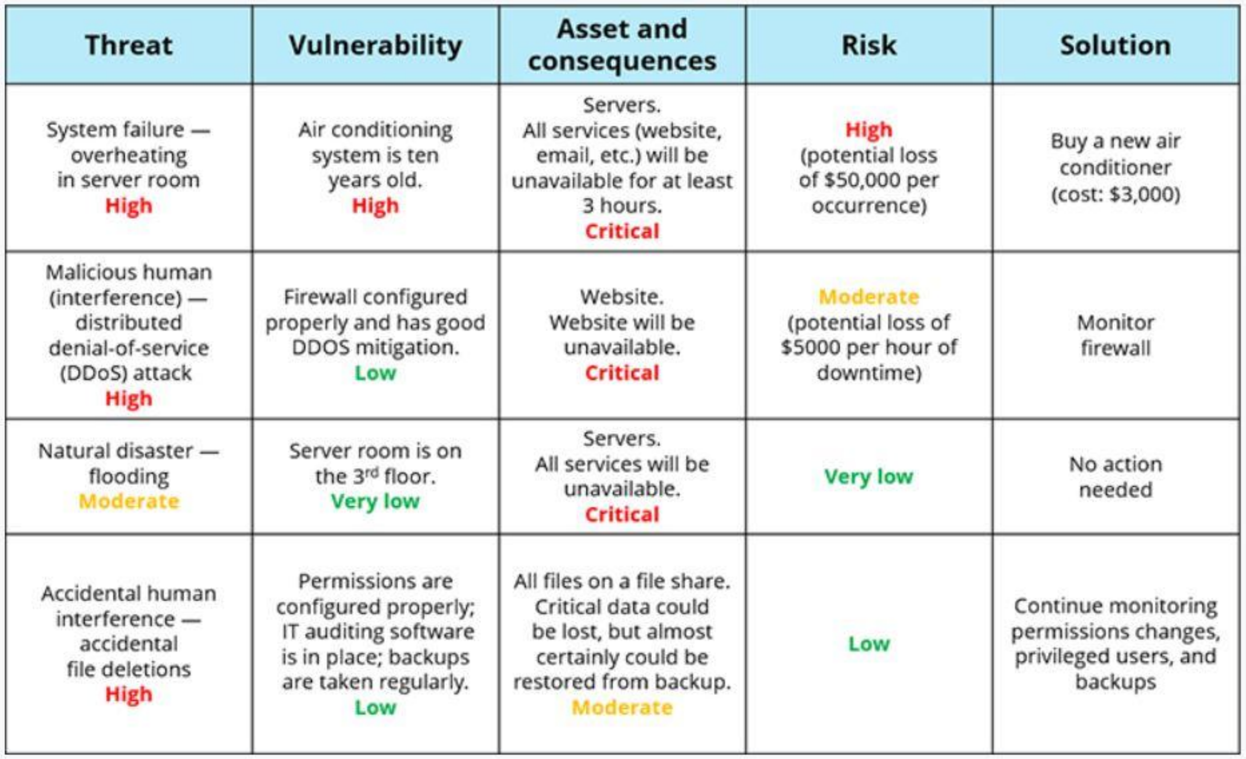
Proactive strategies tend to have regulatory and reputational benefits.



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 provisions. 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 registered 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 Finest 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	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

of 10 for our cyber efforts.		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:

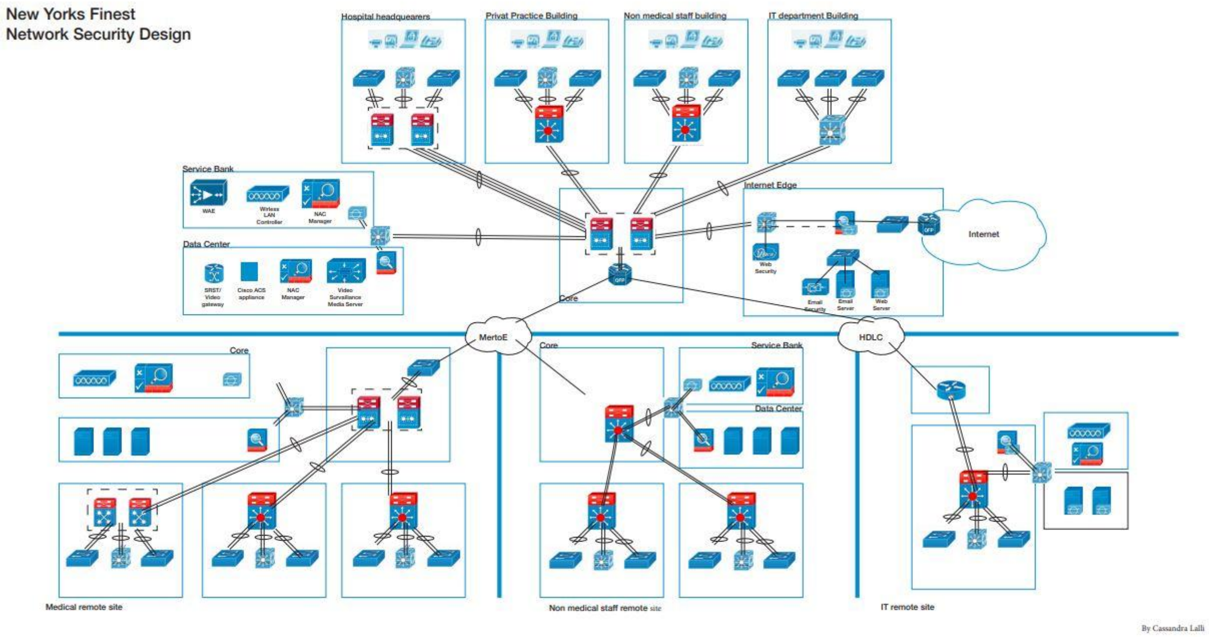
- Executive board members Must understand cyber risk and the effect it has on the Hospital, this includes establishing a culture of security and providing sufficient budget and staff to enable execution.
- Administrators must take responsibility for cybersecurity, both tactically and strategically.
- 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.

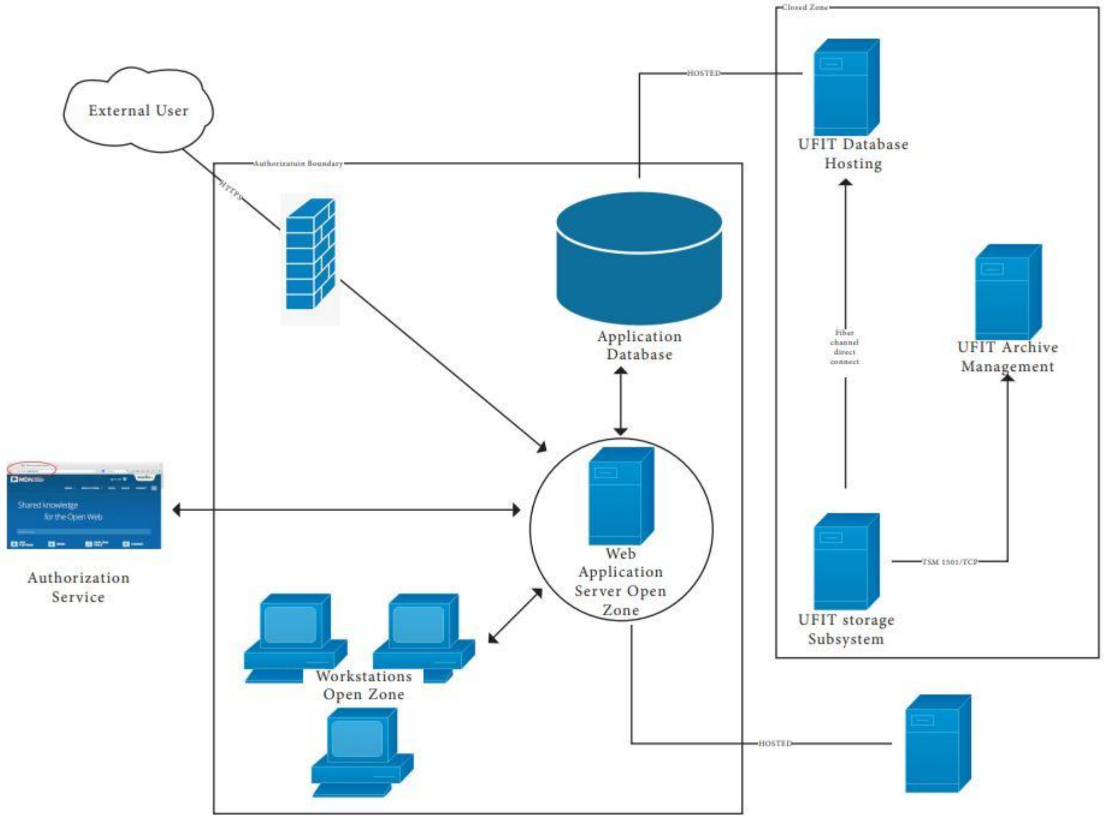
Portal data flow diagram of Hospitals operational

(Cassandra. L, 2020)



(Cassandra. L,2020)

Data Flow Chart



By Cassandra Lalli

(Cassandra. L,2020)

System Design

Design Goals and Considerations.

Hospitals systems are responsible for all patients' health information and history. This system is responsible for the patient's information reaching the doctor or correct department in any circumstance all the while still securing any and all information. It is the hospital's systems that have the responsibility to communicate with internal and external sources, securing the information and having them reach the right source with no flaw. This information will include lab tests, clients medical history, sensitive government information, health insurance information, official documentations, financial situation reports, personal data, utilities, and stock amounts, also keeps secure plans in place for patients information, patients medical history, prescriptions, operations and laboratory test results.

The goal for this new system design is for the medical practitioners to be able to keep track of all patient's medical records and information. This system will have the responsibility of tracing and retrieving any client's information while in the hospital. The system will also be tasked with the improvement and efficiency of the management in daily work, providing required records in a timely fashion. When deciding on the type of Hospital Information System, we have considered the following benefits for this system type:

Planned approach towards working: Data must be stored properly in data stores, this will allow for speedy retrieval and accurate information coming in from out of hospital doctors, labs, patient care centers...etc.

Accuracy: the Accuracy of this system must be of the highest importance due to the reason listed above.

Reliability: This level must be high due to the type and class of information being transmitted and received, proper storage of information is a must.

No Redundancy: Information should not be repeated. In this system there must be no redundancies, the storage of the information will be prioritized for this.

Immediate retrieval of information: the main purpose of this system is for quick access to all information with little to no security threats. Any information request will be given quickly to the right sources with authority with this set into place.

