# AbbVie

# Cybersecurity Assessment

4/20/25

**Team Members: Kennedy Bellamy, Destiny Hale, Ashley Barasebwa**

# Table of Contents

## Company Profile

AbbVie is a biopharmaceutical research and development company in North Chicago, Illinois. It combines the focus and passion of biotechnology with the expertise of a pharmaceutical leader. AbbVie's mission is to research and develop innovative medicines and solutions to improve people's health, working collaboratively with its global R&D and manufacturing sites. Its products treat over 60 million patients annually, help 175 countries, and cure over 75 conditions. Overall, their products impact the lives of millions.

AbbVie was founded in 2013 after separating from its parent company, Abbott, to become a more global, consumer-focused company. In January 2013, the company became official during its New York Stock Exchange bell-ringing opening. In April 2013, AbbVie released its first batch of products off the production line. Within a day, over 23,000 products were made for patients in the United States. After the product launch in May 2013, the company's focus shifted to reviewing and developing drugs for 71 million people infected with hepatitis C. This led to the company's first therapy designation given by the FDA. A year later, the company released its first medicine, Viekira Pak, after it was approved in the United States. This medicine was developed for the treatment of chronic genotype 1 hepatitis C. The results from this medicine cured 95-97 percent of patients who had the virus.

In 2016, AbbVie opened the Cambridge Research Center in Massachusetts. The company used this building to research neurodegenerative diseases such as Alzheimer's disease. In addition to its goal, AbbVie planned to research other neurodegenerative diseases such as Parkinson's and multiple sclerosis. Also in 2016, AbbVie led the biotechnology industry in the Dow Jones Sustainability Index for the third time in a row. It had the highest industry score on 12 of 22 criteria. In 2020, the company launched a new aesthetic line called Allergan Aesthetics. The brand focused on developing aesthetic medicine for all skin types and genders. In 2022, AbbVie opened a new facility in the Bay Area for collaboration in oncology research and development. For over 10 years, AbbVie has invested $50 billion in development and research, creating impactful medicine.

AbbVie operates in both the biotechnology and pharmaceutical industries. Biotechnology industries develop products, improve plants and animals, develop new processes, fight disease, and reduce the environmental impact. In pharmaceutical industries, they research, develop, manufacture, distribute, and market products. With the combination of both industries, AbbVie researches and develops medicines to cure diseases and improve the health of society in the areas of immunology, oncology, neuroscience, eye care, and other specialties.

AbbVie sells a variety of products for cancer, arthritis, and other health conditions. A couple of the company's products are:  Botox, Vraylar, Skyrizi, Rinvoq, and more. However, the two key products are Humira and Vraylar.

Humira is used to treat arthritis, Crohn's disease, and plaque psoriasis. Vraylar is used to treat schizophrenia and bipolar disorder. The revenue gained from Humira from 2011-2022 was over $29.1 billion. However, in 2023, the revenue decreased by 7 billion dollars when it switched to generics. As for Vraylar, the revenue gained was $984 million with a 17.1% increase.

