Pfizer

Cybersecurity Assessment

4-14-2024

Team Members: Leah Drew, Paul Hess, Miranda Begley

Table of Contents

Company Profile (Paul Hess)

Pfizer is a research-based biotechnology company that is involved in the manufacture and development of medicines, vaccines, and other pharmaceutical products. Pfizer is multinational with 36 manufacturing sites and is headquartered in New York City. Pfizer has about 300 products that are used to fight challenging diseases like amyloidosis, cardiovascular metabolic issues, COVID-19, endocrine diseases, hemophilia, infectious diseases, inflammatory diseases, migraines, sickle cell disease, and women's health issues. In 2022, Pfizer’s total revenue was approximately $100 billion.

Pfizer was founded by Charles Pfizer and Charles Erhart, two German entrepreneurs, in 1849 in Brooklyn, New York, and was originally a business that manufactured industrial chemicals. Pfizer became the largest producer of penicillin in 1919 after James Currie and Jasper Kane developed a method for citric acid production.. Pfizer became multinational in 1951.

The pharmaceutical industry is focused on the development, manufacture, and sale of drugs and medications. The pharmaceutical industry is complicated by the many laws that govern their work. For example, exclusivity for drugs developed has a limited timeframe, resulting in companies losing products to their competitors. The complex approval system for new treatments also greatly impacts profitability.

Pfizer is most well-known for their development of a COVID-19 vaccine and treatments. BNT162b2, also called Pfizer-BioNTech COVID-19 Vaccine or Comirnaty, was the first COVID-19 vaccine to receive FDA approval. The vaccine is delivered via an injection into the muscle. PAXLOVID is a medicine approved for emergency use by the FDA. PAXLOVID prevents moderate cases of COVID-19 from progressing to become severe COVID-19 cases. PAXLOVID is taken via two tablets, Nirmatrelvir and Ritonavir.

Asset Ranking (Miranda Begley)

Asset	Description	Ranking	Explanation/Reasoning
IoT devices/cloud	Pfizer distributes IoT devices in order for their employees to complete their job tasks. This includes cell phones, printers, laptops, bluetooth headphones, etc.	1	Attackers could steal confidential information from the company, data from millions of consumers, or mess with the integrity of their data. Pfizer might not be able to ever recover from this event if it occurs.
Inventory Management Systems	Inventory Management Systems are responsible for managing its inventory of products. IThe IMS is used to record how many products they have, order new products, note market trends, and more. The IMS includes IT systems, like the computers, printers, or phones used to note how much inventory Pfizer has.	2	If the inventory management system experiences any type of downtime, Pfizer can lose out on billions of dollars or even have their reputation ruined. If the data that is stored inside the inventory management system is breached, sensitive information can be stolen or corrupted.
Web servers	Web servers are used to host Pfizer's website and communicate with customers. Servers can be targeted by a DDoS attack.	3	A DDoS attack would cause financial consequences for Pfizer. DDoS attacks should be losses for even if they aren't anticipated to happen frequently.
Research databases	Research databases contain information about ongoing and past research. This information may contain the research participants' PII.	4	Insider threats may compromise this information if a disgruntled employee is given access to this data. Participants PII can be exposed which can lead to loss of reputation and trust from participants and customers.
Factories	Factories are where Pfizer manufactures products.	5	This is crucial because factories are required for daily production
Intellectual property	IP consists of trade secrets and other intangible products that are property of Pfizer.	6	IP could be compromised and used by competitors. The company could face the loss of a product and financial losses including the cost used to research that product.

Risk Management Matrix (Miranda Begley)

#	Asset	Risk	Business Consequences	Severity	Likelihood	Score
1	Intellectual property	IP can be compromised	Loss of product and cost used to research it.	70	20%	14.
2	IoT devices	Attackers can compromise IoT devices	Loss of confidential information, data from consumers, or data integrity	90	35%	31.5
3	Web Servers	DDoS Attack	Financial losses and the availability of the web server	15	30%	4.5
4	Research Databases	Insider Threats	Financial losses, loss of PII	75	20%	15
5	Factories	Products could be compromised and could be used to cause physical harm	Loss of reputation and financial losses	85	10%	8.5
6	Inventory Management systems	Hacking, data breaches, unauthorized access, and natural disasters.	Financial losses, loss of reputation, corruption or theft of sensitive information.	78	25%	19.5

Mitigation	Responsible	Accountable	Consulted	Informed
Cybersecurity policy including cameras and live monitoring software.	Security Guards, Cybersecurity team	Chief Information officer	Cybersecurity professionals	Executive Team
Employee training on password safety, authentication, etc. and monitoring software.	IT director	Executive team	Operations	HR
DDoS protection software and recovery plan	Information Technician	Executive Team	Operations	Executive Team
Access control policies using the principle of least privilege and separation of duties	Chief Information Officer	Executive Team	IT team	HR
Create a strong response plan.	Computer Security Incident Response Team	Executive Team	Operations	Chief Information Officer
Regular updates, penetration testing, keycards or biometric authentication, take backups.	IT director	IT team	IT team	Chief Information Officer