Immediate storage of information: Manual systems propose an abundance of problems when it comes to large amounts of data.

Easy to Operate: This is a major priority. The system should be easy to use and fit into the budget of the hospital so that there will be no learning curb.

The System Architecture.

Below is a general understanding of health IT from a technical perspective :

- Application Level
    - Computerized Provider Order Entry (CPOE), Clinical Decision Support (CDS), Electronic Prescribing (e-prescribing), Electronic Medication Administration Records (eMAR), Results from Reporting, Electronic Documentation, Interface Engines...etc
- Communication Level

  - Messaging Standards

    HL7, ADT, NCPDP, X12, DICOM, ASTM, and so on

  - Coding Standards

    LOINC, ICD-9, CPT, NDC, RxNorm, SNOMED CT, and so on

- Process Level
  - Health Information Exchange (HIE), Master Patient Index (MPI), HIPAA Security/Privacy, and so on
- Device Level
  - Tablet PCs, Application Service Provider (ASP) models, Personal Digital Assistants (PDAs), Bar Coding, and so on

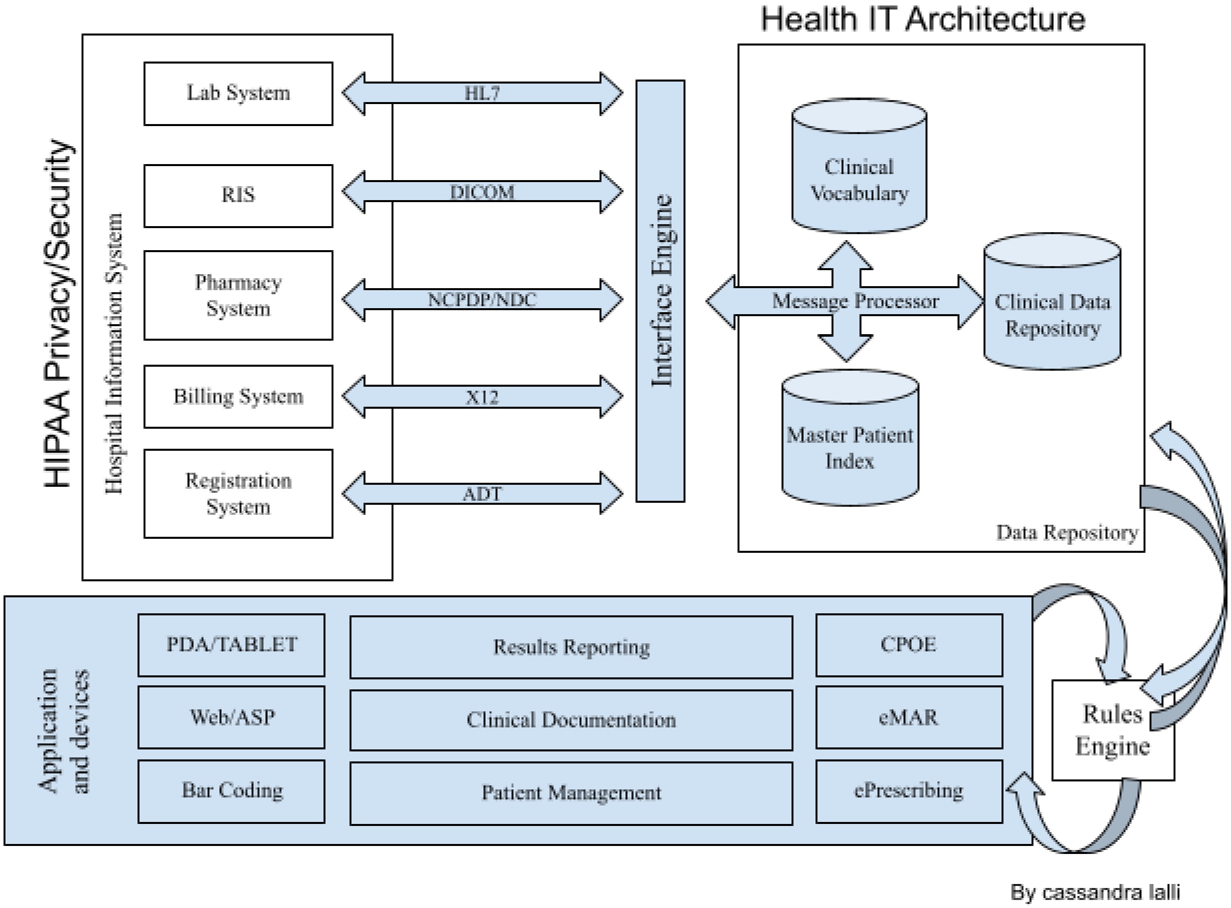
Applications include the following:

- Computerized Provider Order Entry (CPOE)
- Clinical Decision Support (CDS)
- Electronic Prescribing (e-prescribing)
- Electronic Medication Administration Record (eMAR)
- Results Reporting
- Clinical Documentation
- Interface Engines

As listed above the activities mentioned are used for any end-user in the hospital company. There are many examples of this but I have listed the most important that are highly used. The use of these codes comes from the need to quickly access any patent’s data and how quickly the information can be sorted. Since all data is pulled from one storage and there must be no repeating data, each code is vital in understanding the process. There are many different types of coding standards as well below, I will list 5 codes and their defined respected data types:

- LOINC is a laboratory and clinical observation coding standard.
- ICD codes for diagnoses.
- CPT codes for procedures.
- NDC and RxNorm code for medications.
- SNOMED CT codes for clinical concepts.

CPOE refers to an application that allows providers to enter their orders (for lab or other tests, medications, consult requests, or other orders) into an electronic system for processing. Typically, during the "ordering phase," clinical decision support (CDS) is provided about the choices made by the provider (Architecture of Health IT, 2017).



Data design

The type of design New Yorks Fines will be using is the Entity attribute value Model (EVA). Describe the human-machine interface and operational scenarios. This will be the best form of design to keep all data organized and easily accessible. If any new data type is needed. A class diagram can be designed and map any class to the relation table or type column. Any spare data will be stored in the EAV sub-schema. By doing this the Hospital has effectively minimized the negative effects of EAV such as the data validation becoming harder on the table. New York Fines has also made our EHR database flexible to allow modification and additional types of data to be added without changing the physical database schema. Having a Flexible Schema will allow the systems to not get overloaded with all new information coming in daily.

In EAV design all data can be stored in a single generic table with conceptually 3 columns:

- 1 for entity (e.g., patient identification),
- 1 for attribute (e.g., name),
- 1 for value (e.g., "Jens Hansen")

To add more descriptive fields to the entity class, you add attribute values in the attribute field. The main advantages of this design are flexibility and effective entity-centered queries and storage-saving by preventing fields with NULL values (WIEDERHOLD,2016). In an EHR environment, null (inapplicable, unavailable, or unknown) meaning is sometimes required. To handle this situation, a missing value code column should be added to an EAV table, which is non-null only when the value column is null. The main disadvantages are data display, attribute-centered query complexity, and inefficient constraint checking (WIEDERHOLD,2016).

Human-Machine Interface

Data Source = ServerName\InstanceNameOnce we add a user to SQL Server Instance, we should attach the user to databases we want the user to access and provide the appropriate role(s). For each computer that will run our application, we should install the executable version on each computer.

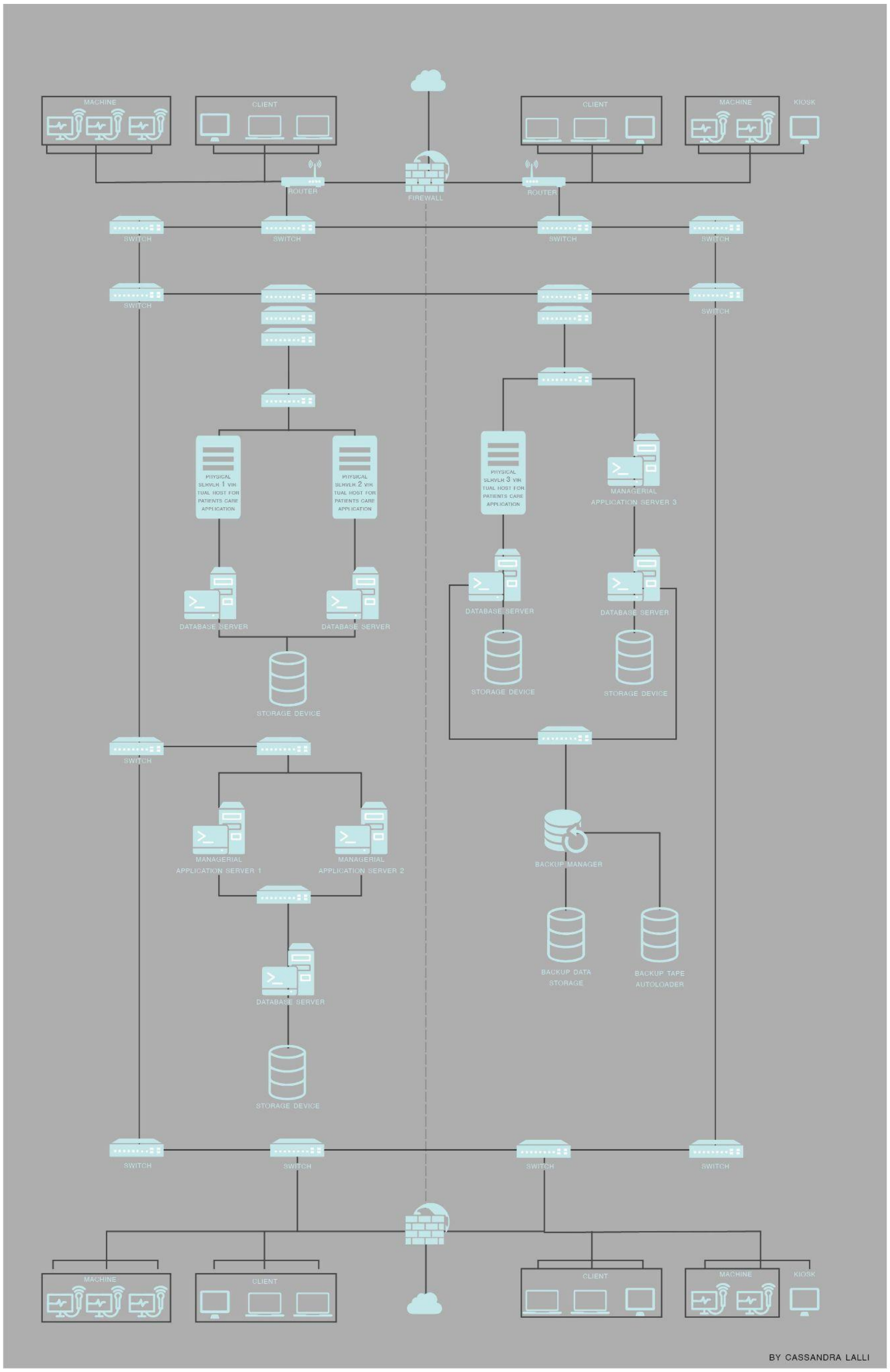
When the user logs in as an admin, the window above will be displayed. The admin adds the user to the system and can back up the database and restore it. The panel on the right side of the screen is used to turn off the system, display information about the system designer, and log out and back log in to the system. When the admin chooses the Manage users button, the window will be displayed and he will be able to add a new user (a new admin, doctor, receptionist, pharmacist, or biologist) by entering the basic information about the user like the first name, last name, age, his Picture ...etc. When the admin chooses the type of user, the table in the 2nd half of the window will automatically display all the users in the system according to the chosen type. The admin can select the user he needs to edit his information from this table or he may remove him entirely from the system by checking the checkbox resided in front of his name when the user login as a receptionist, a window will appear containing :

- Patient Registration: to add a new patient
- Leave Patient: to generate a report about the leaving patient
- Search: to search the patients registered in the system
- Design a drawing appropriate for implementation.