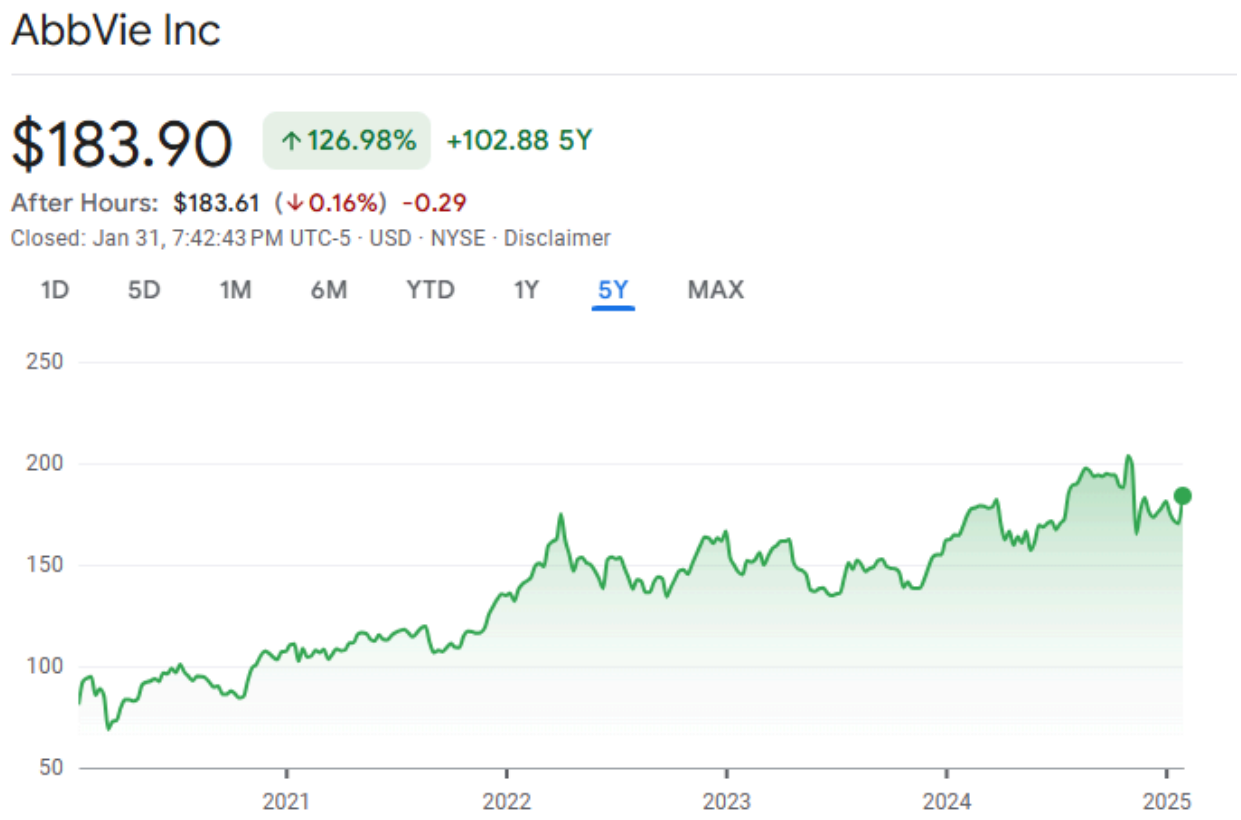


*Image source: Google Finance*

## Overview

Biotechnology companies such as AbbVie are prime targets for cyber attacks, due to them being in the medical field. In this assessment, we discuss the cybersecurity assessment of AbbVie and the policies that shall be taken to mitigate cyber risks. These procedures aim to strengthen AbbVie's defenses, reduce the likelihood of data breaches, and ensure the protection of sensitive medical and research information.

# Asset Ranking

## Asset Ranking

| Assets | Description | Value | Reasoning |
|---|---|---|---|
| E-Clinical Systems | Digital systems that help with clinical trials and healthcare | 8 | Compromisation of availability and integrity also applies to these systems. |
| Order Management System | A system that manages and tracks order entries, customer orders, inventory, etc. | 9 | Credentials from customers can be stolen or order processing can be disrupted leading to loss of products and sales. |
| Employees | The people who work at AbbVie, including the chemists, manufacturing workers, and pharmaceutical engineers | 8 | This asset should be listed due to Employees being a crucial asset to AbbVie, as they drive research, innovation, production, and business operations. They are ranked as a 6 due to their roles having the ability to be replaced. Their roles can even be replaced by AI in the future |
| Supply Chain | The system of individuals, resources, and processes involved in producing and delivering a product to consumers. | 7 | This asset should be listed due to the company not being able to provide all the processes for itself on its own, it needs other entities to help provide for their pharmaceuticals. The value of this asset is at a 7 because it is close to being extremely high. |

| Asset Ranking | | | |
|---|---|---|---|
| Clinical Trial Data | Data from clinical trials is likely stored in a digital database which includes the patient's information, drug effectiveness, and more | 8 | This information is crucial for regulatory approval. Exposure to competitors or leaks may result in financial losses, regulatory penalties, and ethical challenges. |
| Backup systems | where critical data, research files, patient records, and other documents are stored | 8 | Cloud services increase efficiency but offer risks if not properly secured. A malfunction or outage could cause operational disruptions. |
| ERP Systems | any digital tools used for monetary transactions, and business management/engagement | 9 | Not protecting this information could result in a data breach, causing financial fraud or regulatory violations. |
| AI & Data Analytics | Machine learning models and big data analytics are used to refine business operations and enhance drug research | 7 | The main risk is data integrity and AI model security, which plays a role in the decision-making processes. |
| Biosensors & Wearables | Medical devices that monitor patients' vitals | 10 | If these devices are tampered with, this can put the patient's life at high risk. |
| ARCH (AbbVie R&D Convergence Hub) | An AI platform that AbbVie created for analytics and scientific insights | 8 | Availability and integrity of data can be compromised once obtained by malicious actors. |