Cybersecurity Metrics

Pfizer uses Key Performance Indicators (KPIs) for their cybersecurity metrics. One example of a KPI that the cybersecurity team uses is the **“level of preparedness” KPI**, which looks at the percentage of incidents in a one year that could have been prevented with proactive measures. This KPI also looks at how many cybersecurity training meetings occur and tests the knowledge of employees on cybersecurity. Another KPI of Pfizer is the **Intrusion attempts KPI.** This KPI measures things like how many intrusion attempts have been detected by your IDS and how many unauthorized access attempts have been blocked by your firewall. With the intrusion attempts KPI, things like how often your security logs are reviewed and what method is used for these reviews are noted. (Miranda Begley)

A crucial metric that Pfizer uses to determine how well their policies are working is by using the **Mean Time To Detect metric**. The MTTD looks at the average time it takes to detect and respond to a cybersecurity threat. This metric is used to identify where Pfizer’s detection system’s flaws are and make adjustments as needed. (Miranda Begley)

The **Mean Time To Resolve** metric works similarly by calculating the average time that Pfizer takes to resolve a security event. This could enable informed choices. Pfizer can use this metric to update policies based on whether or not they are determined to be working. **First-Party Security Ratings** analyze Pfizer’s cybersecurity posture as a whole. They can be used as a resource to determine if they are adhering to industry best practices. Pfizer may use a service such as UpGuard for this analysis to find ways to improve. **Access Management KPIs** analyze the management of Pfizer’s IAM system. For example whether the principle of least privilege is being applied and how many accounts have two-factor authentication enabled. Monitoring this can help Pfizer to prevent threats from bad actors that would try to gain unauthorized access. (Leah Drew)

Assessment Recommendations

Intellectual Property (Paul Hess)

Intellectual Property could be compromised either intentionally or unintentionally and used by competitors. The company could face the loss of a product and the cost used to research that product.

Detection/Security Continuous Monitoring (DE.CM)/DE.CM-3

The weakest link in cyber security is usually the human element. In this case, the humans handling the documents and other material related to an intellectual property pose the biggest threat to their dissemination. Additionally, the threat posed by the compromise of intellectual property is significant. It is a key component for Pfizer.

Recommended Control

Implement both human and machine reviews of personnel activity for any compromising activity.

The policies Pfizer should adopt to mitigate the threat posed by the disclosure of intellectual property should emphasize that the security of intellectual property is paramount. The procedures Pfizer implements to mitigate the threat of distributed intellectual property should designate different positions’ duties and responsibilities to protect the intellectual property.

Management should regularly check that procedures are being followed by employees via digital alerts that could be triggered and sent to management when procedures are not being followed, such as when log files have not been reviewed on time. By simulating an attempted theft of intellectual property, Pfizer could review the monitoring and ensure it is following the set standards of continuous monitoring.

Factories (Paul Hess)

Intentionally or unintentionally, products could be compromised via cyber means and even become dangerous. Customers may fear to use products from the company if such an event occurs.

Respond/Response Planning (RS.RP)/RS.RP-1

The threat posed by compromised pharmaceutical products is real and has occurred in the past. Pfizer should have a plan in place in the event such a compromise occurs. It is worth the creation of a plan for this type of event as it could greatly help in the aftermath of such a compromise. The very survival of the company could be at stake if such an event is not handled correctly and speedily. To have a product that is supposed to be associated with helping people be associated with making them sick or worse is a disastrous scenario for a pharmaceutical company.

Recommended Control

Create a comprehensive response plan in the event products become compromised.
The policies Pfizer can adopt to support the mitigation method of response planning for product contamination could include the goal of having a step by step response formula that is completely comprehensive and ready to be put into action. The procedures that support the Pfizer policy on response planning for product contamination should be extremely comprehensive and flexible. Implementation of the policy and procedure will likely require strong support from management and the cooperation of many departments. Some controls and validations that could be used to ensure the above procedures are being followed are regular check-ins by management and the testing of as many elements of the response plan as possible.

Web Servers (Leah Drew)

Pfizer has web servers to host their website and communicate with customers. It is possible for these servers to be targeted by a distributed denial of service attack. Downtime on a website would impact Pfizer's reputation and interfere with their ability to access systems they need for normal operations.

Recover/Recovery Planning (RC.RP)/RC.RP-1

A DDoS attack primarily affects the availability of a web server. A lack of availability would cause financial consequences for Pfizer. While it is difficult to take down the web servers of a large company such as Pfizer, it is not impossible. DDoS attacks should be prepared for even if they aren't anticipated to happen often. A strong recovery plan will limit the duration of downtime after the attack is resolved so that the web server can quickly become available again.

Recommended Control

Pfizer's recovery plan should outline the steps that the IT team will take to restore Pfizer's web servers to normal operations after a DDoS attack. The IT team should test affected systems first to determine what is functional. After that, they should bring each affected component back online. Backups may be required to restore the web server to a functional state, so Pfizer should back up these systems daily. Employees should be trained on these procedures, and testing of the entire plan should take place every six months. Testing should take place in a sandbox environment, where applications can freely be taken offline and brought back online again. If live applications are to be tested, then it would be acceptable to test them one at a time and notify customers that maintenance is taking place on the website.