The high-level system design should be further decomposed into low-level detailed design specifications for each system component, including hardware, internal communications, software, system integrity controls, and external interfaces. Leavening Patient to save the history of the patient in this visit, a window like this one will appear, form contain basic information about the patient, Doctor Prescription and medical that given by the pharisaical, If the patient has a test the result will appear in the field of biologist result and finally the total bill of the patient.

When the receptionist clicks on the left button, the details will save in the system and another copy will be printed for the patient (Noori,2015).

Graph



BY CASSANDRA LALLI

Cybersecurity Test and Validation Scheme

Technical Controls

In contrast to HIPAA, the HITRUST CSF does not create broad buckets like Administrative and Security controls. The HITRUST CSF is divided into 19 different control domains In addition to the domains above, HITRUST also has 75 control objectives and 156 specific controls (Datica, 2019). With this said below is the following control domains that apply along with the specific controls that New York's Fines will be using for our security architecture, after reviewing all controls it is our understanding that each of these controls will keep our system safe and at low risk.

- Information Protection Program
  - SC-4: Information in Shared System Resources | Multilevel or Periods Processing
  - AC-4: Information Flow Enforcement
  - PM-11: Mission and Business Process
  - PL-2: Develop Security and Privacy Plans for the System
  - PM-7: Enterprise architecture
  - PM-8:Critical Infrastructure Plan
- Endpoint Protection
  - SC-8:Transmission Confidentiality and Integrity
  - SC-12: Cryptographic Key Establishment and Management
  - SC-13: Cryptographic Protection

- Portable Media Security
    - IR-8: Incident Response Plan
    - MP-4: Media Storage
    - MP-6(3): Media Sanitization | Nondestructive Techniques
    - MP-7; Media Use
    - MP-5: Media Transport
- Mobile Device Security
    - AC-19: Access Control for Mobile Devices
    - PL-4(1): Rules of Behavior | Social Media and External Site/ Application Usage Restrictions
    - AC-19(4): Access Control for Mobile Devices | Restrictions for Classified Information
    - AC-19(5): Access Control for Mobile Devices | Full Device or Container-Based Encryption
    - CM-2(2): Baseline Configuration| Automation Support for Accuracy and Currency

- Wireless Security
    - AC-2: Account Management
    - AC-3: Access Enforcement
    - CA-9: Internal System Connections
    - IA-2: Identification and authentication (Organizational Users)
    - IA-3: Device Identification and Authentication

    - IA-8: Identification and Authentication
    - PL-4: Rules of Behavior
    - SC-40: Wireless Link Protection
    - SC-43: Usage Restriction
    - SI-4: System Monitoring

- Configuration Management
    - SA-4(5); Acquisition Process | System, Component and Service Configuration
    - CM-3: Configuration Change Control
    - CM-9: Configuration Management Plan
    - SA-10: Developer Configuration Management

- Vulnerability Management
    - AC-17(4): Remont Access | Privileged Commands and Access
    - AC-6: Least Privilege
    - SC-12: Session Termination
    - SC-13: Supervision and Review-Access Control

- Network Protection
    - CM-7: Least Functionality
    - AC-4(15): Information Flow Enforcement | Detection of Unsanctioned Information
    - AC-6(3): Least Privilege | Network Access to Privileged Commands

- CS-10: Network Disconnection

- Transmission Protection
  - AC-12(2): Session Termination| Termination Message
  - SI-15: Information Output Filtering
  - AC-16(5): Security and Privacy Attributes| Attribute Displays on Objects to be Output
  - CA-3(6): Information Exchange | Transfer Authorizations
  - CM-6: Configurations Settings

- Password Management
  - IA-5: Authenticator Management
  - IA-5(1): Authenticator Management | Password-based Authentication
  - IA-5(8): Authenticator Management | Multiple System Accounts
  - IA-5(4): Authenticator Management | Automated Support for Password Strength Determination
  - IA-5(18): Authenticator Management | Password Managers
  - SI-11:Error Handling

- Access Control
  - AC-13: Supervision and Review — Access Control
  - AC-3(7) : Access Enforcement | Role-based Access Control

  - AC-6(2)-AC-6(10) : Least Privilege Controles

- Audit Logging & Monitoring
  - AC-11:
  - AC-17(1): Employ automated mechanisms to monitor and control remote access methods.
  - AU-12-AU-12(4) : Audit Record Generation

- Education, Training, and Awareness
  - PM-14: Testing, Training, and Monitoring
  - PM-16: Threat Awareness Program
  - PM-12: Insider Threat Program

- Third-Party Assurance
  - SC-7: Boundary Protection
  - SR-6: Resource Availability

- Incident Management
  - IR-4(1)- IR-4(15) : Incident Handling

- Business Continuity & Disaster Recovery
  - CP-2(1): Contingency Plan | Coordinate with Related Plans
  - CP-4(1): Contingency Plan Testing | Coordinate with Related Plans

    - CP-8(4): Telecommunications Services | Provider Contingency Plan
    - IR-3(2): Incident Response Testing | Coordination with Related Plans
- Risk Management
    - PM-4: Plan of Action and Milestones Process
    - PM-7: Enterprise Architecture
    - PM-9: Risk Management Strategy

- Physical & Environmental Security
    - PE-23: Facility Location

- Data Protection & Privacy
    - SA-8(18): Security and Privacy Engineering Principles | Trusted Communications Channels
    - SC-8: Transmission Confidentiality and Integrity
    - SC-12:Cryptographic Key Establishment and Management | PKI Certificates
    - SC-13: Cryptographic Protection | FIPS-validated Cryptography

Cases Study

The following case study was made by the New Yorks Fines cybersecurity team, in this test we have reached a strong maturity, the number represents the order in which the test was performed, the name represents the control domain that was tested (please see above for which specific controls were tested in their respective domain). Technique stands for the method with which each domain was tested, and lastly the pass or fail criteria in which the test final results are displayed below.

#	Name	Technique	Test Result
1	Information Protection Program	Social Engineering Documentation Review	Pass
2	Endpoint Protection	Penetration Testing	Fail
3	Portable Media Security	Documentation Review	Pass
4	Mobile Device Security	Documentation Review	Pass
5	Wireless Security	Penetration Testing	Pass
6	Configuration Management	Ruleset and Security Configuration Review	Pass
7	Vulnerability Management	Password Cracking Social Engineering	Pass
8	Network Protection	Penetration Testing	Pass
9	Transmission Protection	Penetration Testing	Pass
10	Password Management	Password Cracking Social Engineering	Pass

11	Access Control	Ruleset and Security Configuration Review	Pass
12	Audit Logging & Monitoring	Penetration Testing Social Engineering Documentation Review	Pass
13	Education, Training, and Awareness	Social Engineering	Pass
14	Third-Party Assurance	Social Engineering Documentation Review	Pass
15	Incident Management	Social Engineering	Pass
16	Business Continuity & Disaster Recovery	Documentation Review	Pass
17	Risk Management	Password Cracking Social Engineering Documentation Review	Pass
18	Physical & Environmental Security	Social Engineering Documentation Review	Fail
19	Data Protection & Privacy	Penetration Testing Social Engineering	Pass

New Yorks Finest hospital is proud of the hard work in which the cyber team has put in. There were only 2 critical points of failure in the Endpoint Protection and Physical & Environmental Security domain of our architecture. It is our responsibility to make sure our system as a whole can pass with every domain, and will be revising the controls in these areas.

Cybersecurity Training

Culture of Security Awareness

Chief Financial Officer then have a single thought process when it comes to investments bought to them, if this investment is bought up by a CISO you should always remember they need a return on their investment to do this it is important to touch on each of these topics when drawing up a draft to any member outside of the IT team :

- The size of this risk in comparison to revenue.
  - Most cybersecurity members like to think of the risk as if it happens this is a bad approach, the risk of a cyber attack can be once a year but you should also tally up the amount of lost revenue and customer trust.
- The cost of this solution in comparison to the impact of a breach over a three-to-five-year period.
  - It is good to think about the long term and have others understand that the problem does not go away with a click of the button.
- What capabilities do we already have, and how effective are they? How effective will *this* solution be in comparison?

    - You have to start planning for the future and it is good to have others understand this as well. Malware and phishing attempts are getting smarter and you always have to be on top of it.
- Why do we need *this* solution, rather than an alternative?
    - At the end of the day, you need to sell them on these ideas, facts alone will not be the deciding factor
- Can we consolidate suppliers for simplicity and greater financial leverage?
    - Working with what you have is important, but working with what you know is better, being able to identify high and low risks is a must, and understanding where to send a budget will go a long way.

The CISO needs to respond to this internal dialogue and ensure that these factors are addressed in their business case (IDG Connect, 2021) . While those points are important touching point, you must also organize your submission, the following is a good way to mobile this:

1: Highlight the control gap

The first step in making the business case for investment in cybersecurity is to ensure that you clearly and succinctly define the problem. Describe the control gap in non-technical terms(IDG Connect, 2021):

- Highlight how gateway systems are allowing malicious emails to pass-through
- How your firm cannot track critical data moving between third-party cloud systems.

2: Quantify associated risk and impact levels

It is always good to incorporate the risk levels of the company. Evaluating your gab analyst and then creating risk models for each different risk level is a good way to understand what needs to be hardened and what can lift alone. Present the potential losses alongside recent examples from the media to highlight the potential reality (IDG Connect, 2021).