## Risk Management Matrix

### Risk Management Matrix

| Assets | Risk Description | Business Consequences | Severity | Likelihood | Score | Mitigation | RACI |
|---|---|---|---|---|---|---|---|
| Clinical Trial Data | Unauthorized access and compromised data | Loss of trust and important data | 88 | 82% | 72.16 | Encryption and authentication | **Responsible:** Information Technology **Accountable:** Information Technology **Consulted:** Legal **Informed:** Legal |
| Backup Systems | Failure to successfully recover data and unauthorized access to data backups | Data and financial loss | 89 | 84% | 74.76 | Test backup procedures | **Responsible:** Information Technology **Accountable:** Operations **Consulted:** Legal **Informed:** Information Technology |

## Risk Management Matrix

| Assets | Risk Description | Business Consequences | Severity | Likelihood | Score | Mitigation | RACI |
|---|---|---|---|---|---|---|---|
| Order Management Systems | System failure, human error, data leak, and malware | Disruption of production of treatments/medicines, delay of shipping batches, loss of reputation/collaboration , loss of product sales, and possible loss of company | 100 | 90% | 90 | Employee training, security audits, anti-malware, backup systems, encryption, task automation, IDS | **Responsible:** Supply Chain **Accountable:** Operations **Consulted:** Marketing **Informed:** Sales |
| E-clinical systems | Tampering, system failures, human error, data leak, malware, and ransomware | Disruption of clinical trials, loss of patient data, loss of development for treatments/medicines | 80 | 90% | 72 | Employee training, security audits, anti-malware, backup systems, encryption, task automation, IDS, regular updates | **Responsible:** Operations **Accountable:** Information Technology **Consulted:** Executive Team **Informed:** Executive Team |
| Employees | Unauthorized disclosure of sensitive data | Financial loss | 60 | 70% | 42 | Access Control | **Responsible:** Operation **Accountable:** Marketing **Consulted**: Information Technology **Informed:** |

## Risk Management Matrix

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | Executive Team |
| Supply Chain | Unauthorized access to systems or data | Unauthorized access to systems or data | 70 | 45% | 31.5 | Access Control | **Responsible:** Marketing **Accountable:** Information Technology **Consulted:** Information Technology **Informed:** Executive Team |

## Assessment Recommendations

### Clinical Trial  Data

AbbVie's clinical trial data consists of extremely valuable research and patient information, which is vulnerable to data breaches or illegal access. To mitigate this, I chose the Protect and Detect functions of the NIST Cybersecurity framework. For the Protect function, I chose to focus on the Data Security (PR.DS) category with subcategories PR.DS-1: Data-at-rest is protected and PR.DS-5: Protections against data leaks are implemented, ensuring data is encrypted and safeguarded against leakage. Additionally, I chose Information Protection Processes and Procedures (PR.IP) with PR.IP-4: Backups of information are conducted, maintained, and tested and PR.IP-12: A vulnerability management plan is developed and implemented to reinforce data protection through secure backups and vulnerability management. For the Detect function, I chose the Security Continuous Monitoring (DE.CM) category with DE.CM-1: The network is monitored to detect potential cybersecurity events and DE.CM-4: Malicious code is detected to detect potential attacks on clinical trial data. I also selected Detection Processes (DE.DP) with DE.DP-3: Detection processes are tested and DE.DP-5: Detection processes are continuously improved to ensure ongoing optimization of monitoring efforts.

