Anthem, Inc.
Cybersecurity Assessment

Neil Bridges, Marcos Luchetti, Michael Turkson

Table of Contents

1 Company Profile

2 Key Assets

3 Risk Matrix Overview

4 NIST CSF Recommendations

5 Conclusion

About the Company

- $31 Billion in Earnings in 2020
- Growing industry
- Trend toward online storage of customer data
- Deals with a large amount of sensitive data
- Industry going remote
- Approximately 40 million members
- Offers PPOs, HMOs, various hybrid and speciality products, dental products, and health plan services
- Key competitors: UnitedHealth Group, Centene, Humana, HCSC

Anthem®

Key Assets

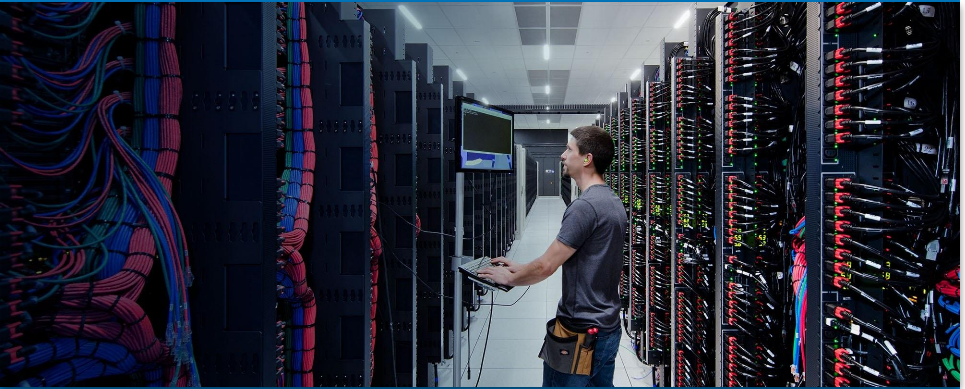
Rank	Asset
1	Cloud Data Infrastructure
2	Medical IoT Devices
3	Medical Software
4	Medical Treatment Equipment
5	Employees
6	Websites & Apps
7	Electronic Health Records
8	Payroll Systems
9	Life Support Equipment
10	Medical Laboratory Equipment
11	Durable Medical Equipment
12	Actuary Equations

Risk Matrix Overview

- Top 4 Risks:
  1. Cloud Data Infrastructure
  2. Medical IoT Devices
  3. Medical Software
  4. Medical Treatment Equipment

- This ranking was decided through a **qualitative** risk analysis of the magnitude of potential consequences (**severity**) and the **likelihood** that these consequences will occur to these assets
  - *Severity × Likelihood = Risk Score*

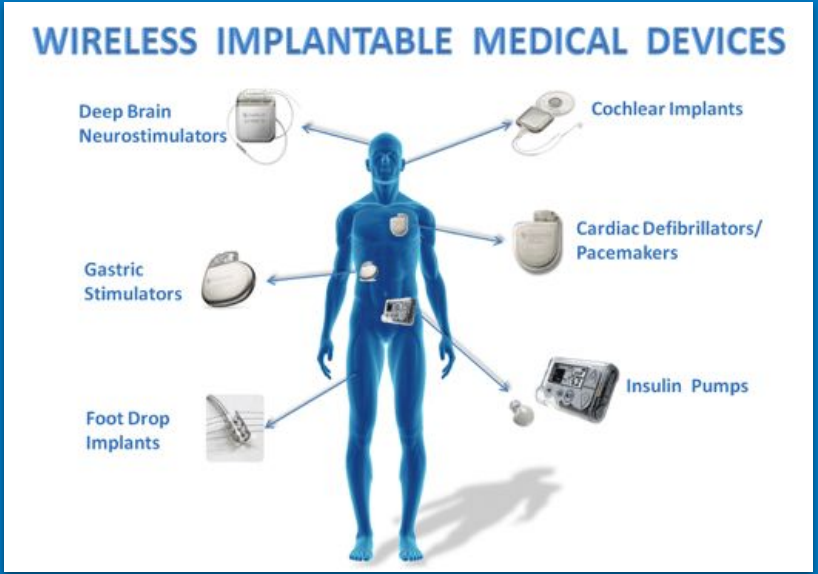
Cloud Data Infrastructure



Severity - 99/100 Likelihood - 45% Score - 44.55

- Anthem's current data infrastructure runs on the IBM Cloud
  - Plays a critical role in storing and transmitting data to patients and employees, administering services
- **Risks**
  - Unauthorized use, stolen credentials
  - Vendor lock-in, insider abuse
  - Accidental data loss, data leaks
- **Consequences**
  - Legal troubles, business downtime
  - HIPAA violation fines, loss of reputation
  - Revenue loss, loss of intellectual property
- **Mitigation**
  - Ensure sufficient storage capacity; log and monitor data
  - Implement data backups, encryption
- **Contingency**
  - Restore backups; check logs to assess the scope and nature of the incident
  - Consult with IBM for further action; continue monitoring the situation