3: Describe the solution

It is always important when talking to someone with no IT background to keep the language nontechnical so as to not have to over-explain yourself or have the other person feel as if you are talking down to them. It is the CISO's job to understand this and your job to grasp this concept, if any revisions are necessary the CISO will let you know. Explain why this solution will address the risk when existing controls do not. Include some alternatives to give the CFO some flexibility for exploration, even if you feel the solution is clear (IDG Connect, 2021).

4: Highlight the value

Cost is a big part of this, if the cost outweighs the means then the stakeholders and clients will be less likely to shell out the money, you always have to put numbers into it for them to understand the means to an end. Do not exaggerate and only ask for what is needed. This is why the previous steps are so important.

Common Security Risks

Malware

Malware is one of the most common types of risk, this can happen in many ways the most common is through phishing emails or downloading things from unauthorized websites.

> Prevention: A proactive approach is the best defense. Common sense dictates users and organizations should have the latest anti-malware programs installed, for starters. It’s also important to recognize suspicious links, files, or websites, which are effective ways of implementing malware. Often, a combination of caution and anti-virus is enough to thwart most malware concerns (FutureEnTech,2021).

Password Theft

Password theft is another common risk factor, if your password is not strong enough it can be cracked by the rockyou.txt file or guessed. Another way to crack a password is to keep it stored online.

> Prevention: There are several reasons for losing a password. Attackers may guess the password or use “brute force” programs to cycle through thousands of potential attempts. They may also steal it from an unsafe location or use social engineering to trick a user into giving it away. Two-factor authentication is a robust protection method, as it requires an additional device to complete the login. Additionally, using complicated logins thwarts brute force attempts (FutureEnTech,2021).

Traffic Interception

This is an anomaly used by a network sniffing tool, this type of cybercrime normally targets logins or valuable data sent through a non-encrypted channel.

Prevention: Avoiding compromised websites (such as those not using HTML5) is an excellent proactive defense. Encrypting network traffic – such as through a VPN – is another preventive method (FutureEnTech,2021).

Phishing Attacks

One of the biggest and most common cyber attacks. Phishing is using emails with fake links that try to be someone else so you click on them and compromise your information. No one should click an email they are unfamiliar with.

Prevention: Generally, a common-sense approach to security is the best prevention. Phishing messages are often rife with spelling and syntax errors. Official emails from organizations do not request personal data, so this is a giveaway there is malicious intent (FutureEnTech,2021) .

DDoS

Distributed Denial of Service is an attack method in which malicious parties target servers and overload them with user traffic. When a server cannot handle incoming requests, the website it hosts shuts down or slows to unusable performance.

Prevention: Stopping a DDoS requires identifying malicious traffic and halting access. This can take time depending on how many malicious IPs are used to distribute the attack. In most cases, servers need to be taken offline for maintenance (FutureEnTech,2021).

Cross-Site Attack

Referred to as an XSS attack. In this instance, a third party will target a vulnerable website, typically one lacking encryption. Once targeted the dangerous code loads onto the site. When a regular user accesses said website, that payload is delivered either to their system or browser, causing the unwanted behavior. The goal is to either disrupt standard services or steal user information.

> Prevention: Encryption is usually required on the host's side. Additionally, providing the option to turn off page scripts is vital to thwart a malicious payload from activating. Users can also install script-blocker add-ons to their browser if they prefer additional browsing control (FutureEnTech,2021).

Zero-Day Exploits

Occurring after the discovery of a "zero-day vulnerability," an exploit is a targeted attack against a system, network, or software. This attack takes advantage of an overlooked security problem, looking to cause unusual behavior, damage data, and steal information.

> Prevention: Stopping exploits is challenging, as it relies on the vendor both discovering the loophole and releasing a fix for it. In some cases, a zero-day vulnerability can exist for an extended period before its discovery. Users must maintain good safety habits until a fix is released (FutureEnTech,2021).

SQL Injection

An SQL attack is essentially data manipulation, implemented to access information that isn't meant to be available. Essentially, malicious third parties manipulate SQL "queries" to retrieve sensitive info.

Prevention: Implementation of smart firewalls is one prevention method; application firewalls can detect and filter out unwanted requests. Generally, the most effective way is to develop code that identifies illegal user inputs(FutureEnTech,2021).

MitM Attack

A Man-in-the-Middle attack occurs when a third-party hijacks a session between client and host. The hacker generally cloaks itself with a spoofed IP address, disconnects the client, and requests information from the client.

Prevention: Encryption and use of HTML5 are recommended (FutureEnTech,2021).

Ransomware

A nasty variant of malware, ransomware installs itself on a user system or network. Once installed, it prevents access to functionalities (in part or whole) until a “ransom” is paid to third parties.

Prevention: Removal is challenging once installed. Keeping anti-virus updates and avoiding malicious links are the best current prevention methods. Also, current backups and replications are key to keeping ransomware attacks from becoming catastrophic (FutureEnTech,2021).

Cryptojacking

Cryptojacking is an attempt to install malware that forces the infected system to perform “crypto-mining,” a popular form of gaining crypto-currency. This, like other viruses, can infect unprotected systems. It is deployed because the act of crypto-mining is hardware intensive.

Prevention: Keep all security apps/software updated and make sure firmware on smart devices is also using the latest version. Cryptojacking can infect most unprotected systems (FutureEnTech,2021).

Drive-By Attack

In a drive-by-attack, malicious code is delivered onto a system or device. The distinction, however, is that no action is needed on the user end, where typically they need to click a link or download an executable.

Prevention: Avoid suspicious websites. Normally, compromised websites are flagged by search engines and anti-malware programs (FutureEnTech,2021).

Trojan Virus

Trojan malware attempts to deliver its payload by disguising itself as legitimate software. One technique used was an "alert" a user's system was compromised by malware, recommending a scan, whereby the scan delivered the malware.

Prevention: Avoid downloading programs or executables from unrecognized vendors or those that attempt to alarm the user to a serious problem (FutureEnTech,2021).

Policies, Access Controls, and Procedures

1. Acceptable Use Policy (AUP)

This allows the IT team to draw a contract for employees to sign. This contract will tell employees what they can and can not do with company computers and any equipment. This must be a contract where the employees understand that violations of any rule will be met with automatic departure from the company. By them signing this they both understand and agree to the terms set by the IT team

2. Access Control Policy (ACP)

ACP outlines the access available to employees in regards to an organization's data and information systems. New Yorks Finest Hospital operates on a zero-trust policy and only allows mitigation of information from department to department with IT supervision. Our data is important and if not in the hospital sector all information must be handled with the utmost care and confidentiality. Policies that are in place are the Access Control and Implementation Guides. Other items covered in this policy are standards for user access, network access controls, operating system software controls, and the complexity of corporate passwords (Hayslip, 2018).

3. Change Management Policy

A change management policy refers to a formal process for making changes to IT, software development, and security services/operations. The goal of a change management program is to increase the awareness and understanding of proposed changes across an organization and to ensure that all changes are conducted methodically to minimize any adverse impact on services and customers (Hayslip, 2018).

4. Information Security Policy

This is a high-level policy that covers our security control. This ensures that all employees who use information technology assets within the breadth of the organization, or its networks, comply with its stated rules and guidelines.

5. Incident Response (IR) Policy

This policy is in case anything happens to the company in a cyber attack. It identifies the chain of command as well as what to do in case of any cyber breach. This policy also outlines the authority that the company must report to, due to hospital cybersecurity regulations all cyber breaches must be reported in the first 24 hours.

6. Remote Access Policy

This policy allows the employees to understand how to use their companies that have been issued out to them by the company when working from home. It outlines how to remote into the network along with the hours of use and how to log into the VPN as well as what to do and what not to do with the computer

7. Email/Communication Policy

A company's email policy is a document that is used to formally outline how employees can use the business's chosen electronic communication medium. This policy cover email, blogs, social media, and chat technologies. The primary goal of this policy is to provide guidelines to employees on what is considered the acceptable and unacceptable use of any corporate communication technology.

8. Disaster Recovery Policy

Our disaster recovery plan will generally include both cybersecurity and IT teams' input and will be developed as part of the larger business continuity plan. If the event has a significant business impact, the Business Continuity Plan will be activated.

9. Business Continuity Plan (BCP)

The BCP will coordinate efforts across the organization and will use the disaster recovery plan to restore hardware, applications, and data deemed essential for business continuity. BCP's are unique to each business because they describe how the organization will operate in an emergency (Hayslip, 2018) .

Communication Networks.

New yorks Fines like any hospital must communicate fast and efficiently, our data can mean a life or death situation when someone is on a hospital stretcher. With this in mind, it is our job to make sure that all information is secure and safely transmitted with little or no interference. To do that we implement a firewall between an internal trusted network and an external network connection, this includes the internet or an untrusted part of an intranet. The firewalls consist of devices called a screening router and a bastion host.

> The screening router allows only messages from a specified list of trusted parties or locations to enter the system. Such requests are directed to the bastion host, which is configured securely to run only a limited set of trusted and necessary services for external users-for example, e-mail routing or remote terminal connections (with strong user

> authentication). Communication packets for authorized services are passed through "proxy" handlers in the firewall, which monitor packet types and sequences to give increased assurance of appropriate use. The router or firewall should be configured to prevent users from making it appear as though they are trusted parties so that an outside workstation cannot appear to be an internal trusted workstation, should prohibit unsafe connections (e.g., for the Network File Service protocol), should prevent viewing internal Domain Name Service information (the host's Internet address information containing details about its internal network configuration), should require direct console log-ins to control critical firewall system functions, and should keep full audit trail information that cannot be modified once written.(Argaw,2020)

Critical Electronic Device

In New Yorks Finest we Define Critical devices such as beds, in-house treadmills, intravenous pumps, and monitors, as well as implantable and connected devices such as pacemakers, and wearable devices that monitor, and record health and lifestyle data can now be connected to clinicians' devices. These devices tend to be a high-risk fact as they may become a weak point in the security chain, in which a malicious user can spread malware. Altho the security of these devices is a high priority, it is difficult to implement a strict security policy due to their diversity of them. With medical devices located in close proximity to clients, it can increase risks to hospital operations and patient safety. Medical devices with low battery power or the built-in resources to efficiently employ security measures such as encryption and forensic processes, threat modeling activities, and malware detection.

> Devices designed to function in isolation often end up integrated into the network, whereas physical security of the wearable devices is nearly impossible as they do not typically have long life spans and their operating system or relevant platforms become outdated relatively quickly(Argaw,2020).