| | |
|---|---|
| **Asset:** | Clinical trial data |
| **Risk(s):** | Unauthorized access and compromised data |
| **Function(s):** | Protect and Detect |
| **Categories:** | Data Security (PR.DS) and Detection Processes (DE.DP) |
| **Sub-Categories:** | PR.DS-1: Data-at-rest is protected, PR.DS-5: Protections against data leaks are implemented, DE.DP-3: Detection processes are tested, and DE.DP-5: Detection processes are continuously improved |
| **Rationale**<br>Data from Clinical trials consists of highly sensitive information regarding patient records and private research. Gaining unauthorized access or experiencing a data breach within the company could result in regulatory penalties and damage to their reputation. To ensure the safety and security of this information, there should be extra measures taken to protect it, such as encryption (PR.DS-1). Leaked data might reveal sensitive patient and research information. Using adequate data loss prevention (DLP) measures reduces the risks of data being exposed (PR.DS-5). DE.DP-3: Cyber threats evolve quickly, which requires ongoing testing and constant improvement to detection processes. Failure to do so risks allowing advanced attacks to go undetected. DE.DP-5: To respond to evolving threats, continuous improvement is required and imperative. This will also increase detection capabilities eventually. | |
| **Policy:** | All clinical data must be backed up regularly and should also be tested consistently to ensure integrity. All clinical data should also be fully encrypted. |
| **Procedure:** | Create automated backup routines and run frequent restoration testing. Maintain an off-site backup source in the event backup systems are also compromised. |
| **Review Period:** | Bi-weekly reviews |
| **Control:** | Periodic verifications should be implemented to check backup restoration processes |

## Backup System

AbbVie's backup systems are critical for disaster recovery, but they are also vulnerable to malware and ransomware, which may hinder data recovery. I choose the Detect and Recover functions to address the risks of this asset. For the Detect function, I chose the Security Continuous Monitoring (DE.CM) category with DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed, and DE.CM-8: Vulnerability scans are performed as the subcategories to ensure continuous oversight of backup infrastructure

for unauthorized access and vulnerabilities. I also selected Detection Processes (DE.DP), which highlights DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability and DE.DP-3: Detection processes are tested as the subcategories to establish responsibilities and examine detection methods. For Recover, I chose Recovery Planning (RC.RP) with RC.RP-1: Recovery plan is executed during or after a cybersecurity incident, and Improvements (RC.IM) along with RC.IM-1: Recovery plans incorporate lessons learned to strengthen backup recovery capabilities through tested strategies and continuous modification.

| | |
|---|---|
| **Asset:** | Backup Systems |
| **Risk:** | Failure to successfully recover data and unauthorized access to data backups |
| **Function(s):** | Detect and Recover |
| **Categories:** | Security Continuous Monitoring (DE.CM), Detection Processes (DE.DP), Recovery Planning (RC.RP), and Improvements (RC.IM) |
| **Sub-Categories:** | DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed, DE.CM-8: Vulnerability scans are performed, DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability, DE.DP-3: Detection processes are tested, RC.RP-1: Recovery plan is executed during or after a cybersecurity incident, RC.IM-1: Recovery plans incorporate lessons learned |
| **Rationale** | |
| DE.CM-7 and DC.CM-8: unauthorized access to backup systems and unpatched vulnerabilities could result in exploitation and ransomware attacks, causing data to be lost or stolen. Backup systems should be regularly monitored to detect security threats early on. DE.DP-1 and DE.DP-3: Clear responsibilities and roles should be established to ensure accountability and efficiency when addressing any sort of incident. Testing regularly is crucial for detecting threats and also ensures that threats are being quickly identified. Lastly, RC.RP-1 and RC-IM-1: the sooner a recovery plan is executed the better for the continuation of the business. Continuously improving recovery procedures ensures adaptability to new threats as well. | |
| **Policy:** | Backup systems should be continuously monitored for unauthorized access attempts. In the case backup systems are accessible and compromised there should be a disaster recovery plan in place along with respective roles and responsibilities. |
| **Procedure:** | Incident response routines that specify what role applies to who while detecting security outbreaks |
| **Review Period:** | Quarterly review and Bi-annual drills and training |

| | |
|---|---|
| **Control:** | Security awareness training and drills for specific roles will be implemented |