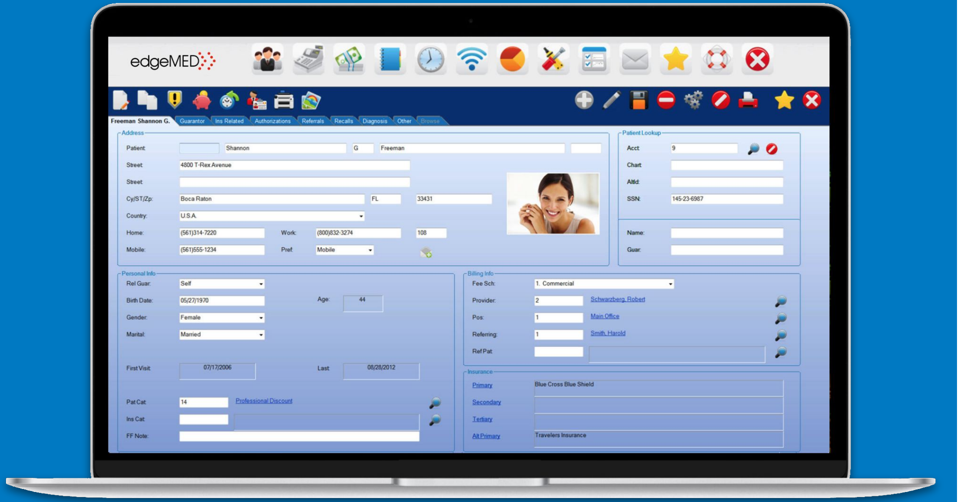
Medical IoT Devices


WIRELESS IMPLANTABLE MEDICAL DEVICES
Deep Brain Neurostimulators
Cochlear Implants
Cardiac Defibrillators/ Pacemakers
Gastric Stimulators
Insulin Pumps
Foot Drop Implants

Severity - 98/100 Likelihood - 42% Score - 41.16

- Devices used in health monitoring, remote treatment, physical and digital infrastructure
  - Includes wearables, surgical robotics, tracking devices, PCs, etc.
- **Risks**
  - Using default usernames and passwords to automatically establish a wireless connection
  - Lack of authentication when pumps are configured to allow FTP connections
  - *Dead facing* - device display is blank, but continues to administer a therapy
- **Consequences**
  - Cost of repair/replacement, costs to cover injuries
  - Loss of trust from patients, falling behind competition
  - Non-compliance issues, revenue loss
- **Mitigation**
  - IDS, strong password protection, encrypted WiFi
  - Maintenance, auditing devices and hospital network, inform users of vulnerabilities
- **Contingency**
  - Capture scope of attack, fix affected devices
  - Log events, review ACLs (modify if necessary)

Medical Software



Address

Patient: Shannon G Freeman
Street: 4800 T-Rex Avenue
Street:
Cy/ST/Zp: Boca Raton FL 33431
Country: U.S.A.
Home: (561)314-7220 Work: (800)832-3274 108
Mobile: (561)555-1234 Pref: Mobile

Patient Lookup

Acct: 9
Chart:
AltId:
SSN: 145-23-6987
Name:
Guar:

Personal Info

Rel Guar: Self
Birth Date: 05/27/1970 Age: 44
Gender: Female
Marital: Married
First Visit: 07/17/2006 Last: 08/28/2012
Pat Cat: 14 Professional Discount
Ins Cat:
FF Note:

Billing Info

Fee Sch: 1. Commercial
Provider: 2 Schwarzberg, Robert
Pos: 1 Main Office
Referring: 1 Smith, Harold
Ref Pat:

Insurance

Primary: Blue Cross Blue Shield
Secondary:
Tertiary:
Alt Primary: Travelers Insurance