For this it is taken by the department to vet both where they are buying from as well as the lifespan of said device, equipment maintenance must be done once a week to all medical-device thus ensuring their security. New York Fines has developed and implemented a patching policy that minimizes equipment downtime and enables timely updates through collaboration with the external manufacturing community and internal stakeholders. Department heads should develop and budget for life-cycle management to retire devices that cannot be replaced right away.IT must maintain a regularly updated inventory of all devices on the network (authorized and unauthorized). Due to doctors using their devices we have implemented a BYOB policy for all healthcare staff at this time. We have implemented reasonable measures and policies to block connectivity of unapproved personal devices, and are working with DUO for mobile device management and software distribution systems.

Handling of Critical Information.

In healthcare, all information should be deemed as critical information. When dealing with people's personal information it needs the highest level of protection at all times while also making sure the information is given speedily and correctly. No information must be mishandled or given to the wrong person.

> Information sharing facilitates situational awareness and a solid understanding of threats and threat actors, their motivations, campaigns, tactics, and techniques. Information sharing should include all stakeholders: providers, manufacturers, suppliers, payers, and electronic record providers, as well as the government where applicable(Argaw,2020).

New York Fines implements the National Health Information Sharing and Analysis Center (NH-ISAC) networks for all healthcare information that is distributed throughout the hospital and third-party companies.

Privacy-conscious data sharing and processing

Sharing information across departments and third-party companies in the hospital is a vital asset for both effective patient care and meaningful research. New York Fines implements advanced cryptographic mechanisms, homomorphic encryption, trusted hardware, secure multiparty computation, and strong trust distribution techniques such as distributed ledger technologies. The implantation of this will allow the hospital to communicate fast, efficiently and keep all data safe from cyber-attacks. The use of these technologies also allows the company to :

- Achieving a more fine-grained control on access permissions, hence reducing or avoiding the need for privileged accounts to third parties
- Implementing minimization principles on the released data for the agreed usage, in line with the latest and stricter data protection regulations and minimizing the risk of breaches and intentional or unintentional data misuse,
- Keeping individual and identifiable data within the confines of the security perimeter of the medical institution that governs them, and
- Enabling distributed logging and access control management, hence avoiding single points of failure and greatly reducing the effect of a breach and the risk of a successful attack, while allowing for more advanced implementations of audibility, accountability, and incident recovery

Risks From Insecure Behavior of Employees.

Vulnerability management, patch management

This is due to an employee being lazy. You must always update any software at the moment that a new patch is realized. If not, the employee will be reprimanded. Patch management will be done once a week when necessary you must always check if a new patch is given, the patch must be set for the computer before leaving the office or before office hours are over. For the computers in the hospital, they will be a patch in sectors. Each sector will be given a number from 1 to 700, only 100 computers will be patched a day, this will put a total of 10 computers from each department in the hospital down for about 1 to 3 hours leaving 90 computer in each department operational.

Administrative privileges and administrative multifactorial authentication

The risks associated with granting administrative privileges to users in health facilities are immense. New Yorks Finest only grants administrative privileges in a controlled and restrictive manner, to minimize the number of such accounts to an enterprise-dependent manageable sum. These accounts should be inventoried, monitored for abnormal use, and evaluated for log entries. To avoid malicious insider threats, New York's fines enforce local password policy and revisit their criteria for privileged access in addition to the vetting of users.

Incident response plan

Our Incident response plan is consistently tested, exercised, and stored offline. This plan has been approved by all necessary stakeholders identified and signed off on. In this plan there are 5 designated team members and a cybersecurity leader (This CISO).each member has a vital role to plan in case of a cyber breach and is vetted each month to understand their role and responsibility. Each of these members must also attend prevention training every 3rd week. A notification system has been established between the health facility and the manufacturers as well.

Incident Response Management

Identify and Document Incident

When responding to an incident it is important to only tell people who have a need to know about the incident. It is possible that an insider is violating law or policy. Allowing them to know they are being watched or investigated gives them the opportunity to destroy valuable evidence. Throughout the process take good notes. An incident response plan should be set up to address a suspected data breach in a series of phases. Within each phase, there are specific areas of need that should be considered.

The incident response phases are:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Preparation

- Ensure your employees are properly trained regarding their incident response roles and responsibilities in the event of a data breach
- Develop incident response drill scenarios and regularly conduct mock data breaches to evaluate your incident response plan.
- Ensure that all aspects of your incident response plan (training, execution, hardware and software resources, etc.) are approved and funded in advance

2. Identification

- When did the event happen?
- How was it discovered?
- Who discovered it?
- Have any other areas been impacted?

- What is the scope of the compromise?
- Does it affect operations?
- Has the source (point of entry) of the event been discovered?

3. Containment

- What's been done to contain the breach short term?
- What's been done to contain the breach long term?
- Has any discovered malware been quarantined from the rest of the environment?
- What sort of backups are in place?
- Does your remote access require true multi-factor authentication?
- Have all access credentials been reviewed for legitimacy, hardened, and changed?
- Have you applied all recent security patches and updates?

4. Eradication

- Have artifacts/malware from the attacker been securely removed?
- Has the system been hardened, patched, and updates applied?
- Can the system be re-imaged?

Recovery

- When can systems be returned to production?
- Have systems been patched, hardened and tested?
- Can the system be restored from a trusted backup?
- How long will the affected systems be monitored and what will you look for when monitoring?

- What tools will ensure similar attacks will not reoccur? (File integrity monitoring, intrusion detection/protection, etc)

6. Lessons Learned

- What changes need to be made to the security?
- How should employees be trained differently?
- What weakness did the breach exploit?
- How will you ensure a similar breach doesn't happen again?

Inform Internal and External Individuals Affected

1.1 Incident command system for Few Yorks Finest

New Yorks Finest implements a well known fire service to handle and respond to various incidents. We have classified cyber incidents as fires when dealing with them within computer systems and networks. This system is designed to allow inter-agency operation for incidents small to large and complex. The ICS is based on the following 14 management characteristics that provide strength and efficiency to the total system

• Common Terminology – Assures that all participants are using the proper terminology for incident response and required resources.

• Modular Organization – This allows for a compartmentalized approach that allows resources or functions to be brought in based on the complexity and severity of the incident.

- Management by Objectives – Establishes all-encompassing objectives and goals • Incident Action Planning – Provides a centralized approach to the planning of the response to the incident as well as setting priorities.
- Manageable Span of Control - Span of control defines how many people (or things) each individual can manage. The typical range is 3 to 7 with 5 being optimal.
- Incident Facilities and Locations – Numerous and varied facilities may be needed for the incident, these include command posts, staging areas, rest areas, etc.
- Comprehensive Resource Management – This means maintaining a comprehensive view of resource utilization. Resources in this case include equipment and personnel.
- Integrated Communications – Establishes a common communication system to address the equipment, systems, and protocols necessary to achieve integrated voice and data communications.
- Establishment and Transfer of Command – At the beginning of any incident command (who is in charge?) must be established. As the incident grows it may be necessary to transfer the command, this requires a briefing that includes the current status, the plan, and other important information
- Chain of Command and Unity of Command – The chain of command assures that subordinates report to supervisors. The concept actually comes form the military where it is not desirable to have privates reporting to generals.
- Unified Command – This is a concept that allows various agencies and entities with different functional, geographical and legal authorities to work together.
- Accountability – This is the management of personnel and resources involved in the incident.
- Dispatch/Deployment – Personnel and resources only respond when requested.

• Information and Intelligence Management – This is the process of gathering, analyzing, assessing, sharing, and managing incident-related information and intelligence.

The incident command sections are defined as follows 15]:

• Command – Incident Commander (IC), Public Information Officer, Liaison Officer

• Operations – Manages the tactical operations

• Planning – Resources, Situation, Documentation (Understanding the situation, establish Priorities, and Strategy)

• Logistics – Communication, Food, Supply, Facilities

• Finance/Administration – Procurement, Compensations, Claims, Cost

• Intelligence/Investigations – Post-incident investigation or intelligence gathering.

Not all components of the ICS are invoked at every emergency incident. Each component is invoked as needed. It is possible that the incident commander will also be the operations chief, planning chief, logistics chief, and finance chief.

Investigate the breach

2.1 Identification

The goal here is to examine the events, analyze them, and determine if there is an incident. As mentioned previously, not all events are incidents. Examples of this are phishing emails that are not opened, a user on a Linux system surfing to a website with known windows exploit, and a large increase in ftp traffic that is authorized.

2.2 Containment

New Yorks Finest classified containment in two catagorigores, Long term and short term goals. With in the short term goal of confinement it is our cyber and IT teams job to

1. Stop communications with hackers from systems
2. Isolate all systems
3. Identify malware or malicious programs
4. unplug the network cable, disable the switch port, put in ACLs on routers or firewalls, and as a last resort unplug the power.
5. keep a low profile, do not let the attacker know that you have discovered their activity.
6. Make a system image to include the file system, and memory.
7. Take pictures of the area and the current state of the screen\

All of these steps are important in knowing how the virus is working as well as proving that We at New Yorks Fines are not at fault, it is also instrumental that we report these findings to all agencies that are concerned within the first 72 hours of the initial breach.

Long term goals are also important when it comes to these types of breach below is an outline of long term goals once a breach has happened:

1. applying patches to the affected system and other similar systems.

2. changing passwords
3. adding firewall rules
4. Remove any accounts that were used by the attacker
5. shutdown hacker processes

It goes without saying that the hackers malware must be removed fully and eradicated from the system so they were not added into the goals, this is our first priority.

2.3 Eradication

The eradication is one of the most important steps of this process, for this the system will be cleaned and attacker artifacts are removed.from this point on we will be looking at the forensic analysis. When the malware is identified a internet or internal search will be runed revealing the characteristics of the malware. If it can not be identified the malware will be exported to a VM and monitored closely until the team has a better understanding. Before executing the backup files they must be checked for malware or an attacker. If a rootkit was installed this will modify the operating system itself, in this case, reformat the hard drive and reinstall the operating system. Once the system is restored perform a vulnerability scan using Nessus and patch all vulnerabilities.

4.5 Recovery

Prior to putting the system back into production check the operation of the system against the test plan and baseline documentation. This should be done by the system administrator and the owner of the system. The owner of the system makes the final decision on putting the system back into production. Once in production monitor the system closely and check carefully for signs of compromise.