## Order Management System

Order Management Systems (OMS) are systems that manage and track order entries, customer orders, inventory, etc. These systems provide efficient and accurate shipping, delivery, processing, and inventory for order fulfillment. However, the risks associated with these systems are system failure, human error, data leak, and malware. This can damage AbbVie's reputation, disrupt sales, and stop production. To safeguard OMS, AbbVie must apply the identify and respond functions, focusing on the categories of supply chain risk management and analysis. These involve the following subcategories: cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders (ID.SC-1); response and recovery planning and testing are conducted with suppliers and third-party providers (ID.SC-5); detection systems are investigated (RS.AN-1); and notifications from the impact of the incident is understood (RS.AN-2). Utilizing the functions will help AbbVie prioritize the systems and mitigate potential damages and impacts in an event of a possible cyber attack. With the implementation of both categories and subcategories, stakeholders, marketing, sales, and executive teams will be informed about these risks and improve the company's security posture to ensure business operations and resilience.

| | |
|---|---|
| **Asset:** | Order Management Systems |
| **Risk(s):** | System failure, human error, data leak, and malware |
| **Function(s):** | Identify & Respond |
| **Categories:** | Supply Chain Risk Management (ID.SC) & Analysis (RS.AN) |
| **Sub-Categories:** | Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders (ID.SC-1); response and recovery planning and testing are conducted with suppliers and third-party providers (ID.SC-5); detection systems are investigated (RS.AN-1); and notifications from the impact of the incident is understood (RS.AN-2) |
| **Rationale:**<br>Order management systems are an integral part of AbbVie's production of medications and the supply chain. However, if these systems are compromised, AbbVie would lose track of its shipments and order fulfillment. ID.SC-1: cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders is ensuring that organizations must define, implement, evaluate, | |

| | |
|---|---|
| manage, and agree to these processes. This also applies to third-party providers. In rare cases, cyber attacks can occur from outdated systems and software from third-party providers. This applies to subcategories of ID.SC-5: response and recovery planning and testing are conducted with suppliers and third-party providers, RS.AN-1: detection systems are investigated, and RS.AN-2 notifications from the impact of the incident are understood. If an attack or disruption occurs within the supply chain, this will enable effective responses and mitigation solutions from both parties. This will improve AbbVie's security posture in business operations and resilience. | |
| **Policy:** | All stakeholders must be sure that all roles and responsibilities are assigned to make sure operations are up to par and that every OMS is updated. This also includes informing third-party providers for them to comply with this policy to update their software. |
| **Procedure:** | Testing, investigation of software, monitoring for suspicious activity, and weekly updates of these systems. |
| **Review Period:** | Semi-Annually |
| **Control:** | Performing monthly security audits to make sure OMS is updated and maintained. |

## e-Clinical Systems

E-clinical systems are digital systems that help medical professionals document clinical trials with patients in healthcare facilities. If these systems aren't properly taken care of, this could lead to the loss of information and development for medicines. The attacks that may put these systems at risk are tampering, system failures, human error, data leaks, malware, and ransomware. E-clinical information is valuable to AbbVie because this information stores the results from treatments, medicine, and patient health history. The application of protect and detect functions with a focus on the categories of information processes and procedures, and security continuous monitoring will provide an understanding of how to protect these systems and information. This also involves the subcategories of backups of information are conducted, maintained, and tested (PR.IP-4); protection processes are improved (PR.IP-7); monitoring for unauthorized personnel, connections, devices, and software is performed (DE.CM-7); and vulnerability scans performed (DE.CM-8). Utilizing the functions will help AbbVie develop safeguards and implement activities that will help identify cyber threats. The implementation of the categories will further keep the availability and integrity of information, establish roles and responsibilities, and

develop policies for maintaining the systems. Also, with the implementation of the subcategories, this will prevent the systems from getting compromised.

