Anthem, Inc.

Cybersecurity Assessment

April 17, 2022

Team Members - Neil Bridges, Marcos Luchetti, Michael Turkson

Table of Contents

Company Profile

Company Description

Anthem, Inc. is a leading company that provides healthcare services through its affiliated companies to over 118 million people in 14 states across the U.S.. As of 2021, over 45 million people are registered within Anthem's family of health plans. Their mission is to improve lives and communities, simplify healthcare, and exceed expectations. Their strategy to fulfill this mission focuses on three objectives: to create the best health care value in the industry, to excel at day-to-day execution, and to capitalize on new opportunities to drive growth. Anthem has been hailed as one of the best companies in the country, receiving awards for their corporate responsibility, inclusion & diversity, and workplace & wellness.

Company History

In 2004, WellPoint Health Networks Inc. and Anthem, Inc. merged to become WellPoint, Inc. Between 1992 and 2005, these two companies have acquired Blue plans from 14 states. Over that time and beyond, they have also acquired managed care companies, health plans including vision and dental, and data analytics-driven personal health care guidance companies throughout the country. In 2014, WellPoint, Inc. changed its corporate name to Anthem, Inc. Today, as an independent licensee of the Blue Cross and Blue Shield Association, they now serve members in California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia and Wisconsin; and specialty plan members in other states.

About the Industry

Healthcare is a continuously growing industry comprising various companies and healthcare institutions that serve millions of patients. These companies are expected to have a high standard of care and satisfaction for their customers. Health insurance, healthcare marketing, pharmaceuticals, healthcare tech, and health administration are the more notable sectors of the U.S. healthcare industry. Recently, the COVID-19 pandemic left a profound impact in the healthcare ecosystem. The transition from paper to digital has changed the way these companies do business. There is now a much broader use of technological resources by healthcare companies to process electronic health records (EHRs) and provide telehealth services such as video doctor visits and remote patient monitoring tools. Reports show that healthcare spending accounts for over 19.7% of the U.S. GDP (2020), and is likely to increase as time goes on.

Key Products

Anthem, Inc. is affiliated with many companies that deliver a variety of health benefit solutions, including health care plans and related services, life and disability insurance benefits, dental, vision, behavioral health benefit services, in addition to long term care insurance and flexible spending accounts for customers. Their Individual & Family insurance plans offer affordable coverage options in health, dental, and vision insurance. Every Anthem health insurance plan includes $0 preventive care visits, prescription coverage for many commonly used medications, and predictable out-of-pocket costs. With Anthem, customers can also receive 100% coverage for dental exams, cleanings, and X-rays, as long as the dental provider is in the plan's network. Anthem also lets customers purchase a comprehensive vision plan by itself or add it to any of their other health or dental insurance plans. Anthem vision insurance grants 100% coverage for checkups and eye exams, and allowances to buy glasses or contacts.

Stock Performance

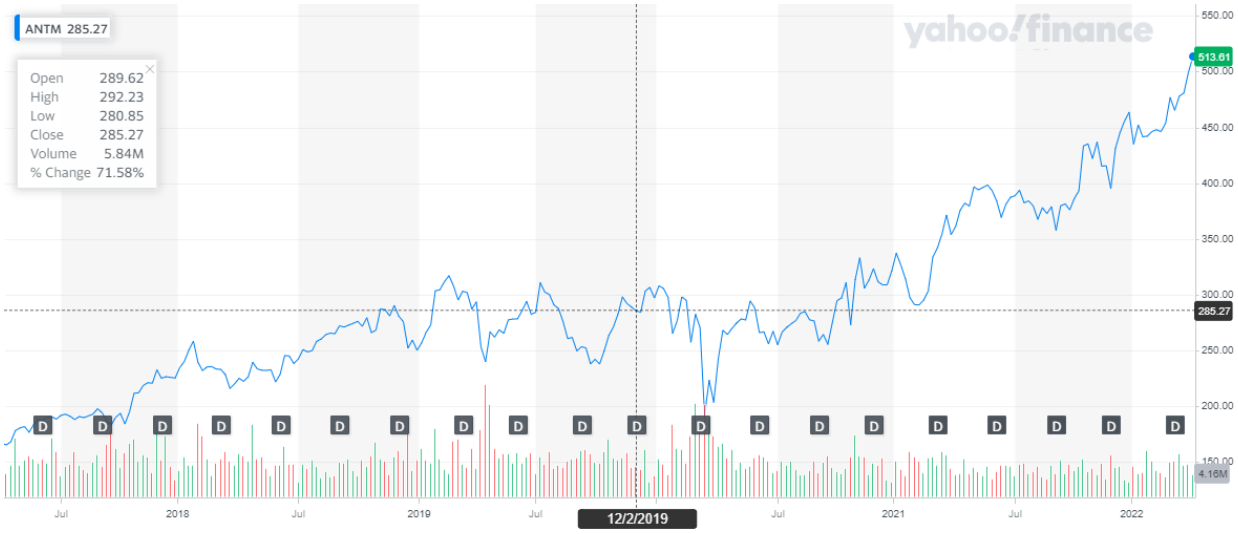

Figure 1. Anthem, Inc. (ANTM) 5-year stock performance chart (Yahoo! Finance)

Summary of Key Findings

Regarding Anthem, cybersecurity plays a vital role in protecting information that is constantly transmitted over the Internet and subjected to breaches. The following assets are included in Anthem's primary evaluation recommendations: actuary equations, websites, cloud data infrastructure, medical software, electronic health records, and payroll systems. All of the assets are linked to the appropriate functions that will help them. Data protection, identifying vulnerable spots, and recovery plans for each asset are all functions Anthem must implement. IDS installations, advanced passwords, two-factor authentication, and risk management assessments are all examples of best controls and practices. Separating networks, establishing technological controls, and monitoring controls are just a few of the measures Anthem will need to adopt to protect the security of these assets. The parts that follow go through the best practices, policies, procedures, and controls that Anthem should put in place to strengthen their cybersecurity.