4.6 Follow Up

In the follow-up phase,all weak links and lessons learned from the attack are documented. A report is generated by the cyber team this report should contain :

- how the attacker got in
- what was done
- how the issue was found
- what was done to fix it
- recommendations to prevent future attacks by the same method

4.7 Seven Deadly Sins

1. Failure to report or ask for help
2. Incomplete or nonexistent notes
3. Mishandling or destroying Evidence
4. Failure to create working images
5. Failure to contain or eradicate
6. Failure to prevent re-infection

7. Failure to apply lessons learned

Enforcement

GDPR requirements

Security and breach reporting requirements are covered in Articles 32-34 of the GDPR. Controllers and processors are required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The assessment of what might be appropriate involves considering the context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals. Appropriate measures are set out as possibly including:

- pseudonymization and encryption;
- ensuring confidentiality, integrity, availability, and resilience of processing systems and services;
- ability to restore availability and access to personal data in a timely manner in the event of an incident; and
- the regular testing and evaluating of technical and organizational measures designed to ensure the security of data processing.

Controllers and processors are also required to ensure anyone acting under their authority accessing the personal data, does so only in accordance with their instructions. Compliance may) be demonstrated by adherence to an approved code of conduct or certification mechanism (GDPR, 2018).

The Article 29 Working Party (WP29) guidance identifies three types of breaches. Some breaches may engage all three elements:

- confidentiality breach – unauthorized or accidental disclosure of or access to personal data;
- integrity breach – unauthorized or accidental alteration;
- availability breach – accidental or unauthorized loss of access to or destruction of data (e.g. by a power cut or systems failure).

All breaches must be recorded alongside the decision-making process engaged to decide whether or not to report the breach. Only breaches that are likely to result in a risk to the rights and freedoms of data subjects have to be reported to the Supervisory Authority (SA).

Timing of breach reporting to the SA

Data controllers are required to report a personal data breach to the competent SA without undue delay and, where feasible, not later than 72 hours after becoming aware of it unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

If a notification is made after the 72 hour period has expired, the data controller must explain the reasons for the delay.

The notification must include at least:

- a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned;
- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

Communication of a personal data breach to the data subject

Where a breach is reported to an SA and not to the data subjects, the SA may subsequently require the data controller to notify affected data subjects.There is no requirement to make a notification to the data subject where any of the following conditions have been met:

- technical and organizational measures have been applied to the personal data which will render it unintelligible to unauthorized persons (such as encryption);
- the controller has taken steps to ensure the originally high risk is no longer likely to materialize; or
- to notify each data subject would involve disproportionate effort, in which case a public communication or other methods of information can be used which would inform the affected data subjects in a similarly effective manner.

How to notify data subjects

The communication must describe in clear and plain language, the nature of the breach and at least:

- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

Breach reporting obligations on processors

Data processors are required to notify controllers of a personal data breach without undue delay, which effectively means immediately.

NISD requirements

NISD is relevant to you if you are an Operator of an Essential Service (OES) or if you are a Digital Service Provider (DSP). Where sectors are subject to sector-specific Union legal acts relating to information and network security, these will take precedence.

How will organizations be regulated?

Organizations will be regulated in the Member State of their main establishment which will be where their head office is located. Where an organisation is subject to NISD but does not have a main establishment in the EU, it must appoint a representative in one of the Member States in which it offers services and it will be subject to regulation in that Member State.

Incident response will be separate from incident reporting. The National Cyber Security Centre (NCSC) will be the UK's Computer Security Incident Response Team (CSIRT). Voluntary reporting can be made to either the CA or the NSCS. Incident response support on cyber related incidents will be provided by the NCSC where required. CAs or possibly the relevant Lead Government Department will provide support for non-cyber or resilience incidents (e.g. hardware failure, fire, physical damage) (GDPR, 2018).

Operators of essential services

- Member States are required to identify OESs in categories set out in Annex II of the Response with an establishment in their territory by 9 November 2018. These categories include operators of essential services in the energy, transport, financial services (including banks), health and drinking water supply and digital infrastructure (including internet exchange points, domain name system service providers and top level domain name registries). Lists must be reviewed and updated at least every two years. The UK has published its list of OESs and their Competent Authorities (CAs) in the Response.
- Member States may make their own rules as to how to identify OESs in each sector but this is to be decided against the broad criteria that the entity provides a service essential for the maintenance of critical societal and/or economic activities where the provision of that service depends on network and information systems and an incident to the network and information systems of that service would have significant disruptive effects on its provision. Whether or not a disruption has a significant disruptive effect should take into account the number of users relying on the service, the dependency of other essential service sectors on it, the impact the incident might have, the market share and geographic

reach of the entity and its importance in maintaining a sufficient level of service taking into account availability of alternative providers.

Security and notification requirements for operators of essential services

- Member States must ensure all OESs take appropriate and proportionate technical and organisational measures to manage risks (defined as “any reasonably identifiable circumstances or event having a potential adverse effect on the security of networks and information systems”) posed to the security of networks and information services which they use to deliver their services and to minimise the impact of any network security incidents with a view to ensuring continuity of service.
- OESs must notify the competent authority or the CSIRT of incidents having a significant impact on the continuity of the service they supply. Notifications must be made without undue delay (and within 72 hours in the UK) and must contain enough information to allow the competent authority or the CSIRT to determine any cross-border impact of the incident. To assess the nature of the incident, the number of affected users, the duration of the incident and the geographical spread of its impact must be taken into account.
- The public may be informed of an incident by the CA or the CSIRT.

2.2 HITECH Act The HITECH Act was implemented as part of the American Recovery and Reinvestment Act of 2009. Under this act, HIPAA was strengthened to include fines, and a data breach notification. In order to determine if a breach actually occurred the Hospital must perform an investigation to determine what data may have been breached. Civil Penalties are listed in the Table belwo :

Violation category	Each violation	All such violations of an identical provision in a calendar year
Did Not Know	$100–$50,000	$1,500,000
Reasonable Cause	$1,000– $50,000	$1,500,000
Willful Neglect—Corrected	$10,000– $50,000	$1,500,000
Willful Neglect—Not Corrected	$50,000	$1,500,000

Cost

Cost elements can be divided up into the following:

1. Per-incident loss estimates based on insurance claims, payout data, and activity-based incident cost estimates

2. Aggregate loss or impact estimates on the national scale

3. Academic or research papers on the short- and long-term impacts of cyber incidents

4. Individual case studies with scenario-based impact estimates.

These elements are what help New Yorks Finest make their assumption in the overall cost of a company breach. While the numbers aren't exact and may vary depending on the servitity of the breach this is the estimate we have concluded to.

(Cost per event in the millions)

Event Type	Number of Events	Mean	Standard Deviation	Median	Max
Data Breach	602	$5.87	$35.70	$0.17	$572
Security Incident	36	$9.17	$27.02	$0.33	$100
Privacy Violation	234	$10.14	$55.41	$1.34	$750
Phishing	49	$19.99	$105.93	$0.15	$710
Total	921	$7.84	$47.28	$0.25	$750

Response and Update Policies

Below are the steps that New Yorks Fines takes to review their response plan as well as maintain and update to fit the new cyber threats that have arised. We learn and are always adapting and improving on our risk models.

1) The person who discovers the incident will document all actions taken from this point on . List possible sources of those who may discover the incident. The known sources should be provided with a contact procedure and contact list. Sources requiring contact information may be:

a) Helpdesk.

b) IT Manager.

c) government entities

List all sources and check off whether they have contact information and procedures. Each source will contact one 24/7 reachable entity such as a grounds security office. Those in the IT department may have different contact procedures than those outside the IT department.

2) If the person discovering the incident is a member of the IT department or affected department, they will proceed to step four.

3) The Helpdesk/manager/IT Staff will refer to the IT emergency contact list or affected department contact list and call the designated numbers in order on the list. The Helpdesk will log:

a) The name of the caller.

b) Time of the call.

c) Contact information about the caller.

d) The nature of the incident.

e) When the event was first noticed, supporting the idea that the incident occurred.

4) The IT staff member or affected department staff member who receives the call will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the incident response manager using both email and phone messages. The staff member will log the information received in the same format as the grounds security office in the previous step. The staff member could possibly add the following:

a) Is the system affected business critical?

b) What is the severity of the potential impact?

c) Name of system being targeted, along with operating system, Internet Protocol (IP) address, and location.

d) IP address and any information about the origin of the attack.

5) Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.

a) Is the incident real or perceived?

b) Is the incident still in progress?

c) What data or property is threatened and how critical is it?

d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?

e) What system or systems are targeted, where are they located physically and on the network?

f) Is the incident inside the trusted network?

g) Is the response urgent?

h) Can the incident be quickly contained?

i) Will the response alert the attacker and do we care?

j) What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

6) An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:

a) Category one - A threat to public safety or life.

b) Category two - A threat to sensitive data.

c) Category three - A threat to computer systems.

d) Category four - A disruption of services.

7) Team members will establish and follow one of the following procedures basing their response on the incident assessment:

a) Worm response procedure.

b) Virus response procedure.

c) System failure procedure.

d) Active intrusion response procedure - Is critical or sensitive data (Personally Identifiable Information (PII), CJI, etc.) at risk?

e) Inactive Intrusion response procedure.

f) System abuse procedure.

g) Property theft response procedure.

h) Website denial of service response procedure.

i) Database or file denial of service response procedure.

j) Spyware response procedure.The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident.

8) Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.

9) Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.

10) Upon management approval, the changes will be implemented.

11) Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:

a) Reinstall the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.

b) Make users change passwords if passwords may have been sniffed.

c) Be sure the system has been hardened by turning off or uninstalling unused services.

d) Be sure the system is fully patched.

e) Be sure real time virus protection and intrusion detection is running.

f) Be sure the system is logging the correct events and to the proper level.

12) Documentation—the following shall be documented:

a) How the incident was discovered.

b) The category of the incident.

c) How the incident occurred, whether through email, firewall, etc.

d) Where the attack came from, such as IP addresses and other related information about the attacker.

e) What the response plan was.

f) What was done in response?

g) Whether the response was effective.

13) Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond, in case of an appeal.

14) Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.

15) In the event of a loss or suspected loss of criminal justice information, contact the Michigan State Police Information Security Officer via the CJIS-016 Form available on the MSP LEIN website

16) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

17) Review response and update policies—plan and take preventative steps so the intrusion can't happen again.

a) Consider whether an additional policy could have prevented the intrusion.

b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.

c) Was the incident response appropriate? How could it be improved?

d) Was every appropriate party informed in a timely manner?

e) Were the incident response procedures detailed, and did they cover the entire situation? How can they be improved?

f) Have changes been made to prevent reinfection? Have all systems been patched, systems locked down, passwords changed, antivirus updated, email policies set, etc.?

g) Have changes been made to prevent a new and similar infection? h) Should any security policies be updated?

i) What lessons have been learned from this experience?