| **Asset:** | **E-Clinical Systems** |
|---|---|
| **Risk(s):** | Tampering, system failures, human error, data leak, malware, and ransomware |
| **Function(s):** | Protect & Detect |
| **Categories:** | Information processes and procedures & security continuous monitoring |
| **Sub-Categories:** | Backups of information are conducted, maintained, and tested (PR.IP-4); protection processes are improved (PR.IP-7); monitoring for unauthorized personnel, connections, devices, and software is performed (DE.CM-7); and vulnerability scans performed (DE.CM-8) |
| **Rationale**<br>E-clinical systems document every clinical trial, treatment, and medical history. This system is highly valuable to AbbVie because it helps them to keep a record of all progress from their products. However, this data holds confidential information that could be tampered with or stolen by attackers. PR.IP-4: Backups of information are conducted, maintained, and tested is to ensure that the data is copied and in good condition and verify that the backup servers can be used to restore that data. To make sure these systems and servers are updated, DE.CM-7: monitoring for unauthorized personnel, connections, devices, and software is performed, and DE.CM-8: vulnerability scans performed must be applied to ensure every device is monitored and weaknesses has been identified and addressed. This will prevent the systems from getting compromised. | |
| **Policy:** | All e-clinical data on backup servers must be encrypted and tested. |
| **Procedure:** | All data within these systems will be encrypted will state-of-the-art encryption technology and tested monthly to make sure they are updated and in good condition. |
| **Review Period:** | Annual |
| **Control:** | Endpoint Detection and Response (EDR) is installed on the servers for continuous monitoring to ensure the data is encrypted and systems are updated. This allows ensures data integrity and availability. |

## Employees

Employees are a critical asset to AbbVie, as they are the core human infrastructure that supports the company's research, development, and operational success. Unauthorized disclosure of sensitive data by an employee can result in financial loss, lawsuits against the company, and risks to patient safety. Two functions from the NIST Framework that are applicable to this asset are protect and detect, which focus on awareness, training and security continuous monitoring. Two subcategories within the awareness and training category that are applicable to employees are: PR.AT-1: All users are informed and trained, and PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities. Two subcategories included in the security continuous monitoring are: DE.CM-2: The physical environment is monitored to detect potential cybersecurity events and DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events. These categories were chosen to describe a mitigation to this risk due to their emphasis on equipping employees with the knowledge and awareness needed to recognize threats, handle sensitive data responsibly, and prevent unintentional or malicious data leaks.

| | |
|---|---|
| **Asset:** | Employees |
| **Risk:** | Unauthorized disclosure of sensitive data |
| **Function(s):** | Protect & Detect |
| **Categories:** | Awareness and training & security continuous monitoring |
| **Sub-Categories:** | PR.AT-1: All users are informed and trained, and PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities. DE.CM-2: The physical environment is monitored to detect potential cybersecurity events and DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events. |

**Rationale**

The reasoning for the choice of the categories Awareness and Training (PR.AT) and Security Continuous Monitoring (DE.CM) is due to their critical role in preventing and detecting insider threats, as cybersecurity training ensures employees understand the risks of data leaks, while continuous monitoring enables real-time detection of suspicious activities that could compromise AbbVie's sensitive pharmaceutical information. The subcategories were chosen due to their essential role in mitigating insider threats, as ensuring all users and third-party stakeholders are properly trained (PR.AT-1, PR.AT-3) reduces the risk of accidental or intentional data leaks, while monitoring the physical environment and personnel activity (DE.CM-2, DE.CM-3) ensures early detection and response to potential cybersecurity incidents involving sensitive AbbVie data.

| | |
|---|---|
| **Policy:** | All employees and third-party stakeholders (e.g., suppliers, partners) must complete regular cybersecurity awareness training on data protection, insider threats, and their roles in safeguarding sensitive information. |
| **Procedure:** | AbbVie will design a structured cybersecurity awareness training program that covers data security best practices, insider threat risks, regulatory compliance such as HIPAA and GDPR, and the company's policies on handling sensitive information. |
| **Review Period:** | Monthly |
| **Control:** | Employees who fail to complete required security training within the designated timeframe will have their system or data access restricted until they comply. |

## Supply Chain

The supply chain of AbbVie's pharmaceutical company is vital to the company's processes to carry out its mission. One risk that can arise from the usage of a supply chain is unauthorized access to systems or data, which could lead to disruptions in production, exposure of product formulas, and third-party information. Two functions from the NIST Framework that pertain to this asset are respond and recover, which concentrate on communications and analysis. Two subcategories within the communications category that are relevant to the supply chain include: RS.CO-4: Coordination with stakeholders occurs consistent with response plans and RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness. Two subcategories falling under the analysis category are: RS.AN-4: Incidents are categorized consistent with response plans and RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers). These categories were chosen to outline the critical actions needed to respond to and recover from potential cyber threats to the AbbVie supply chain.