Asset Ranking

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 Management Matrix

Key Assets

Asset	Description	Value	Explanation/Reasoning
Cloud Data Infrastructure	Anthem's current infrastructure, in partnership with IBM; provides AI for automating operations and analytics tools to improve services	1	The cloud infrastructure is the backbone of Anthem; it plays a critical role in storing and transmitting data to patients and employees, and administering services
Medical IoT Devices	Technologies that aid in health monitoring, remote treatment, physical & digital infrastructure; includes wearables, surgical robotics, tracking devices, PCs, etc.	2	IoT devices store and transmit sensitive data, putting privacy of PII & EHRs at risk; surgical robotics can be manipulated to be harmful
Medical Software	Electronic Health Record (EHR) software, medical software for database, research, diagnosis, billing, and imaging, telemedicine software, etc.	3	All this software collects, processes, and transmits vital information that needs to be protected from leaks or tampering; poor coding, use of outdated/poorly coded software may result in costly security breach
Medical Treatment Equipment	A medical device or tool designed to treat a specific condition; includes infusion pumps, medical lasers, LASIK surgical machines	4	This equipment uses modern technology which can be tampered with; it is vital for performing operations to address abnormalities and to restore organs or tissues to working order
Employees	Healthcare providers (HCPs), nurse practitioners, physician assistants (PAs), laboratory technicians, and other support staff	5	Employees have access to vital information; risks include fraud, waste, and abuse of sensitive data and/or IT systems
Websites & Apps	(www.anthem.com & Sydney Health app) - Used by patients to access information about their Anthem health plans, etc.	6	Must be accessible 99.99% of the time; processes sensitive information that must be kept confidential
Electronic Health Records	A system dedicated to collecting, storing, manipulating, and making available clinical information important to the delivery of patient care.	7	Having a patient's history, clinical findings, diagnostic test results, medication, and many other things keeps the facility reliable

Payroll Systems	These systems monitor the critical function of paying employees by processing attendance and calculating wage rates.	8	Employees will not be satisfied without proper compensation
Life Support Equipment	Devices that maintain a patient's bodily functions; includes heart-lung machines, medical ventilators, dialysis machines, incubators	9	Without life support machines, it would be difficult to support the organ systems' ability to function; life support is an essential asset for any healthcare provider and must be protected from damage and/or tampering
Medical Laboratory Equipment	Equipment used for analyzing blood, urine, genes, and other biological material; includes blood collection supplies, chemistry analyzers, drug testing analyzers, microbiological systems, etc.	10	This equipment is important for the medical clinics or diagnostic laboratories that are owned by Anthem; these tests are necessary for diagnosing illnesses and prescribing drugs to patients
Durable Medical Equipment	Equipment used for providing therapeutic benefits; includes wheelchairs, hospital beds, walkers, oxygen tanks, insulin pumps, breast pumps, kidney machines, nebulizers, etc.	11	This equipment is a necessity for providing care for certain conditions or illnesses; patients need to feel safe and comfortable; this equipment is "durable," therefore they can be trusted to work long-term and do not require much maintenance
Actuary Equations	Actuary calculations based on a large amount of data, statistics, and other math to calculate the right price to customers	12	Charging the right price is extremely important to make sure that they do not charge too little and go bankrupt or charge too much and drive their customers to more reasonably priced competitors

Qualitative Method

#	Related Asset	Risk Description	Business Consequences	Severity	Likelihood	Score	Mitigation	Contingency
1	Cloud Data Infrastructure	Unauthorized use, stolen credentials, vendor lock-in, insider abuse, accidental data loss, unavailability	Stolen data, reputational loss, cost to investigate, unavailability	99	45%	44.55	Sufficient storage, establish a baseline, proper logging and monitoring, encryption, data backup, implement disaster recovery strategy	Restore backups; check logs to assess the scope and nature of the incident; consult with IBM for further action; continue monitoring
2	Medical IoT Devices	Medical equipment manipulated to harm patients, work less efficiently, etc.; lack of authentication, dead facing	Cost of repair/replacement, loss of trust, non-compliance troubles, legal troubles, injury costs	98	42%	41.16	IDS, strong password/authentication policy, encryption, security by design, data policies, auditing	Monitor equipment, capture scope of attack; temporarily revoke access to affected devices, review physical hardware policies and make changes were needed, log events, review ACLs
3	Medical Software	Outdated software, poor coding & configurations, insider threats	Stolen records, manipulated systems, HIPAA violation fines, loss of reputation	94	40%	37.6	Updates, implement security by design, employee training, IDS, data policies, auditing	Contact victims, notify them of stolen data, notify organizations such as credit card companies, banks, etc., notify law enforcement; freeze accounts, lock systems; record data related to incident & continue monitoring; update policies, firewall configurations, etc.

4	Medical Treatment Equipment	Parts failure, unavailability of spare parts and/or replacements, old model becoming obsolete, inefficiency	Falling behind the competition, lower standards, lack of accuracy, cost of retraining personnel	97	38%	36.86	Strategic planning in the acquisition of equipment, guarantees, etc.; securing spare parts, technical support; having well-trained maintenance personnel	Implement incident response strategies, replacement of faulty parts, training refresh
5	Employees	Poor cybersecurity training/culture, malicious insiders	Data leaks, stolen/manipulated data, invasion of privacy	70	48.00%	33.6	Training, nonrepudiation, NDAs, logging	Terminate malicious employees, assess logs to determine scope of attack
6	Websites & Apps	Broken authentication, data exposure, using vulnerable components, unavailability	Compromised medical info, non-compliance costs, stolen data, loss of trust, reputation	80	40.00%	32	Security by design, encryption, password protection, 2FA, IDS, data policies, auditing	Assess the scope and nature of the incident; review firewall configurations, policies, ACLs and make changes were needed; lock affected systems & fix security before using them again; monitor the event; notify accounts on anthem.com and Sydney Health App of event
7	Electronic Health Records	Compromised patient information, including personal data	HIPAA Violation could involve many lawsuits, along with stolen hospital records	98	28.00%	27.44	Have an incident response plan, employee training, limit EHR access to employees, create subnetworks	Contain the breach, preserve any evidence that can be saved, notify everyone that has been affected. Notify all involving organizations

8	Payroll Systems	Compromised financial information, hour padding	Stolen financial data, loss of revenue	99	25.00%	24.75	Audits and changing logs, encryption	Employees should be informed. Determine whether employee information has been hacked. Nonexempt workers should be required to utilize paper timecards. Recreate the current pay period's missing timecards and attendance records. Determine how to distribute paychecks before the next pay day
9	Life Support Equipment	Availability concerns (availability of batteries, PC on hospital network, public address systems), radio interference, electrical failure	Loss of reputation, legal troubles, loss of trust, cost of repair/replacement	100	20.00%	20	Routine maintenance of equipment, audits, physical security	Ensure safety of patient; record details of the event (when, why, how it happened); attempt to repair, then continue monitoring; if irreparable, replace immediately
10	Medical Laboratory Equipment	Hazards, spills, inefficient/broken tools	Lack of accuracy in data, loss of patients, unreliable data	80	15.00%	12	Maintenance, cleaning, repair, upkeep of equipment, train personnel regularly	Have spare parts always on hand for emergency use
11	Durable Medical Equipment	Needing repair, replacement, upgrades	Falling behind competition because of using older models, loss of patients	50	22.00%	11	Maintenance, cleaning, repair, upkeep of equipment, train personnel regularly	Have spare parts always on hand for emergency use; ensure quick access to suppliers for replacements; always have replacements in stock

12	Actuary Equations	Equations being leaked to competitors, Using the equations for determining customer's rates	Customers and competitors are aware of how rates are determined	90	5.00%	4.5	A self-contained system, encryption, 2 factor authentication, employee training	Try to contain the leak of information as much as possible, contain the incident and make sure the system is secure