Cybersecurity Program Maintenance

Procedures to Track Performance

New Yorks Finest prides itself high-risk on our Cyber efforts to keep our companies data safe, to do this we track performances through 12 ways. This is so the company knows the level of proficiency that is taken with each of our methods. By doing this we have secured our maturity and the companies cyber postures is still currently growing, Below are the methods used by New Yorks Finest:

1. Level of preparedness

To do this we track all devices on our network whether it is a gust, customer, or employee. Before starting the job all employees must sign an agreement acknowledging that they are being monitored, for guest or customers they must accept our monitoring and privacy to be allowed to use wifi. All employee devices are fully patched and up to date with maintenance every Tuesday and Friday. Vulnerability scans and vulnerability management controls are in place and tested every month

2. Unidentified devices on internal networks

A network intrusion detection system is put in place for any device connected to the internal network. As well as a BYOD policy that all employees must follow.

3. Intrusion attempts

We log all intrusion attempts, whether they are successful or not. This also allows us to measure the performance of your policies to see what needs to be hardened.

4. Security incidents

All incidents are logged and managed. It is important that we knowledge the mistakes of the company and learn from them c.

5. Mean Time to Detect (MTTD)

MTTD measures how long it takes your team to become aware of indicators of compromise and other security threats (Cipher,2020).

6. Mean Time to Resolve (MTTR)

This is a response to how quickly our team can react and resolve an issue. By tracking this we can better understand the strength and wellness of our team and put countermeasures in place.

7. Mean Time to Contain (MTTC)

This is a measure of time in which the team notes the time it takes to close and identified attack vectors?

8. First party security ratings

For the company’s stakeholders, we use this method, this is an easy way for the average man to understand what is going on on the cyber front. The company is given a simple A-F letter grade based on 50+ criteria including network security, phishing risk, DNSSEC, email spoofing, social engineering risk, DMARC, risk of man-in-the-middle attacks, data leaks, and vulnerabilities (Tunggal, 2021). Security ratings can feed into your cybersecurity risk assessment process and help inform which information security metrics need attention(Tunggal,2021).

9. Patching cadence

A common method used with cybercriminals is to exploit the time in between patch and updating machines, due to this New Yorks Fines measures the time it takes to maintain computers and patchwork that is done by our team. By doing this we secure the window of opportunity that the cybercriminals take advantage of.

10. Access management

New Youeks fines implement a zero-trust policy. With that said there are still certain individuals with access to multiple departments, due to this we manage all employee's access levels to make sure they are needed for their jobs.

11. Vendor patching cadence

This metric involves determining how many risks your vendor has and how many critical vulnerabilities are yet to be remediated (Tunggal,2021).

12. Meantime for vendors incident response

As a company that focuses on the future and safety of our brand, we also monitor the MTTR for the company affiliated with us. By doing this we secure our system and make sure that there is no breach through a 3-party vendor.

Monitor and Measure Performance for Areas of Improvement

Areas of improvement are very important to a company's maturity level, you should always monitor and measure the performance of your safeguards high-risk in high risk areas. Low risk should not be ignored as well, with this said below are the Procedures New Yorks finest implement keep improving upon itself:

1. Mean-Time-to-Detect and Mean-Time-to-Respond

As we stated before in the previous section we employ MTTC to measure the time it takes to contain a breach, but we also like to employ the MTTI as well, a combined timing of the time it takes to identify the problem along with how fast it was contained is crucial in measuring the companies responses and how effective it is.

2. Number of systems with known vulnerabilities

Previously we have stated that managing patching and updates are necessary, but the scanning process for these high-risk vulnerabilities is just as important. Knowing the vulnerabilities of the devices is necessary whether it is of low risk or high. You should know all the weak points of the company no matter how minute.

3. Number of SSL certificates configured incorrectly

An SSL certificate is a small file that certifies the ownership of a cryptographic key to the website or company with which data is being exchanged, guaranteeing the authenticity of the transaction. Monitoring the security requirements for each certificate, as well as ensuring that they are properly configured on servers, prevents them from falling into the wrong hands and that your company's digital identity is not used to steal user information (Cipher,2020).

4. Volume of data transferred using the corporate network

Altho employees have limited access to the internet, only being allowed to access websites and apps the companies approve it is still vital to know what the employees are downloading (Cipher,2020). This is a known weak point for the company and is why data is always being monitored.

5. Number of users with "all-level" access employees.

It is crucial to monitor the few employees with access to all departments and make sure this privilege is not being misused or given to the wrong person.

6. Number of days to deactivate former employee credentials

Once an employee departs from a company their credentials should be terminated asap, and will not remain in the system for more than 24 hours. We monitor the systems to make sure that this happens, as well as time the employee's credentials terminate.

7. Number of communication ports open during a period

As a general rule, avoid allowing inbound traffic for NetBIOS (UDP 137 and 138, TCP 135-139 and 445). Be observant of outbound SSL (TCP 443): a session that stays active for a long time could be an SSL VPN tunnel that allows bi-directional traffic. Any common ports for protocols that allow remote sessions, like TCP 22 (SSH), TCP 23 (telnet), TCP 3389 (RDP), and TCP 20 and 21 (FTP) should be monitored for a length of time (Cipher,2020).

8. Frequency of review of third party accesses

Once a third-party client, freelancer, or temp worker's contract is completed their credentials must be removed from the system or placed into a non-activated state (if long-term on and off-contract is in place) within the first 24 hours of competition.

Identify New Threats, Vulnerabilities, or any Countermeasures

All security professionals must be well versed in identifying new threats, vulnerabilities, and any countermeasures. The steps listed below are the procedures that New Yorks Fines implements to keep up our knowledge and effectiveness of the cyber programs.

Strong Password

Strong passwords are the backbone of cybersecurity. We implement a 9 character 2 symbols and 1 number password check for anyone with any employee that is to sign in to the network.

Avoid Public PCs

There is a no public access policy, in this policy, we outline that in no way, shape, or form any information of the company including work emails can not be accessed through a public pc, internet cafe, or a network outside of the company.

Locking up the Windows

All company-issued laptops must be locked somewhere safe at night. Any room with a computer in it must be turned off and locked into the respected room they are assigned.

Don’t follow the Security Breach link

Most of the time while accessing your email, you get messages of your email getting breached. It leads you to a page where you can change your password. Most of the time it is a fake message. The best practice is to avoid such messages. You need to double-check your client’s account to ensure that the message is genuine (Eshna,2019).

Encryption

All data is transferred through encrypted channels, there is no exception to this rule. New yorks fines uses 3 types of encryption to secure our data as well as having data storage that is fully encrypted.

Vulnerability and Patch Management as done by IT Security Management

This is done every Friday and Tuesday, the computers will be broke up into different departments, with each department having 10 computers at a time will be updated and patched. Once the 10 computers are back online the next set of computers will follow.

Checking Vulnerabilities

New Yorks Fines does have many different types of vulnerability checking methods as well as a safeguard. Below are the measures we implement throughout the company:

- Network Scanning
- Firewall
- Penetration Testing
- Verifying Vulnerabilities

Identifying Vulnerabilities

There are many different types of Vulnerabilities to a company these are some of the more notable Vulnerabilities that the company must be aware of and proactive with:

Malware

Malware can be downloaded or uploaded to the system. The number 1 way malware enters a computer is through phishing scams. Workers must always be vigilant when receiving an email.

Server

Servers are what connect the computers to a network. The server allows a client to request data to be transferred through the system and to the correct computer the client wants to message.

Applications

All applications come with a risk. This being said New Yorks Fines has made a list of applications that can connect to the hospital's networks and what can not. These include but are not limited to pirating sites, any site that operates off HTTP, HTML sites...etc

Mitigating vulnerabilities

Being able to identify vulnerabilities is only half of the job, the next step is a course of action to mitigate them, below are the steps New Yorks fines takes to do so:

Patch

All systems must be patch the moment a new patch comes out, this takes priority when it comes to new yours fines computers and devices.

Patch Management

All patches must be done Tuesday and Fridays, this time will allow the team to coordinate with each other to get all the computers to be patched within those 2 days.

Stronger security in adherence with global security provisions

This system requires a single configuration for firewall, VPN, and other security systems. A single console does the trick in this system. All the work is done automatically. Computers are deployed to handle all the possible threats posed by them. The situation cannot be better than ever when the same thing is treated for the betterment (Eshna,2019).

Obtain Feedback on the Effectiveness of Policies

To obtain feedback on the effectiveness of policies New York's Fines hospitals implements a review of all policies every 6 months or if any major changes occur such as:

- Complying with new global laws, such as the General Data Protection Regulation
- State changes in cybersecurity regulations
- A data breach at the company
- New management
- Adopting new technologies
- New types of threats

Along with this if any of the following scenarios were ever to happen there must be a review and feed pack to all of the safeguards put in place:

• Implementation of new information services and systems; or significant changes to existing university information services or systems, that may store or transmit Export Controlled or Restricted data (see Data Classification and Data Types for additional information)
• Implementation of new critical infrastructure or significant changes to existing critical infrastructure.
• Implementation of a new enterprise system or significant changes to existing enterprise systems.
• Implementation of new systems or significant changes to existing systems, which permit third-party access to university systems or data.

- Implementation of cloud services for the storing or processing of Export Controlled, Restricted or Controlled data.

Technical Tools to Monitor the Internal and External Environment

Below are all technical controls as well as monitoring tools for both our internal and external environment:

Access control

Access controls are an essential part of security; they not only help the company from preventing outside intruders by limiting access but also insider threats by limiting the resources and access to each part of the network. This allows easy isolation from the network if a threat is to be discovered.

Anti-malware software

Malware can be downloaded or uploaded into the systems, Anti-malware software will always for early detection to any problem that can arise. It is important to understand viruses like trojans can hide themselves among apps and files, this device should be used to detect malware but once it is done removing, an employee from the cyber team must do a thoro removal malware review of the infected computers before being allowed back into the network.

Anomaly detection

An ADE allows for quick response time. It scans the network and notifies the professional when there is an anomaly on the network. This can help employees report to the heads of the department and allows the Cyber team to understand the weak points of the system. This will allow the cyber team to harden defenses for future ventures.

Application security

In the medical industry, we use many apps for patient care. This is a weak point in our systems having application security is a must for any app associated with our company, this also includes 3rd party vendors. We will not form a partnership with any application that does not have safeguards in place.

Data loss prevention (DLP)

Hackers do not target companies, they target people. Human error is a big factor in breaches. With this known, we have set in place a Data loss prevention plan. These outlines conduct at work along with policies and safeguards in place.

Email security

We implement Microsoft email security as well as a 3rd party vendor to take control of the email security. Some of the things they do to ensure our security is endpoint encryption, SSL injection, and password protection.

Endpoint security

Endpoint security is to be treated as an add-on, and not a solution. With our BYOD policy in place and employees working from home we must add this to every computer in the office or out of.