Research Databases (Leah Drew)

Research databases contain information about ongoing and past research. This information may contain the research participants' PII. Insider threats may lead to this information being compromised if a disgruntled employee is given access to this data.

Protect/Identity Management, Authentication and Access Control (PR.AC)/PR.AC-4:

In the event of an insider threat, the personally identifiable information of patients could be leaked and Pfizer could suffer financial losses related to the breach. Insider threats that are due to poor access control are preventable. Most employees will not need access to the database and should not be given access. Using the principle of least privilege and separation of duties will limit the number of employees that could potentially steal sensitive information. Even if an employee has some access to the database, they will not be able to access everything with a strong access control policy.

Recommended Control

The system administrator should manage the Identity and Access Management system. The principle of least privilege should be applied to roles and employees should have no way to legitimately authenticate to the database if they do not have authorization. Two-factor authentication should be required for all employees. All access to the database should be logged and should be reviewed daily by the system administrator. System administrators should not have full control; a third party should also review the logs. Pfizer should review the IAM system to determine whether the permissions granted to roles are appropriate every three months. The software providing access control services should be updated regularly, which can be verified based on version number, and software should be tested to ensure that it is working correctly monthly.

Inventory Management Systems (Miranda Begley)

Inventory Management Systems are responsible for managing its inventory of medications and other healthcare products. Some of the ways that the Inventory Management Systems manage inventory is by recording how many products they have, ordering new products, noting market trends, and more. Some of the items that are involved in the Inventory Management Systems would be the IT systems, like the computers, printers, or phones used to note how much inventory Pfizer has.

Identify/Asset Management (ID.AM)/ID.AM-1

Pfizer's inventory management system is crucial for running their business. There are multiple risks associated with the inventory management system, including possible hackings of the system, data breaches, and unauthorized access to the system. Natural disasters can also occur that can ruin the buildings or devices that run the system. If the inventory management system experiences any type of downtime, Pfizer can lose out on billions of dollars or even have their reputation ruined. If the data that is stored inside the inventory management system is breached, sensitive information can be stolen or corrupted.

Recommended Control

Ensuring that this system has up-to-date, high security standards and a skilled cybersecurity professional to vulnerability test the inventory management system will help prevent data breaches. A keycard or biometric authentication should be used in the workplaces that have access to the inventory management system. Pfizer should have a set building and back up IT systems that can be used in the case of any downtime of the system.

Internet of Things (IoT) Security (Miranda Begley)

Pfizer distributes devices associated with the IoT in order for their employees to complete their job tasks. Some of the devices that can be associated with the IoT include cell phones, printers, laptops, bluetooth headphones, etc. These devices can be used to monitor their equipment, manage their security, communication with other peers/employees, training, or even collecting data for the company.

Protect/Awareness and Training (PR.AT)/PR.AT-1

Anyone in the world can potentially hack into one of the employee's IoT devices and steal confidential information from the company, data from millions of consumers, or mess with the integrity of their data. Unauthorized access to these devices is also another huge risk associated with the IoT. While these devices help regulate business procedures, it is important that the security of these devices are top-notch.

Recommended Control

It is very important to make sure that all Pfizer employees are well trained in safe guards that will protect their IoT devices. Education on proper passwords, biometric authentication, cybersecurity risks, unauthorized access, and other things associated with the security of their devices should be given. Awareness on what could happen if the wrong person gets a hold of their device should be regularly given to employees. Continuous monitoring of these devices and the ICloud it uses can help protect them from hackers. Strong encryption techniques should be used on all data to protect customers and employees.

Conclusion (Leah Drew)

For a large company such as Pfizer, it is important to follow the NIST cybersecurity framework using the five functions of identify, protect, detect, respond, and recover. In this assessment, we have identified the following assets to focus on: intellectual property, factories, web servers, research databases, the inventory management system, and IoT devices.

We should not undervalue the importance of identifying assets to protect. ID.AM-1 was selected for this purpose. Keeping an up-to-date inventory of devices and systems that need to be managed provides a strong foundation for Pfizer's cybersecurity.

RC.RP-1 and RS.RP-1 emphasize the importance of creating strong plans for response and recovery. It is important to assume that a cyberattack will happen and prepare for that event rather than to hope that it will not happen. Creating a clear plan and informing employees of the procedures will help the organization to respond and recover efficiently.

DE.CM-5, PR.AC-4, and PR.AT-1 were selected as subcategories due to Pfizer's large number of employees and systems. Humans are the weakest link in any cybersecurity system, and we should not underestimate the consequences of employee error or insider threats. Monitoring employees and restricting the systems that they are authorized to access as outlined in previous sections will help Pfizer to protect against and respond to a cyberattack.

This assessment is only a starting point. To improve their cybersecurity stance, Pfizer will now need to create policies and procedures based on the recommended controls above. Additionally, cybersecurity is not something to be assessed once and never thought about again. Pfizer will need to review and update their plan as Pfizer's assets and the industry as a whole change.