Quantitative Method

Asset	Asset Value (AV)	Exposure Factor (EF)	Single Loss Expectancy (SLE)	Annual Rate of Occurrence (ARO)	Annualized Loss Expectancy (ALE)	TCO of Mitigation	ALE w/out Mitigation	ROI
Cloud Data Infrastructure	$1,200,000	100.00%	$4,240,000	1	$4,240,000	$134,000	$4,240,000	$4,106,000
Medical IoT Devices	$6,000,000	100.00%	$3,000,000	1	$3,000,000	$25,000	$3,000,000	$2,975,000
Medical Software	$230,000	100.00%	$4,240,000	1	$4,240,000	$10,000	$4,240,000	$4,230,000
Medical Treatment Equipment	$25,000,000	100.00%	$2,000,000	1	$2,000,000	$45,000	$2,000,000	$1,955,000
Employees	$8,000,000	100.00%	$8,000,000	1	$8,000,000	$9,000	$8,000,000	$7,991,000
Websites and Apps	$2,000,000	20.00%	$400,000	2	$800,000	$200,000	$800,000	$600,000
Electronic Health Records	$10,000,000	100.00%	$10,000,000	1	$10,000,000	$25,000	$10,000,000	$9,975,000
Payroll Systems	$8,000,000	100.00%	$8,000,000	1	$8,000,000	$60,000	$8,000,000	$7,940,000
Life Support Equipment	$1,460,000	100.00%	$1,460,000	1	$1,460,000	$87,600	$1,460,000	$1,372,400
Medical Laboratory Equipment	$1,000,000	80.00%	$800,000	1	$800,000	$30,000	$800,000	$770,000
Durable Medical Equipment	$3,500,000	100.00%	$3,500,000	1	$3,500,000	$12,000	$3,500,000	$3,488,000
Actuary Equations	$5,000,000	100.00%	$5,000,000	0	$250,000	$50,000	$250,000	$200,000

Cybersecurity Metrics

Super-user access (Marcos Luchetti)

With super-user privileges, a malicious insider could use these controls to manipulate Anthem's corporate infrastructure, causing significant damage to its assets and reputation. That is why it is important to identify the percentage of employees with super-user access and monitor their activities. Having clearly defined roles and responsibilities will help solve this issue, and we also recommend limiting the number of users with super-user access to a limited number of individuals. This metric will help Anthem in determining the appropriate personnel that should have access to super-user privileges. In addition, this metric will also improve security in that it can help detect when a super-user account has been compromised by an external attacker.

Amount of days to deactivate unused/former employee access (Marcos Luchetti)

To protect Anthem's data, we advise deactivating employee access of company systems immediately after their departure. If an employee is discovered to be a malicious insider, the same rule still applies. This metric will help ensure if the IT and HR departments are working in tandem with one another. Keeping unused/former employee credentials active may result in a costly security breach, compromised devices, and a complicated situation for forensic investigators.

Cybersecurity awareness training (Marcos Luchetti)

All employees—senior executives, healthcare providers, nurse practitioners, physician assistants, lab techs, and other support staff—must have completed cybersecurity awareness training. Security training procedures have to be well documented and monitored for completion. We also advise monitoring awareness training assessments to determine which groups/individuals need additional training. In addition, phishing campaigns would help to determine the effectiveness of Anthem's cybersecurity training. These metrics will help the company in gauging its cybersecurity posture with the goal of meeting compliance standards and improving its information assurance over time.

Endpoint detection coverage (Michael Turkson)

Unmonitored devices can potentially become a malware and infiltration honeypot if it is left unattended. Anthem can effectively monitor all devices, even those in the cloud, using endpoint security, while also enforcing access perimeters to keep unwanted devices off the network. Because mobile and cloud usage is at an all-time high, hospitals and healthcare

institutions must become increasingly alert and focused on data security. Both the losing provider and the gaining cyber-criminal on the Dark Web black market pay a significant price for unlawfully obtained healthcare data.

Vulnerability outlier analysis (Michael Turkson)

Outlier identification is important because outliers in data might forecast important information in a range of medical and other application sectors. In Anthem, outlier status may be determined using two methods: computing a facility outlier value within a given year, comparator group, and A1C threshold while considering at-risk population populations, and assessing standardized model residuals throughout a given year and A1C threshold.

Cost per incident (Neil Bridges)

While incidents should be avoided whenever possible, some incidents will fall through the cracks. It is important to keep track of the costs these incidents can have in terms of lost data, offline services, loss of brand trust, and many other metrics. This can help justify the costs behind cybersecurity measures as well as making efforts to minimize the losses associated with incidents.

Uptime (Neil Bridges)

Due to the importance of online services for the revenue of the company, uptime should be a metric that is monitored to ensure that services are constantly available. It can cause a great amount of customer frustration to not have their services available to them. Measuring the uptime of the services can either make their own inhouse services know how they are doing or let the company talk to outside vendors for their performance.

Frequency of reviewing third party access (Neil Bridges)

Anthem will often have to work with third party vendors and grant them access to their network. It should be checked often to make sure that these third parties only have access as long as they need it and it does not give them more access than is intended due to the sensitivity of the data that is handled by Anthem.

Assessment Recommendations

Actuary Equations (Neil Bridges)

For any insurance company knowing how much to charge customers for their service. This is where the actuary calculations based on a large amount of data, statistics, and other math come in to calculate the right price to their customers. Charging the right price is extremely important to make sure that they do not charge too little and go bankrupt or charge too much and drive their customers to more reasonably priced competitors. Every insurance company would want to make sure that competitors can not know the math behind the prices they charge to their customers.

It is important to make sure that no one outside the company or even inside the company has access to these calculations since competitors could undercut them very easily if they knew how they were determining prices. Also, they need to make sure that these equations can be recovered in the case that a rogue employee deletes them or the hard drive where they are stored becomes corrupted.

Protect: Awareness and Training (PR.AT-1,2)

While it is very important that procedures and policies are in place, they are useless if the users are not aware of them. After the procedures and policies have been decided on, the users need to undergo training so they can properly understand them and what they mean. This is especially important for actuary equations since users need to make sure not to accidentally compromise the equations. Even if very effective procedures are set up it can be very easy for a user to accidentally compromise the network.

Protect: Information Protection Processes and Procedures (PR.IP-4,10)

The actuary equations are very important to the company and to make sure the data is protected backups should be conducted, maintained, and tested. Oftentimes backups are set up but they are never tested. They might as well not even have backups since when a problem occurs they have no idea if the backups will work or not. Similarly, if a problem does occur with the Actuary equations they need to be respond to make sure that not everything will be lost. There could be measures in place to make sure people outside the company don't get all the data. Also, the equations need to be able to be turned back on.

Recover: Recovery Planning (RC.RP-1)

Since Actuary equations are such an integral part of Anthem, they are constantly being updated as accountants work to upgrade them and more data comes in. Because of this it

is very important that after a cybersecurity incident a plan should be in place. The equations should be able to be recovered quickly. This will require a well thought out plan to limit the downtime as much as possible.