| | |
|---|---|
| **Asset:** | Supply Chain |
| **Risk:** | Unauthorized access to systems or data |
| **Function(s):** | Respond & Recover |
| **Categories:** | Communications and analysis |

| | |
|---|---|
| **Sub-Categories:** | RS.CO-4: Coordination with stakeholders occurs consistent with response plans and RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness. RS.AN-4: Incidents are categorized consistent with response plans and RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers). |
| **Rationale** | |
| The reasoning for the choice of the categories, Communications and Analysis, is due to their essential role in ensuring timely incident response, as clear communication helps in mitigation efforts, and analysis helps identify the source, assess impact, and prevent future data leaks within AbbVie. The subcategories were chosen due to their role in ensuring an effective cybersecurity response at AbbVie, as coordinated stakeholder communication and voluntary information sharing enhance situational awareness, while incident categorization and a structured vulnerability response process enable timely identification, analysis, and mitigation of security threats. | |
| **Policy:** | Establish a formal protocol to ensure that third-party vendors, suppliers, and external partners align with AbbVie's cybersecurity response plans |
| **Procedure:** | Develop a secure portal to coordinate cybersecurity information with supply chain partners. |
| **Review Period:** | Annual |
| **Control:** | Require all technological communications with supply chain partners to be conducted through encrypted email, secure portals, or virtual private networks (VPNs) to prevent unauthorized access. |

## Conclusion

AbbVie has strategically aligned selected NIST framework subcategories with key functions such as Identify, Protect, Detect, Respond, and Recover- focusing on insider threat prevention, the integrity of clinical trial data, and supply chain resiliency to further strengthen the company's cybersecurity posture to ensure the business operation and resilience. The selected subcategories—PR.AT-1, PR.AT-3, DE.CM-2, and DE.CM-3—were chosen because they directly support the Protect and Detect functions of the NIST Framework and are critical in

addressing the risk of unauthorized disclosure of sensitive data by employees. By enforcing a mandatory cybersecurity awareness training policy for all employees and third-party stakeholders, AbbVie can ensure users are equipped with the knowledge to recognize and prevent insider threats. This is supported by a structured training program that emphasizes data protection, insider threat recognition, and regulatory compliance. The associated control of restricting system access for noncompliance further strengthens accountability. Also, the implementation of continuous monitoring of the physical environment and personnel activity provides early detection of suspicious behavior, allowing for rapid response. Together, these measures significantly enhance AbbVie's cybersecurity stance by reducing the risk of data leakage and enabling timely detection of insider threats.

The selected subcategories—RS.CO-4, RS.CO-5, RS.AN-4, and RS.AN-5—were identified as key components in enhancing AbbVie's incident response to the risk of unauthorized access to AbbVie's systems or data through its supply chain. These subcategories support the Respond and Recover functions of the NIST Framework by strengthening coordination, communication, and analysis during cybersecurity events. Implementing a formal policy that aligns third-party stakeholders with AbbVie's response plans ensures a unified and timely approach to incident management. The use of a secure portal for communication fosters consistent and efficient exchange of cybersecurity information, while controls such as encrypted communications and VPNs mitigate the risk of data exposure. Together, these measures enhance AbbVie's ability to detect, analyze, and contain threats originating from its supply chain, which helps strengthen AbbVie's cybersecurity defenses.

The selected subcategories of Identify and Respond, such as ID.SC-1, ID.SC-5, RS.AN-1, RS.AN-2 can help AbbVie implement supply chain risk management policies to protect the operation of their order management systems (OMS). All stakeholders must make sure that roles and responsibilities are assigned and comply with the processes that follow. The procedures, such as testing, investigation of software, monitoring for suspicious activity, weekly updates of these systems, and updating third-party systems, will further maintain and prevent the systems from being compromised. On rare occasions, a cyber attack can happen from outdated third-party software and services which lead to damage to systems and business operations from both parties. However, implementing a control such as monthly security audits will ensure systems are up to par. If an attack or disruption occurs within the supply chain, this will enable effective responses and mitigation solutions from both parties.