Firewalls

All computers that are used on the New Yorks Fines hospital network must have a firewall in place to block access to non-authorized traffic.

Intrusion prevention systems

This system constantly scans and analyzes network traffic/packets, and must be monitored by an employee at all times. Due to false positives on the network, a security professional must swiftly investigate all attacks registered by the system.

Network segmentation

Network segmentation allows you to grant the right access to the right traffic while restricting traffic from suspicious sources.

Security information and event management (SIEM)

SIEM tools and software give responders the data they need to act quickly.

Virtual private network (VPN)

All company computers must use their assigned VPNs to access the network. If an employee is working from home there VPN will be paired up with DUO, to ensure security and password protection.

Procedures for budget allocation

For the cybersecurity budget, the Chief CISO is in charge of distributing the funds, these are the steps they take to ensure the budget is being used to the fullest:

1. The first portion of the budget goes into compliance, Health care industry must abide by HIPAA and can not run without the Compliance standards being met. Some of the things this portion of the budget includes focusing on data classification, encryption, and lifecycle management.
2. After this requirement is met the next portion of the budget should be allocated to advancing the company's risk assessment. We must consistently monitor the risk controls set in place for the companies safety, to do this an assessment must be conducted every 2 weeks, if new risk is found the CISO must allocate more of the budget to these areas as per the assessment to ensure the company’s safety
3. Security training for employees is increasingly a must, this will be the next factor of the budget. All employees must understand the risk and how to prevent the company from experiencing a breach. The company is only as strong as its weakest link.
4. New Initiatives, this is the final place for the budget. Any New Initiatives the company may want to take on must-have security measures in place before becoming life or moving on the fine process of planning. This allows for the company to secure any new weak points that might accrue due to the new initiatives to take place

Procedures to catch any oversights

As humans we are prone to eros and oversight below are the following step New Yorks Fines takes to make sure those over sites are dealt with to our best ability:

1. Make Cybersecurity an Enterprise-Wide Initiative

If you see something say something, It is not only our professionals that can catch something wrong with the computers. With this said all employees must call the cyber department if anything is wrong with the computers all complaints filed will be logged and once the problem has been solved a report will be written up to the CISCO who will file them under what department they are from for consideration.

2. Test Your Cyber Protections Often

Both White Box and Black Box pen testing will happen every month. The schedule will go as follows: first month White Box pentest, second month Blox box pentest, third-month revisions from pen test results, fourth to sixth-month monitoring, then repeat.

3. Develop a Better Rapport with Your CISO

The CISO is in charge of introducing themself to the head of each department, this will allow him to build a better relationship and understand the needs of the department. From this he will finalize himself with the number of people in each department and the common IT problems with the department, this will allow him to allocate some IT members of the team to quickly fix problems so they do not stack over time.

4. Think Hard About the Skills You Need

In the cyber department, many skills are needed and all employees should share the workload, with that said before a hiring process begins the CISO will take priority over HR in writing their needs for the department. With this said 2 personnel should be assigned a specialist in the pen-testing, monitoring, and mitigation departments of the cyber team, they will be the point person for anything involving an incident and must communicate with the CISO swiftly.

5. Bring Outside Perspectives into the Boardroom

Finally, a form will be submitted every month, in the digital form all employees are required to fill out the suggestions and concerns of their department with the cyber effort, the forms questions and answers will be filed and reviewed by the CISO. Any notable suggestion will be brought up to the Stakeholders and a meeting will commence between the department head and the CISO to see if the changes should be implemented.

References

Alotaibi, Y. K., & Federico, F. (2017, December). *The impact of health information technology on patient safety*. Saudi medical journal. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5787626/.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020, July 3). *Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks*. BMC Medical Informatics and Decision Making. https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01161-7

Architecture of Health IT . (2017). *Architecture of Health IT*. Architecture of Health IT | AHRQ Digital Healthcare Research: Informing Improvement in Care Quality, Safety, and Efficiency. https://digital.ahrq.gov/key-topics/architecture-health-it.

Askar, A. J. (2019, July). *Healthcare Management System and Cybersecurity*. researchgate. https://www.researchgate.net/publication/335568182_HEALTHCARE_MANAGEMENT_SYSTEM_AND_CYBERSECURITY..

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.

Brewington, F. (2012, August 27). *Data Design Chapter 09*. SlideShare. https://www.slideshare.net/fallonbrewington/chapter-09-14085200.

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.

Criminal justice Information Center. (2020). *Example Incident Response Plan*. michigan.gov. https://www.michigan.gov/documents/msp/Example_Incident_Response_Policy_666657_7.pdf.

Cybersecurity & Infrastructure Security Agancy. (2020, October 26). *CO S ST OF A CYBER INCIDENT: YSTEMATIC REVIEW AND CROSS-VALIDATION*. cisa. https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf.

Cipher. (2020, May 28). *10 Cybersecurity Metrics You Should Be Monitoring*. Cipher. https://cipher.com/blog/10-cybersecurity-metrics-you-should-be-monitoring/.

Datica. (2019, November 11). *What Are HITRUST Requirements?* Datica. https://datica.com/blog/what-are-hitrust-requirements#:~:text=The%20HITRUST%20CSF%20is%20a,to%20achieve%20and%20maintain%20compliance.

Daniels, D. (2021, June 10). *14 Network Security Tools and Techniques*. Gigamon Blog. https://blog.gigamon.com/2019/06/13/what-is-network-security-14-tools-and-techniques-to-know/.

Executech. (2019, September 30). *Top 15 Types of Cybersecurity Risks & How To Prevent Them*.

Executech.

https://www.executech.com/insight/top-15-types-of-cybersecurity-attacks-how-to-prevent-them/.

Eshna. (2019, April 25). *Staying Ahead of e-Mail Vulnerability and Security Flaws: IT Security Management*. Simplilearn.com. https://www.simplilearn.com/e-mail-vulnerability-and-security-flaws-article.

FutureEnTech. (2021, April 28). *Types of Cyber-Attacks and How to Prevent Them*. FutureEnTech. https://futureentech.com/types-cyber-attacks-prevent/.

Future Health Concepts. (n.d.). 10 Pieces of Medical Equipment All Hospitals Need.

https://www.futurehealthconcepts.com/blog/posts/10-pieces-of-medical-equipment-all-hospitals-need.html.

GDPR. (2018). *GDPR cybersecurity and breach reporting requirements - Taylor Wessing's Global Data Hub*. Home - Taylor Wessing's Global Data Hub. https://globaldatahub.taylorwessing.com/article/gdpr-cybersecurity-and-breach-reporting-requirements.

Hayslip, G. (2018, March 16). *9 policies and procedures you need to know about if you're starting a new security program*. CSO Online. https://www.csoonline.com/article/3263738/9-policies-and-procedures-you-need-to-know-about-if-youre-starting-a-new-security-program.html.

HITrust. (2019). *Risk Analysis Guide for HITRUST Organizations & Assessors* .

https://hitrustalliance.net/. https://hitrustalliance.net/uploads/RiskAnalysisGuide.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.

Heywood, D. (2018, March 2). *Cybersecurity, data breach and incident reporting under the GDPR and NISD*. Lexology. https://www.lexology.com/library/detail.aspx?g=1b4a3144-6f76-40dd-b62f-588dc7ea004c.

Maryville University. (2021, January 22). *HIPAA Compliance and the Protection of Cybersecurity*. Maryville Online. https://online.maryville.edu/blog/hipaa-compliance-and-the-protection-of-cyber-security/.

National Research Council (US) Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. (1997, January 1). *Technical Approaches to Protecting Electronic Health Information*. For the Record Protecting Electronic Health Information. https://www.ncbi.nlm.nih.gov/books/NBK233433/.

IDG Connect. (2021, April 1). *Cybersecurity and board-level buy-in: how to speak the language of a CFO*. IDG Connect. https://www.idgconnect.com/article/3611671/cybersecurity-and-board-level-buy-in-how-to-speak-the-language-of-a-cfo.html.

Information Technology Laboratory Computer Security Division. (2020). *Release Search - NIST Risk Management Framework: CSRC*. CSRC. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1.

Kocabas, O.; Soyata, T.; Aktas, M.K. Emerging Security Mechanisms for Medical Cyber-Physical Systems. IEEE/ACM Trans. Comput. Biol. Bioinform. 2016, 13, 401–416.

Krishnan, A. (2020, December 22). *Cybersecurity budget breakdown and best practices*. SearchSecurity. https://searchsecurity.techtarget.com/tip/Cybersecurity-budget-breakdown-and-best-practices.

Lessons Learned Information Sharing. (2020). *Emergency Management Programs for Healthcare Facilities: The Incident Management System* . LLIS.gov. file:///C:/Users/cassa/Downloads/765413.pdf.

NIST. (2008). *Archived NIST Technical Series Publication* . govinfo. https://www.govinfo.gov/content/pkg/GOVPUB-C13-6c7a70faefc0886fd6368ad878f7487e/pdf/GOVPUB-C13-6c7a70faefc0886fd6368ad878f7487e.pdf.

Noori, A. S., & Najem, A. F. (2015, May 21). *Hospital Management System Design and Implementation*. Academia.edu. https://www.academia.edu/29078722/Hospital_Management_System_Design_and_Implementation.

O'Dowd, E. (2016, November 4). *Using Firewalls to Strengthen Healthcare Network Security*. HITInfrastructure.

https://hitinfrastructure.com/news/using-firewalls-to-strengthen-healthcare-network-security.

Price, N. J. (2019, July 17). *5 Steps Boards Can Take for Better Cyber-Risk Oversight*. Diligent Insights. https://insights.diligent.com/cyber-risk/5-steps-boards-take-better-cyber-risk-oversight.

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008, September 30). *Technical Guide to Information Security Testing and Assessment*. CSRC. https://csrc.nist.gov/publications/detail/sp/800-115/final.

Sriram, R. D. (2017, August 9). *Health IT at NIST - Program Overview*. NIST. https://www.nist.gov/programs-projects/health-it-nist-program-overview.

Symantec. (2018). *Cyber Security and Healthcare: An Evolving Understanding of Risk*. broadcom.com. https://docs.broadcom.com/doc/2018-istr-executive-summary-for-healthcare-professionals-en.

Tunggal, A. (2021, May 25). *14 Cybersecurity Metrics + KPIs You Must Track in 2021: UpGuard*. RSS. https://www.upguard.com/blog/cybersecurity-metrics.

WIEDERHOLD, G. I. O. W. I. E. D. E. R. H. O. L. D., & SHORTLIFFE, E. D. W. A. R. D. H. (2016). *System Design and Engineering in Health Care*. eknygos. http://eknygos.lsmuni.lt/springer/56/233-264.pdf.