Recover: Improvements (RC.IM-1,2)

After the cybersecurity team has gone through these problems a couple times they should be able to improve from this knowledge. They can use what they learned from the last time these incidents occured to make sure that they can bring everything back online even faster. The recovery plans in place should be a living document that is constantly updated with the knowledge that they gain through each experience.

Control: Self-Contained Network

For very important data some companies turn to self-contained networks. They are separate from the normal network that all other devices are running on for the company. This allows important data to be protected even if the primary network is compromised and data from that network is lost. This should be used for the Actuary equations system since these equations are integral to the company and this information being leaked to competitors could be disastrous. While this can be costly to set up a whole new network it is a central part of any insurance company and the cost is justifiable.

Policy: Each device for Actuary purposes is on a separate network

Every workstation used for actuary purposes is on its own separate network with all outgoing and incoming traffic is highly regulated to make sure no data is being leaked out. These will only be company provided workstations and employees will not be able to use their own computers or phones while working on Actuary equations. This allows the IT department to control what is installed on these devices as well as making it easier to install the network on each device since they will all be similar as well as ensuring that employees can not take these devices home and showing confidential info to others. Also, this network will only be accessible on site and employees will not be able to access it from home networks or VPNs. When working from home there are too many risks associated such as leaking of confidential information intentionally or unintentionally and the easiest way to make sure this does not happen is to have all employees work in person.

Procedure

The information technology team will be responsible for ensuring that each device is secure on the Actuary systems network separate from the company's normal network. Also, they are responsible for distributing these devices, setting them up on the network, monitoring outgoing and incoming traffic for this network. They will also ensure that employees are using the company provided devices instead of their own devices. They will provide a quarterly report about the workstations in this department as well as the security

of these devices to the executive team. Also, they will conduct their own test to ensure the strength of their security quarterly and submit a report to the executive team and conduct a penetration test by a third-party organization semi-annually fixing any issues found and submitting a report to the executive team .

Review Frequency

This procedure will be reviewed between the executive team and information technology department to ensure that all security concerns are being adequately addressed. If either party is unhappy with costs or how security is being handled a plan will be made to remedy the situation and plan a better system.

Websites (Neil Bridges)

Anthem is a very large organization with many customers that need to communicate with them everyday. Having an online presence like their website makes it so their customers can easily communicate with the organization for whatever they need. It is very important that the website is constantly up. If the website is down it may cause customer frustration and anger at the Anthem Brand as well as potentially costing future customers. Also, since customers can access the medical records through the website and set up appointments it may cause backups at medical offices.

Respond: Mitigation (RS.MI-1,2)

Since it is so important that the Website has a constant uptime if any incidents occur the cybersecurity team has to be ready to deal with it. They need ways of making sure even if they attack it will either not affect the uptime or limit the downtime as much as possible. There are many different steps that can be made to make sure they can quickly respond and limit the effect as much as possible. The effects can either be contained where they make sure the attack won't get out of hand or it can be mitigated so the effect is limited.

Respond: Analysis (RS.AN-1,5)

Analysis is also a very important process for the website since they need to make sure their processes are effective. This helps them analyze if their efforts in the past helped limit the downtime when attacks occur as well as limiting other possible negative effects. This can also help when people report possible security problems. The cybersecurity team can use internal testing or security researchers to make sure there are few security problems for the system.

Identify: Governance (ID.GV-1,3)

Since the website can send customer's their own medical information, governance is an extremely important part of the functions. They need to make sure that they follow all governmental guidelines to make sure that they can not be fined. This can include

encrypting the data they send out to their customers as well as a higher level of verification to make sure the right people are getting the data. Also, they must follow the normal guidelines for any website to make sure that all their data is protected.

Identify: Business Environment (ID.BE-4,5)

The website is a very integral part of the company since it will usually be the main way that customers interact with the company. It is very important that proper functions are created to make sure that the website can do everything it needs to for the company. This can include setting appointments, paying bills, sending medical information, along with many other functions. They also need to make sure that all these functions are operational even during times of duress.

Control: Contingency Plan

For any company there needs to be a plan in case of problems arising. If websites are taken down either intentionally or unintentionally there should be a well established plan to make sure that the problem can be solved quickly. A backup plan should be set up far in advance to make sure everyone knows how to bring the network back online, have backups in case of lost data, make sure that backups are operational, and to continue to have functions operational even when an attack or problem is ongoing.

Policy: Continue mission and business functions

Anthem's website is central to their company and provides a wide variety of functions. It can allow many people to sign up for their insurance, pay their bills, access their medical information, make sure their doctors are in network, and have many other questions answered for them. Even in the case of issues there will be measures taken to make sure that business functions are operational. If networks go down it can cause a large loss of revenue both in the form of loss of transactions as well as loss of consumer goodwill which could drive them to competitors.

Procedure

The information technology will make multiple independent servers to make sure that an attack on one server will not cause a loss of critical functions. Even when issues arise or an attack is on one server the other servers should remain operational allowing the website to remain online. However, the information technology team will still remain ready to solve problems quickly to ensure that all servers can remain operational as much as possible. Stress tests should be conducted by both the information technology department and third-party organizations to make sure that the website can remain operational through problems and their findings to the executive team.

Review Frequency

The plans in place will be reviewed once every year by both the executive team and the information technology team to ensure that maximum uptime is achieved for the website. The information technology team will compile a report on their plans and their efficacies once a year during the review. The cost of running the websites and their plans must also be evaluated against the cost of outsourcing this work.

Cloud Data Infrastructure (Marcos Luchetti)

Using IBM cloud technologies, Anthem's data infrastructure helps the company reach its market demands, launch new products for plan members, and deliver on the mission to transform healthcare with trusted and caring solutions. Anthem processes 20 billion claims a year, storing hundreds of thousands of petabytes worth of individual and population clinical data, claims data, electronic health records (EHRs), and more. They also work with thousands of physicians, hospital partners, employers, and government agencies, who also rely on this data infrastructure to provide a greater standard of healthcare services to their patients. It was in 2015 when Anthem invested $500 million on a cloud data infrastructure. Since then, cloud technology has become more broadly implemented because of its efficiency, flexibility, and scalability. It has become a popular way for companies to backup their data and monitor customer behavior.

Despite its advantages, the cloud presents several risks and challenges related to control, security, and availability. Cloud service providers have total control over a given company's data on their servers, which can be problematic for a number of reasons. Once data is sent to the cloud, it can be difficult for a company to have it managed the way they want it to, and getting the data back can be expensive and cumbersome. Cloud servers are also prone to cyber attacks resulting from misconfiguration, unauthorized access, insecure interfaces/APIs, account hijacking, etc. All of this threatens the confidentiality of data, potentially resulting in data loss/leakage, accidental exposure of credentials, and compliance issues with data protection regulations such as PCI DSS and HIPAA. Another risk of cloud computing is unavailability, which can occur from DoS attacks, power outages, faulty systems, etc. Since cloud computing relies completely on the Internet, users will not be able to access any information when the servers become unavailable, which can be costly for a company.