Severity - 94/100 Likelihood - 40% Score - 37.6

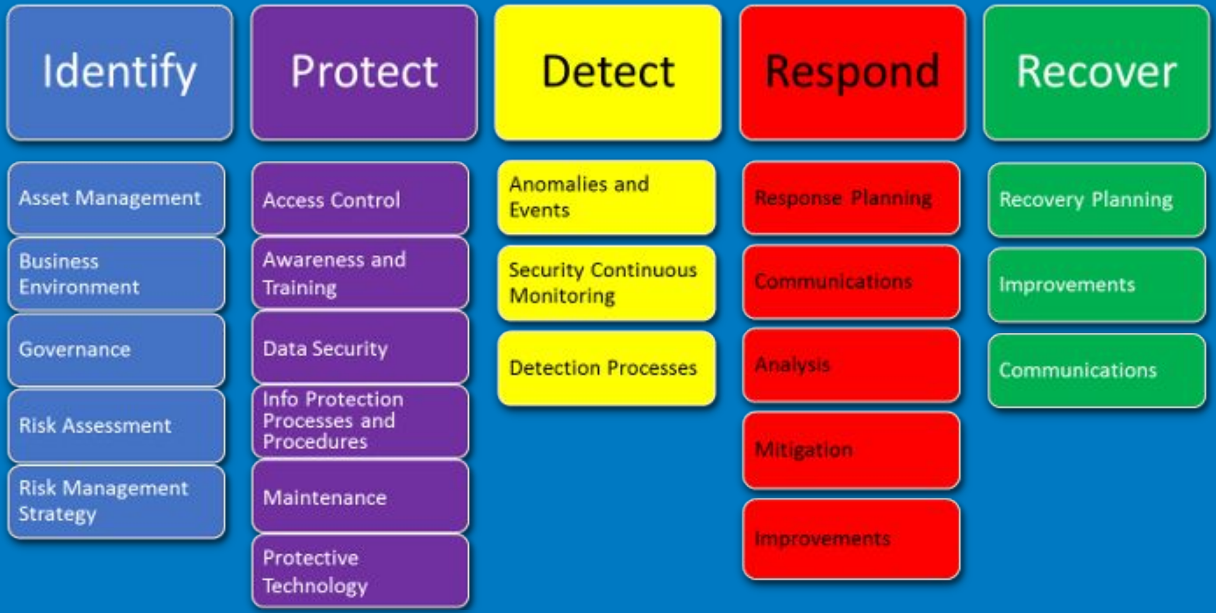
- Software that stores, processes, and transmits vital information
  - Used in databases, research, diagnosis, billing, imaging, telemedicine, processing EHRs, patient tracking, etc.
- **Risks**
  - Outdated software, vulnerabilities in code
  - Misconfiguration, software bugs
  - Flawed display of information, human error
- **Consequences**
  - Lack of accuracy in data, loss of patients
  - PHI, EHR leaks, HIPAA privacy violation fines
  - Identity theft, medical fraud = damaged reputation
- **Mitigation**
  - Patch and update software regularly
  - Perform vulnerability tests, security by design
- **Contingency**
  - Inform victims and law enforcement of event
  - Lock software, report incident to OEM

Medical Treatment Equipment

Severity - 97/100 Likelihood - 38% Score - 36.86

- Medical devices or tools designed to treat a specific condition
  - This equipment is critical in performing operations that address abnormalities and restore organs or tissues to working condition
- **Risks**
  - Parts failure
  - Unavailability of spare parts and/or replacements
  - Using obsolete models
- **Consequences**
  - Lower standard of equipment = inefficiency
  - HIPAA violation fines, loss of reputation
  - Clinical mistakes, increased need for hospital resources and unnecessary medical care delays
- **Mitigation**
  - Strategic planning in the acquisition of equipment, warranties, etc.
  - Securing spare parts, technical support, having well-trained maintenance personnel
- **Contingency**
  - Implement incident response strategies
  - Replacement of faulty parts, training refresh

NIST Cybersecurity Framework

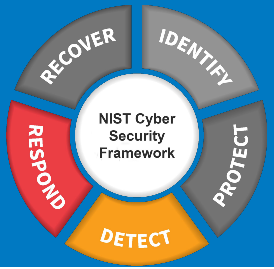


Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

NIST CSF Recommendations

- Asset: **Cloud Data Infrastructure**
    - Risks: unauthorized use, tampering, accidental data loss, inadequate capacity
- Recommended functions/categories/subcategories:
    - **Identify: Risk Assessment** (ID.RA-1,3)
        - **ID.RA-1** addresses the identification and documentation of cloud data infrastructure vulnerabilities
            - The risk assessment policy must address scope, roles, coordination, etc.
        - **ID.RA-3** ensures that internal and external threats are identified and documented
            - Integrate risk assessment results and risk management decisions
    - **Protect: Data Security** (PR.DS-4,5)
        - **PR.DS-4** calls for adequate capacity to ensure availability is maintained
            - Provide an uninterruptible power supply in case of emergency
        - **PR.DS-5** implements protections against data leaks
            - Principle of least privilege