The selected subcategories of Protect and Detect such as PR.IP-4, PR.IP-7, DE.CM-7, DE.CM-8 would ensure the data integrity and availability of AbbVie's e-clinical systems. E-Clincal data holds valuable information that can be stolen by malicious actors. Therefore, AbbVie must implement backup and encryption policies to protect their information. The procedure would follow that all data within these systems will be encrypted with state-of-the-art encryption technology and tested monthly to make sure they are updated and in good condition. This includes vulnerability scanning and constant monitoring for unauthorized access in the prevention of

tampering and data breaches. To futher keep the integrity and availability of the information stored on these systems and servers, a control of installing endpoint detection and response software will be implemented for continuous monitoring. While technical safeguards are essential for AbbVie's systems, it is equally important to consider the human factors, such as design thinking, that influence the effectiveness and adaptability of these cybersecurity measures.

AbbVie's cybersecurity stance is the use of human-centered approaches such as design thinking. While much of the cybersecurity field is driven by technological innovation, detection systems, and the enforcement of regulations, human aspects that contribute to vulnerabilities are also important. The design thinking approach is a method that prioritizes end users, behaviors, and workflows in problem-solving. This approach identifies underlying issues that typical assessments or audits may miss, such as user conflict, communication errors, and system errors. Starting with empathy and connecting with employees' genuine experiences across departments makes it easier to determine when cybersecurity measures impact productivity or clarity. Design thinking helps to link strategy with practical workflows by identifying gaps that occur when cybersecurity protocols are not tailored for these particular circumstances.

Additionally, this design thinking process and approach has long-term crucial benefits. It is easier to scale cybersecurity solutions across several teams, geographical locations, and technological platforms when empathy, co-creation, and continuous problem-solving are encouraged. The ability to adapt is crucial for AbbVie, whose worldwide client base includes highly regulated and constantly changing markets. Secure practices and platforms should meet a wide range of needs while maintaining strong data protection standards, specifically in sensitive areas like research and development, clinical trials, and patient information systems.

Overall, the implementation of a design thinking approach into AbbVie's cybersecurity development enhances the company's ability to build defenses that are both highly effective and fully adaptable to the experiences of employees and the realities of their workforce. Solutions become more comprehensive, long-lasting, and significant when cybersecurity is also considered a human-oriented problem rather than just a technology essential. The technical suggestions made in the report are strengthened and complemented by this wider perspective, which ensures that AbbVie is not only protecting its resources but also enabling its employees to actively contribute to the development of a safe online environment.

# References

AbbVie Celebrates Launch as New Biopharmaceutical Company with Employees, Patients | AbbVie News Center | January 2, 2013

https://news.abbvie.com/2013-01-02-AbbVie-Celebrates-Launch-as-New-Biopharmaceutical-Company-with-Employees-Patients

AbbVie Receives U.S. FDA Approval of Viekira Pak For The Treatment of Chronic Genotype 1 Hepatitis C | AbbVie News Center | December 19, 2014

https://news.abbvie.com/2014-12-19-AbbVie-Receives-U-S-FDA-Approval-of-VIEKIRA-PAK-TM-Ombitasvir-Paritaprevir-Ritonavir-Tablets-Dasabuvir-Tablets-for-the-Treatment-of-Chronic-Genotype-1-Hepatitis-C

AbbVie Reports Full-Year and Fourth-Quarter 2024 Financial Results | AbbVie Investors

https://investors.abbvie.com/news-releases/news-release-details/abbvie-reports-full-year-and-fourth-quarter-2024-financial

A History of Impact | AbbVie

https://www.abbvie.com/landing/a-history-of-impact.html

Areas of Focus | AbbVie

https://www.abbvie.com/science/areas-of-focus.html

Abbvie Stock Performance | Google Finance

https://www.google.com/finance/quote/ABBV:NYSE?hl=en&window=5Y

Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 | National Institute of Standards and Technology | April 26, 2018

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Humira | AbbVie

https://www.rxabbvie.com/pdf/humira.pdf

Our Cambridge Research Center Opens in Cambridge, Massachusetts | AbbVie News Center | May 18, 2016

https://news.abbvie.com/2016-05-18-Our-Cambridge-Research-Center-Opens-in-Cambridge,-Massachusetts

Vraylar | AbbVie

https://www.rxabbvie.com/pdf/vraylar_pi.pdf