The following Identify and Protect function categories and subcategories of the NIST Cybersecurity Framework are appropriate for this asset's risk:

Identify: Risk Assessment (ID.RA-1,3)

- **ID.RA-1** addresses the identification and documentation of asset vulnerabilities
- **ID.RA-3** ensures that internal and external threats are identified and documented

Identification and documentation of the cloud data infrastructure's vulnerabilities and internal/external threats is one of the most important first steps to take in protecting critical information from cyber attacks. Having documentation of identified threats and vulnerabilities will be useful in better understanding the cybersecurity risk to Anthem's operations and how it can impact their mission, functions, image, and/or reputation, as well as the impact on other assets and individuals. Identifying these risks early on will better prepare the company for problems later on.

Identify: Risk Management Strategy (ID.RM-1,2)

- **ID.RM-1** addresses the company's need for establishing risk management processes that are monitored over time and agreed to by company stakeholders
- **ID.RM-2** specifies that the strategy's risk tolerance must be determined and clearly expressed

Anthem needs to have a risk management strategy which outlines their priorities, constraints, risk tolerances, and assumptions to be considered in supporting operational risk decisions related to their data infrastructure. The risk management processes in the strategy are to be established, managed, and agreed to by the company's stakeholders. In addition, Anthem's risk tolerance needs to be defined and clearly communicated. All of these measures are important in that Anthem will show customers and stakeholders that they have developed a risk management strategy that is constantly regulated and clearly communicated to everyone. Having a strategy that addresses the risks associated with operating a massive cloud data infrastructure which contains billions of claims and hundreds of thousands of EHRs will help guide Anthem in properly securing critical assets, including their reputation.

Protect: Data Security (PR.DS-4,5)

- **PR.DS-4** prompts adequate capacity to ensure availability is maintained
- **PR.DS-5** ensures that protections against data leaks are implemented

Protecting Anthem's cloud infrastructure involves many activities, including but not limited to addressing storage capacity needs and preventing data leaks. For a company such as Anthem that deals with hundreds of thousands of petabytes worth of sensitive data, having a sufficient amount of storage is highly important. Not having enough storage space for all of the data that they process can result in unavailability of services, prompting concerning business consequences. Moreover, protecting against data leaks is just as important, if not more, and a massive data leak can spell more serious, potentially irreparable damage to Anthem's business and reputation.

Protect: Protective Technology (PR.PT-3,4)

- **PR.PT-3** incorporates the principle of least functionality by configuring systems to provide only essential capabilities
- **PR.PT-4** corresponds to the protection of communications and control networks

Anthem's data infrastructure systems must only provide functions related to its essential functions. That is, these systems should only be used for storing, organizing, and transmitting data, building indexes, backing up important data, and restoration activities. Moreover, the protection of communications and control networks is vital to Anthem as they may be susceptible to cyber attacks, such as a man-in-the-middle attack where data that is transmitted over a conversation between a server and a client is intercepted by a malicious third party.

Control: Risk Management & Assessment

It would be ideal for any company to implement a continuous cybersecurity risk management strategy to maintain protections against the changing threat landscape. The PM-9 control from the NIST SP 800-53 will help Anthem in developing a comprehensive strategy to manage security risk to their operations and assets, individuals, other companies, and on national security, as well as the use of Anthem's systems. This also helps in managing privacy risk to individuals resulting from the authorized processing of PII. This is a strategic approach to prioritizing threats, ensuring that the most critical threats and vulnerabilities are handled properly. A cybersecurity risk management strategy is made up of six steps, as recommended by the NIST Framework: Prepare, Identify, Protect, Detect, Respond, and Recover. These help companies in achieving more effective, efficient, and cost-effective security and privacy risk management processes. The RA-3 control from the NIST SP 800-53 would also help shape Anthem's risk management activities by focusing on risk assessment. Risk assessment is the process of analyzing the identified information security risks, estimating their potential impact on the company, and then prioritizing each risk based on its severity or other factors.

Policy: IT infrastructure evaluation

The risk assessment will evaluate Anthem's IT infrastructure and security-related policies and procedures. This operation includes assessments of the company's network, security, and vulnerabilities. Components to be assessed include internal systems, attack surfaces, human error, and more. With that said, the Corporate Security department must conduct a risk assessment to assign value to Anthem's assets, as well as to evaluate their compliance with industry regulations. Once analyzed, these risks can be prioritized based on urgency or business impact. This assessment will help them to better understand their own cybersecurity posture and where they can improve.

Procedure

Anthem's Board of Directors should remain responsible for overseeing the risk management processes that are implemented by the executives, ensuring that the strategy is implemented consistently across the company. The board is also responsible for approving certain risk-tolerance levels and action plans regarding major risks. The Audit Committee must continue to assist the Board of Directors in assessing, monitoring, and managing exposure to said risks. Lastly, the board delegates to its committees responsibility for assisting in the oversight of categories of risk within their areas of responsibility. Anthem's Corporate Security department, who is responsible for Security Operations, Security Technology, and Risk & Intelligence should follow the procedures outlined by the above controls.

The procedures for conducting a risk assessment include identifying threats to and vulnerabilities in the system and determining the likelihood and magnitude of harm from unauthorized access and uses, or destruction of the system and the information it processes, stores, or transmits. The Corporate Security department should also assess the risk and impact of adverse effects on individuals arising from the processing of personally identifiable information (PII).

Review Frequency

The Board of Directors must consistently review and update the risk management strategy at least annually to address changes within the company. Risk assessments are to be documented and the results reviewed by the Board of Directors at least annually, and the risk assessment itself should be updated yearly or when there are significant changes to the system.

Control: Data Protection

The CIS Critical Security Control 13 provides guidelines on the processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information. It addresses concerns related to storage capacity, tampering, and information disclosure. This involves implementing three sets of controls: managerial, procedural, and technical, to prevent data from leaving the environment in an unstructured or unauthorized way.

Policy: Establish managerial, procedural, and technical controls

The Corporate Security department must establish managerial, procedural, and technical controls to ensure that data is protected. As a managerial control, a data inventory must be implemented to better understand the environment and interconnection between systems and subsystems. These can also be used to help define data retention requirements and policies. Procedural controls will also be implemented, which involves activities such as scanning for sensitive information to ensure its integrity, as well as developing processes, procedures, and configurations which ensure that data is where it needs to be. These are

to be used to provide structure and consistency within Anthem, thereby protecting data. Several technical controls will be used to further protect data, which include whole-disk encryption, blocking popular file transfer and email sites, Data Loss Prevention (DLP) tools and Privileged Account Management (PAM). All workstations must be configured with appropriate file and folder permissions and access control lists (ACLs) to restrict data access to authorized users.

Procedure

The Corporate Security department is responsible for the implementation of managerial, procedural, and technical controls. These plans must be approved by the Board of Directors before being implemented. Events are to be logged and analyzed by the Corporate Security department, and then reported to the Board of Directors to determine the effectiveness of the controls.

Review Frequency

This policy will be reviewed semi-annually by the Corporate Security department. This report will be shared with the Board of Directors for further review, and to address possible modifications. The report must be submitted by the end of Q2 and Q4.