NIST CSF Recommendations



- Asset: **Medical Software**
  - Risks: vulnerabilities in code, flawed display information, human error, insider threats
- Recommended functions/categories/subcategories:
  - **Detect: Security Continuous Monitoring** (DE.CM-4,8)
    - **DE.CM-4** employs measures to detect and eradicate malicious code and bugs
      - Block and/or quarantine malicious code, report on bugs
    - **DE.CM-8** establishes scanning for potential sources of vulnerabilities
      - Port scanning, host-based scanning, network-based scanning, etc.
  - **Respond: Communications** (RS.CO-1,5)
    - **RS.CO-1** states that personnel must know their roles and order of operations when a response is needed
      - Train employees, establish roles and responsibilities
    - **RS.CO-5** recommends voluntary information sharing with external stakeholders to achieve broader cybersecurity situational awareness
      - Cooperate with law enforcement

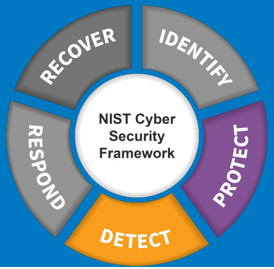
NIST CSF Recommendations

- Asset: **Websites**
  - Risks: Data exposure, unavailability, broken authentication
- Recommended functions/categories/subcategories:
  - **Respond: Mitigation** (RS.MI-1,2)
    - **RS.MI-1:** Incidents are contained
    - **RS.MI-2:** Incidents are mitigated
  - **Identify: Governance** (ID.GV-1,3)
    - **ID.GV-1:** Organizational cybersecurity policy is established and communicated
    - **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

NIST CSF Recommendations

- Asset: **Actuary Equations**
  - Risks: Compromised Equations, Loss of Data
- Recommended functions/categories/subcategories:
  - **Protect: Awareness and Training** (PR.AT-1,2)
    - **PR.AT-1:** All users are informed and trained
    - **PR.AT-2:** Privileged users understand their roles and responsibilities
  - **Recover: Recovery Planning** (RC.RP-1)
    - **RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident

NIST CSF Recommendations



- Asset: **Electronic Health Records**
  - Risks: Compromised patient information, including personal customer data
- Recommended functions/categories/subcategories:
  - **Protect: Identity Management, Authentication and Access Control** (PR.AC-1,3)
    - **PR.AC-1**: Authorized devices, users, and processes have identities and credentials that are issued for use
    - **PR.AC-3**: Controls remote access
  - **Detect: Anomalies and Events** (DE.AE-1) & **Security Continuous Monitoring** (DE.CM-1)
    - **DE.AE-1**: For users and systems, a baseline of network operations and expected data flows is built and managed
    - **DE.CM-1**: The network is being monitored for potential cyber-attacks

NIST CSF Recommendations

- Asset: **Payroll Systems**
  - Risks: Compromised financial information, hour padding
- Recommended functions/categories/subcategories:
  - **Identify: Risk Management Strategy** (ID.RM-1,2)
    - **ID.RM-1**: The organization needs to implement risk management practices that are monitored over time and agreed upon by all stakeholders
    - **ID.RM-2**: The risk tolerance of the approach must be identified and explicitly communicated
  - **Respond: Response Planning and Communications** (RS.RP-1, RS.CO-4)
    - **RS.RP-1**: During or after an incident, a response plan is implemented
    - **RS.CO-4**: Stakeholder coordination happens in accordance with response plans

Conclusion

- Anthem experienced a massive data breach in 2015, in which more than **37.5 million records** were stolen by hackers
    - This breach went **undetected for a month**, which is unacceptable for a company that processes **20 billion claims a year** and stores hundreds of thousands of **petabytes** worth of individual and population clinical data, claims data, EHRs, etc.
- With this cybersecurity assessment, we provide Anthem with best practices, policies, procedures and controls which will serve to improve all aspects of their cybersecurity infrastructure