PELORUS
Enabling Technology in the Right Direction

CASE STUDY

# Securing Critical Data in the Pharmaceutical Sector: A DFIR Case Study By Pelorus

## Background:

PharmaCo is a global pharmaceutical business that focuses on the creation, production, and distribution of prescription medications. The business has several research and manufacturing sites throughout the globe and is the owner of large amounts of sensitive intellectual property, including confidential clinical trial data and unique formulas. PharmaCo has put in place a strong incident response strategy to properly handle any security issues due to the nature of the sector and the crucial need to ensure patient safety and maintain regulatory compliance.

## Overview of the incident:

One morning, PharmaCo's security team noticed unusual network activity that may be a sign of a cyberattack. Unauthorized access attempts and irregular file transfers from a server hosting sensitive research data are all part of the activity. The event is

### Challenges:

- Large amounts of sensitive intellectual property at risk
- Need for a strong incident response strategy to ensure patient safety and regulatory compliance
- Detection of unusual network activity that may be a sign of a cyberattack
- Communication and stakeholder management during a security event

### Results:

- Swift identification and escalation of the security issue
- Comprehensive investigation to determine the nature and consequences of the occurrence
- Prompt action to contain the incident and prevent future compromise
- Thorough examination of systems and procedures to find and fix any vulnerabilities
- Cataloging of incident response procedure and recording of lessons learned for continuous improvement

swiftly escalated by the security staff to the incident response team (IRT), which takes prompt action.

The incident response team quickly accepts the warning and starts the incident response procedure after detection. The affected server, the type of activity, and any relevant logs or network traffic data are all gathered to learn as much as they can about the occurrence. The group creates lines of communication and puts together a cross-functional incident response team, including senior management, IT, and security officials.

## Investigation and triage:

In order to fully grasp the nature and consequences of the occurrence, the incident response team first performs a comprehensive investigation. To determine the attackers' strategies, possible vulnerabilities exploited, and prospective data exfiltration, they analyze logs, network traffic, and system artefacts. Additionally, if required, they consult with forensic specialists and gather evidence for legal purposes.

## Containment and Mitigation:

After the security breach is confirmed, the incident response team concentrates on stopping the incident to prevent future compromise. They cut off unauthorized connections, secured the compromised server from the rest of the network, and repaired any vulnerabilities found. The team determines the degree of data exfiltration, if any, and implements the necessary countermeasures.

Pelorus Technologies has a proven track record of delivering high-quality solutions that help clients address complex challenges related to cybersecurity, digital forensics, and intelligence gathering. As a leading provider of cybersecurity solutions, Pelorus Technologies is continuously monitoring the evolving threat landscape and developing solutions to address emerging threats. We have a unique distinction of being an organization who has served 50+ Law Enforcement Agencies.

Effective stakeholder management is essential during a security event, as is communication with all parties involved. The incident response team communicates openly and often with top management, legal counsel, regulatory agencies, and other parties who might be impacted. They offer prompt reports on the occurrence, the responses made, and any potential effects on patient safety, legal compliance, and intellectual property.

## Recovery and remediation:

After the crisis has been contained, the team concentrates on getting things back to normal. They use a safe backup to reconstruct the hacked server, adding additional security features like two-factor authentication, access limits, and encryption. A thorough examination of systems and procedures is also carried out by the team in order to find and fix any vulnerabilities that may have contributed to the incident.

## Lessons Learned and Documentation:

The incident response team conducts a post-event evaluation to gauge the success of their reaction after the occurrence. They catalog the incident response procedure, note strengths and flaws, and record lessons learned. This data is used by the team to improve detection and response capabilities, introduce new preventative measures, and update the incident response plan.

Pelorus Technologies has a proven track record of delivering high-quality solutions that help clients address complex challenges related to cybersecurity, digital forensics, and intelligence gathering. As a leading provider of cybersecurity solutions, Pelorus Technologies is continuously monitoring the evolving threat landscape and developing solutions to address emerging threats. We have a unique distinction of being an organization who has served 50+ Law Enforcement Agencies.

## Continuous Improvement:

PharmaCo invests in continual training, awareness campaigns, and tabletop exercises for staff members to maintain a proactive security posture. The incident response team regularly runs exercises and simulations to evaluate the efficiency of their response strategy and guarantee readiness for upcoming situations. To stay current on new risks and best practices, they also share threat intelligence and work together with other professionals in the sector.

## Conclusion:

PharmaCo effectively mitigated the security issue, minimizing the possible impact on patient safety, intellectual property, and regulatory compliance through quick identification, efficient reaction, and departmental teamwork. PharmaCo's mission to protect vital assets and uphold confidence in the pharmaceutical business is furthered by the incident response team's methodical methodology, commitment to continuous improvement, and determination to uphold posture.

Pelorus Technologies has a proven track record of delivering high-quality solutions that help clients address complex challenges related to cybersecurity, digital forensics, and intelligence gathering. As a leading provider of cybersecurity solutions, Pelorus Technologies is continuously monitoring the evolving threat landscape and developing solutions to address emerging threats. We have a unique distinction of being an organization who has served 50+ Law Enforcement Agencies.