Control: Principle of Least Functionality

The principle of least functionality mitigates the risk of data leakage/unauthorized access by limiting the storage/transmission of information on certain systems, services, and/or applications. Essentially, if a system/service/application has the ability to perform a task which is unnecessary for business functions, but has the potential to compromise sensitive data, then disabling this function would greatly mitigate that risk.

Policy: Limiting access and functionality of IT assets

Component functionality will be limited to a single function per device, such as a database server or a web server, where feasible. Access to Anthem's information systems is to be granted and managed by the user role and business function. Any unnecessary and/or vulnerable functions, ports, protocols, services, and applications will be disabled, uninstalled, or modified to meet security standards.

Procedure

The Corporate Security department is responsible for removing, uninstalling, and/or modifying/disabling IT assets, controls, services, and configurations. Any events and/or complications that arise will be documented. Controls are to be assessed semi-annually to determine effectiveness and make changes where necessary.

Review Frequency

An annual review of the controls, their effectiveness, and employee feedback will be compiled by the Corporate Security department and reported to the Board of Directors. This report must be submitted by the end of the year.

Medical Software (Marcos Luchetti)

Anthem uses a variety of medical software to perform a multitude of healthcare related activities. For instance, electronic health record (EHR) software processes a considerable amount of data, including patient information, history, scheduling, e-prescribing, and financial information. Patients' demographics, medical history, laboratory results, and allergies are usually stored in EHRs and shared across physicians. Hospital management software (HMS) processes an even higher amount of data, including all patient data, doctor and medical staff information, and hospital billing. These HMS systems are used to manage all sections of a hospital, including reception, laboratories, etc. It registers patients' information, issues online drug prescriptions and billing of drugs, consumables, etc., as well as managing labs and billing information. Lastly, healthcare customer relationship management (CRM) software is used to manage crucial patient data, such as test results, treatment history, and diagnoses. CRM software is also used to track patient visits, create and manage marketing campaigns, provide customer support, etc.

Software-related risks may result from using outdated, poorly coded, or misconfigured software which hinder the system's security. It is important that Anthem attends to these risks so as to avoid any business consequences that result from data loss/theft, unauthorized access to and modification of data, including files and configurations, as well as weak passwords and encryption. Failure to prevent sensitive data exposure will result in costly fines, upwards of millions of dollars, and a damaged reputation that would be difficult to recoup. In addition, failure to comply with data protection guidelines such as HIPAA would result in legal troubles that can cripple Anthem's healthcare business for years.

The following Detect and Respond function categories and subcategories of the NIST Cybersecurity Framework are appropriate for this asset's risk:

Detect: Anomalies and Events (DE.AE-1,4)

- **DE.AE-1** prescribes having a baseline of network operations and expected data flows for users and systems
- **DE.AE-4** states that incident alert thresholds must be established

The Detect function of the NIST CSF presents several useful processes and procedures that can help minimize the risks associated with operating medical software. For example, establishing a baseline of network operations and expected data flows for users and systems would be helpful in determining what is normal traffic/activity and detecting

abnormal traffic/activity, which has a chance of being harmful to software assets. Once detected, this activity can be informed to experts to be analyzed further, and then stopped, thereby preventing a security breach. It is also important that Anthem establishes incident alert thresholds, which can be useful in filtering out specific activities and variables, assigning incident severity, notifications, overrides, etc.

Detect: Security Continuous Monitoring (DE.CM-4,8)

- **DE.CM-4** communicates the importance of detecting malicious code
- **DE.CM-8** suggests performing vulnerability scans

Other helpful activities found in the Detect function include detecting malicious code in software and performing vulnerability scans. Detecting malicious code before it severely impacts business processes can go a long way in improving Anthem's cybersecurity posture. This can be accomplished by configuring firewall rules, using updated antivirus software, closing unnecessary ports, and running antispyware. These activities will help to reduce the likelihood of malicious code being executed. Furthermore, performing vulnerability scans will help in maintaining strong security on networks and information systems. This also satisfies one of HIPAA's compliance requirements, which enforces vulnerability scanning to protect sensitive data. A vulnerability scan can reveal known vulnerabilities in software, and can be used to determine which software is safe to use, and which is susceptible to attack. Taking all this into account, information security experts at Anthem can act on this information by wiping computers of vulnerable software, essentially mitigating the risk of a security breach.

Respond: Communications (RS.CO-1,5)

- **RS.CO-1** expresses that personnel know their roles and order of operations when a response is needed
- **RS.CO-5** recommends voluntary information sharing with external stakeholders to achieve broader cybersecurity situational awareness

In the event of a security breach, Anthem personnel must be aware of their roles and responsibilities so that they can respond appropriately. This involves maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. Response activities are to be coordinated with internal and external stakeholders to gain additional support whenever a response is needed. For instance, coordinating response activities with law enforcement agencies would be highly useful in responding effectively to a security breach.

Respond: Improvements (RS.IM-1,2)

- **RS.IM-1** explains how response plans must incorporate lessons learned after an event
- **RS.IM-2** states that response strategies are to be updated periodically

This function and its related categories and subcategories will help Anthem in improving their incident response activities and incorporating lessons learned from previous and ongoing detection/response activities. Incident response strategies should be updated periodically to address any changes/vulnerabilities in the company's software. Learning from past mistakes and constantly making improvements over the course of time will only boost Anthem's resilience to cyber threats, contributing to a more secure software environment that is more conducive for business.

Control: System Monitoring

System monitoring activities are conducted to detect attacks and indicators of potential attacks, as well as unauthorized connections. Companies monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. System monitoring involves the use of various tools and techniques, such as intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software. The SI-4 control from the NIST 800-53 framework provides guidelines on system monitoring, encouraging companies and organizations to collect information deemed essential, and to track specific types of transactions of interest to the company/organization. This control is also useful in identifying unauthorized use of systems, also invoking internal monitoring capabilities or the deployment of monitoring devices. The procedures outlined in this control will help in detecting abnormal network activity, and in the establishment of incident alert thresholds for a more efficient incident response system.

Policy: Monitor the systems

There will be monitoring of all IT systems connected to the network to detect attacks and indicators of potential attack, and to detect unauthorized local, network, and remote connections. Detected events and anomalies will be analyzed to determine their potential impact on business operations. Legal opinion must be obtained before proceeding with system monitoring activities.

Procedure

Anthem's Corporate Security department is responsible for monitoring IT systems connected to the network. They must adjust the level of system monitoring activity when there is a change in risk to business operations and assets, individuals, or other companies. In addition, they must provide significant system monitoring information to the Board of Directors for further consultation.

Review Frequency

The system monitoring policy must be reviewed annually, with the report submitted to the Board of Directors by the end of the year. This report must contain information regarding the scanners' configuration and performance, as well as captured events and anomalies, to determine effectiveness and make changes if necessary.

Control: Incident Handling

Incident response plays an important part in the definition, design, and development of mission and business processes and systems. The NIST 800-53 IR-4 control encourages implementation of an incident handling capability for incidents that is consistent with the incident response plan. This will become important in the event of an incident, as most of the response activities will have been handled by the incident handling capabilities that were set in place in preparation for such occasions. This saves the company time and effort in creating solutions to problems in the heat of the moment.

Policy: Implement an incident handling capability

The incident handling capability must include preparation, detection and analysis, containment, eradication, and recovery measures, and incident handling activities have to be coordinated with contingency planning activities. Emergency contact lists of people inside and outside the company need to be created so that they can be contacted in case of an incident. Lastly, evidence of an incident must be stored and preserved on an encrypted hard drive.

Procedure

The Corporate Security department is responsible for installing, configuring, and monitoring IT systems to be used in incident handling. The Board of Directors must incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, implementing the resulting changes accordingly. The board must also ensure that the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the company. In order to be most effective, incident handling activities must be coordinated among many different entities in the company, including mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, legal departments, risk executives, etc. There must also be a way to report incidents–this should be done with an email address and/or a phone number.

Review Frequency

The review frequency for the incident handling policy is to be done annually. The report must contain all information about incidents, lessons learned, contact lists, and employee feedback to assess its effectiveness. This report must be compiled by the Corporate

Security department and submitted to the Board of Directors before the end of the year. The report will also be assessed by the Audit Committee.

Control: Roles and Responsibilities

Defining roles and responsibilities in a business can prevent confusion within a company and any consequences that result from this uncertainty. Having defined roles and responsibilities will also help in acquiring employees with certain skills, filling in the gaps that need to be filled. Assigning roles such as “penetration tester,” “data recovery professional,” or “security awareness training specialist” helps in determining what level of access they should have in using the company’s IT systems. And once these individuals are made aware of their roles and responsibilities, the easier it is to deter and detect incidents. Non-repudiation is achieved as employees are more easily held accountable for their actions, and are more likely to work efficiently.

Policy: Establish user roles and responsibilities

HRS-07 from the Cloud Controls Matrix states that the roles and responsibilities of contractors, employees, and third-party users must be documented as they relate to information assets and security. This control will be used to hold users accountable for their responsibilities related to incident response. Employees and contractors can only use IT systems to complete occupational tasks and to communicate with other employees. Third-party users can only use IT systems for business purposes (e.g., communicating with business partners, presenting information, etc.). System monitoring devices will be used to detect anomalies on the network and on IT systems.

Procedure

The Board of Directors is responsible for assigning roles and responsibilities to Anthem employees, contractors, and third-party users as they relate to IT systems and security. The Corporate Security department will be responsible for monitoring systems to ensure that employees are working within their roles and responsibilities. Incidents will be detected and reported to the Board of Directors. As a penalty, employees may be forced to go on temporary leave or dismissed permanently. Certain situations, such as an insider attack by an employee, contractor, or third-party user, will result in a lawsuit. The board must document all the defined roles and responsibilities and make any changes when there is a change in the company.

Review Frequency

This policy is to be reviewed annually by the Board of Directors, with a report compiled and provided to the board by the Corporate Security department. Roles and responsibilities have to be evaluated to determine if they should be changed, merged with one another, or

removed completely. This report has to be submitted by the end of the year. The board must consult with Anthem executives in assessing the roles and responsibilities of users.

Electronic Health Records (Michael Turkson)

Electronic Health Records are an electronic representation of a patient's medical history that Anthem keeps track of over time. They include demographics, progress notes, issues, prescriptions, vital signs, prior medical history, vaccines, laboratory data, and radiology reports, among other things. The electronic health record streamlines the clinician's workflow by automating access to information. Other care-related tasks, such as evidence-based decision support, quality monitoring, and outcomes reporting, can be supported directly or indirectly by the EHR through various interfaces.

Despite the fact that the majority of EHR systems are safe and secure, doctors and practice managers are nevertheless concerned about data breaches caused by ransomware and other cyber security intrusions. Data tampering, data loss during a natural catastrophe, and illegal access to patient information are all challenges that most practices encounter.

The following NIST Cybersecurity Framework Protect and Detect function subcategories are acceptable for this asset's risk:

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

Healthcare businesses may utilize Identity Management, Authentication, and Access Controls to safeguard patient profile information, grant and restrict user access privileges, and manage improved identity governance. It safeguards sensitive data within the system and verifies a user's position in order to have access to it. It recognizes, authenticates, and allows access to applications, systems, networks, and portals while recognizing the individual's status in a healthcare context as a patient, health plan member, healthcare professional, employee, or vendor. When an unencrypted communication is sent over the internet, it can readily be intercepted and viewed by unauthorized parties. If records must be transferred electronically, healthcare facilities should ensure that they have some control over who has access to them. Secure remote access allows you to access your records at any time.

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

Maintaining a separate network for users to manage allows anthem to identify and respond to risks to electronic health records. In order to determine what is normal traffic, a baseline of network operations and expected data flows for users and systems should be established. Once spotted, this behavior may be reported to professionals for additional analysis and then terminated, averting both a security breach and hipaa violations.

Anthem's systems must be monitored to detect attacks and signs of possible attacks, as well as illegal local, network, and distant connections, in line with their monitoring objectives. This control can also be used to detect illegal system usage by triggering internal monitoring capabilities or the deployment of monitoring devices. Controlling EHR systems may be done by implementing authentication mechanisms such as two-factor authentication and retaining specific credentials for permitted users.

Control: Intrusion Detection System and Advanced Passwords

An Intrusion Detection System (IDS) and advanced passwords are mitigation against ransomware within electronic health records. An Intrusion Detection System compares network traffic records to signatures that recognize known malicious behavior to hunt for harmful activity. An effective IDS will regularly update signatures and notify your anthem if it finds potentially dangerous behavior. Along with giving specified access to EHR systems, having complex passwords across the board minimizes the chances of threats against the systems.

Policy: Install IDS on all machines, and require employees with EHR access to set complex passwords

To guard against malicious ransomware, all workstations linked to business networks, whether directly or indirectly, must have an intrusion detection system. Employees must also follow password rules that include two words separated by a hyphen, two digits at the end, and one unique character. Workstations must be properly patched every week to keep the intrusion detection systems actively running.

Procedure

The IT Department is in charge of mandating active intrusion detection software on any systems that are accessible over the internet. At the very least, both host-based and network-based intrusion detection systems must be examined and their logs evaluated on a daily basis. Logs of intrusion detection must be retained for at least 30 days. The team will keep an eye on both host-based and network-based intrusion detection systems. At the very least, check the intrusion detection logs on a daily basis. Determine which intrusion detection systems and software are acceptable. Act on reported occurrences to minimize damage, archive any hostile or unauthorized software for investigation, and suggest improvements to avoid future incidents. Notify impacted clients on the scope of the breach, how it was resolved, and what steps they should take next.

Review Frequency

At the very least, both host-based and network-based intrusion detection systems must be examined and their logs evaluated on a daily basis. Logs of intrusion detection must be retained for at least 30 days. Reports will be taken on a monthly basis, by the IT department with a final review with operations once a year. From there, you'll be able to see what's been working and what needs to be improved.

Payroll Systems (Michael Turkson)

The process of paying salaried, hourly, and contingent employees is automated with payroll software. Payroll software is frequently sold as a stand-alone solution by human resources technology vendors and specialist payroll providers. Payroll software is becoming a more integral part of multifunctional, integrated human capital management systems. Payroll software, as opposed to paper-based methods, speeds up the payroll process while also decreasing mistakes and allowing managers to more easily tailor paychecks for individual employees. Establishing a separation of roles to guarantee that no single person is responsible for both the creation and approval of payroll transactions. This eliminates the possibility of corporate cash being misappropriated. Unauthorized modifications to payroll master data or the formation of fictional or "ghost" workers might occur if suitable safeguards are not in place.

The following NIST Cybersecurity Framework Identify and Respond function subcategories are acceptable for this asset's risk:

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

Maintaining a risk plan across payroll systems provides a sense of security and demonstrates that Anthem is prepared in the event of a disaster. It will be helpful to have documentation of discovered threats and vulnerabilities in order to better understand the cybersecurity risk to Anthem's operations and how it may affect their systems. All of these metrics are significant because they demonstrate to Anthem's clients and stakeholders that they have built a risk management plan that is regularly monitored. Having a plan in place to handle the risks of running payroll systems

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

Because emergency pay systems and detection give companies with a back-up to support their payroll process in a way that helps minimize interruption during catastrophic events like a natural catastrophe or a security breach, Anthem integrating reaction planning for payroll systems is critical.

When conventional payroll services or providers are unavailable, an emergency payroll service provider may be able to assist in the continuance of payroll distribution through cheque, direct deposit, or pay card.

The purpose of data protection training is to teach users about the methods and technologies that may be used to prevent data leakage, and minimize the impacts and maintain the privacy and integrity of sensitive data. Concerns about storage capacity, manipulation, and information leakage are addressed. Similar to the preceding item, requiring authentication is a control that would be desirable.

Control: Fraud Risk Assessment and Two-Factor Authentication

A fraud risk assessment, as well as requiring workers to utilize two-factor authentication through hardware token, will protect the Anthem Payroll System from security breaches. An evaluation of fraud risk would be tailored to Anthem's specific business and activities. Because changes in the internal and external environment are inevitable, management and managers responsible for each department should conduct a risk assessment by examining the organization's exposure to fraud risk events within payroll. Because the assessment should be refreshed on a regular basis to mitigate risks to an acceptable level, the assessment should be refreshed on a regular basis. Employees with payroll access will benefit from two-factor authentication using a hardware token, which will increase protection to their login information and restrict invasions.

Policy: Perform risk assessments on Anthem's payroll system and issue hardware keys to employees for 2FA purposes

Every three months, a risk assessment will be conducted to detect vulnerable places within Anthem's payroll systems in order to safeguard against threat turnover. By tracking login time and roles inside the system, all workers will participate in this evaluation. In addition, after entering their standard credentials, each employee will register a hardware token device that will require them to provide a six-digit number to access to the payroll system.

Procedure

In terms of risk assessment, the IT department will examine payroll records for missing data such as date of birth, social security number, and so on. Verify the existence of several employees who share the same address in payroll information. Check dates for odd patterns and exceptions and stratify payment amounts, hours worked, and hourly rates. In

addition, the IT department will offer information on the amount of tokens that have been connected with Anthem accounts as well as reactivating tokens as necessary.

Review Frequency

The IT department will compile monthly reports on the assessment, with a final evaluation with executives once a year. You'll be able to see what's working and what needs to be improved from there and the security strength of the payroll system.

Conclusion

The actuary equations and websites of Anthem are critically important to Anthem's operations. To protect actuary equations a self-contained network would make sure other breaches do not affect it. Also, training employees who will deal with these equations ensure there will be less human errors on leaking data. Also, since this data is so important, backup plans should be in place to make sure nothing happens with them as well as making sure a constantly improving recovery plan is in place in case of an incident so it isn't too devastating. Websites are an easy target for attacking so mitigation and analysis plans should be in place to adequately respond and improve their experiences for the future. Since the websites are so integral there also needs to be systems in place to ensure even in the case of incidents, downtime is limited as much as possible in the form of a contingency plan. Also, since the website can handle such critical data they need to follow government guidelines on handling sensitive information.

Creating and maintaining a risk management strategy is essential for protecting critical assets. This includes conducting a risk assessment of Anthem's cloud data infrastructure which identifies and documents vulnerabilities and internal/external threats. The risk management strategy further outlines company priorities, constraints, risk tolerance, and assumptions to be considered in making risk decisions related to their data infrastructure. Anthem's cloud data infrastructure relies heavily on employing these cybersecurity measures to mitigate the risk of a data breach. Moreover, we advise implementing protective data controls related to storage capacity, tampering, and information disclosure. We also recommend limiting access and functionality of Anthem's information systems, disabling any unnecessary/vulnerable functions and services that could severely impact security and performance. Anthem's medical software can be secured by detecting anomalies and events, and establishing incident alert thresholds that indicate incident severity, overrides, and other factors. Continuous monitoring of software to detect errors/malicious code and vulnerability scanning will also help improve Anthem's cybersecurity posture. Furthermore, it is important that the individuals using the software are aware of their roles and responsibilities so that they can respond appropriately to incidents. We also recommend coordinating response activities with external stakeholders to achieve a broader cybersecurity situational awareness. The response strategies must

implement incident handling controls to save the company time and effort in resolving problems when they arise.

Both Anthem`s electronic health records and payroll systems are important to the functioning ability for the organization as a provider of healthcare to the public. In the case of electronic health records, installing an intrusion detection system on all systems and requiring password upgrades enhances the overall security of the information and reduces threats to the system. It also allows the IT/Cyber team to more readily discover concerns and maintain track of personnel who have specific levels of access. User access is the most serious vulnerability to payroll systems. Implementing two-factor authentication methods will increase security by preventing unwanted users from accessing the system and minimizing circumstances like exchanging login credentials. Anthem achieves a greater degree of cybersecurity as a company by employing several tiers of protection, comparable to the functions of firewalls.

For healthcare organizations like Anthem, cybersecurity plays a vital role in protecting information that is constantly transmitted over the Internet. Much of this information is sensitive and must remain confidential for the sake of privacy. The protection of this data is also important in that a massive security breach could cause a considerable blow for the reputation of any organization. This was made evident in 2015, where it was revealed that Anthem experienced a massive data breach 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 like Anthem, 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 the guidelines for best practices, policies, procedures and controls which will serve to improve all aspects of their cybersecurity infrastructure. However, maintaining a strong cybersecurity stance requires having due diligence over cyber activities, consistent compliance, and shrewdness over cyber risks and mitigation methods that are constantly evolving. Under these conditions, we recognize that there will always be room for improvement in cybersecurity and we recommend that Anthem remains vigilant and committed to the continuous development and enhancement of their cybersecurity infrastructure.